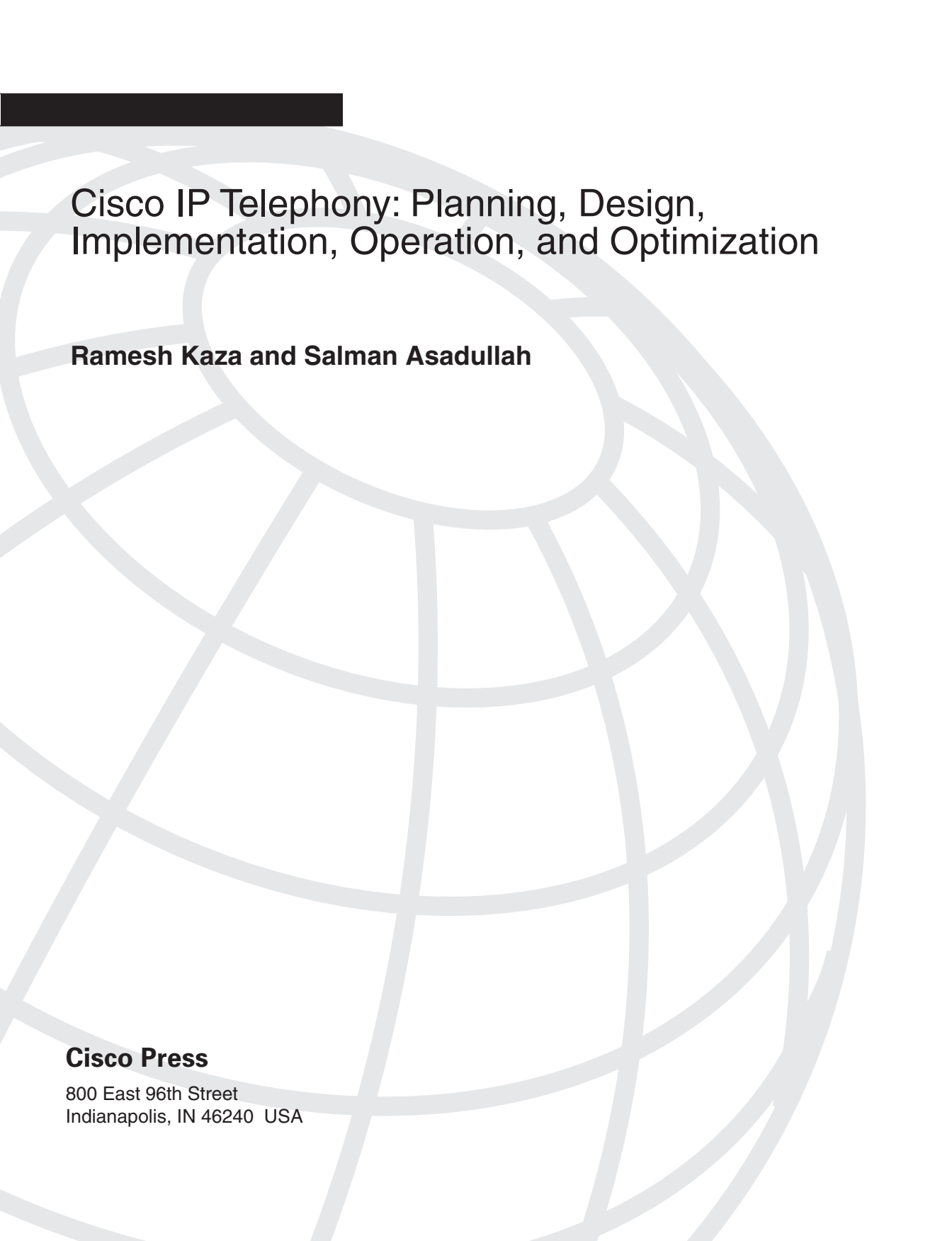




Cisco IP Telephony:

Planning, Design, Implementation, Operation, and Optimization

A guide to successful deployment of the
Cisco IP Telephony solution



Cisco IP Telephony: Planning, Design, Implementation, Operation, and Optimization

Ramesh Kaza and Salman Asadullah

Cisco Press

800 East 96th Street
Indianapolis, IN 46240 USA

Cisco IP Telephony: Planning, Design, Implementation, Operation, and Optimization

Ramesh Kaza and Salman Asadullah

Copyright© 2005 Cisco Systems, Inc.

Published by:

Cisco Press

800 East 96th Street

Indianapolis, IN 46240 USA

All rights reserved. No part of this book may be reproduced or transmitted in any form or by any means, electronic or mechanical, including photocopying, recording, or by any information storage and retrieval system, without written permission from the publisher, except for the inclusion of brief quotations in a review.

Printed in the United States of America 1 2 3 4 5 6 7 8 9 0

First Printing: February 2005

Library of Congress Cataloging-in-Publication Number: 2003108110

ISBN: 1-58705-157-5

Warning and Disclaimer

This book is designed to provide information about Cisco IP Telephony. Every effort has been made to make this book as complete and as accurate as possible, but no warranty or fitness is implied.

The information is provided on an “as is” basis. The authors, Cisco Press, and Cisco Systems, Inc. shall have neither liability nor responsibility to any person or entity with respect to any loss or damages arising from the information contained in this book or from the use of the discs or programs that may accompany it.

The opinions expressed in this book belong to the authors and are not necessarily those of Cisco Systems, Inc.

Trademark Acknowledgments

All terms mentioned in this book that are known to be trademarks or service marks have been appropriately capitalized. Cisco Press or Cisco Systems, Inc. cannot attest to the accuracy of this information. Use of a term in this book should not be regarded as affecting the validity of any trademark or service mark.

Feedback Information

At Cisco Press, our goal is to create in-depth technical books of the highest quality and value. Each book is crafted with care and precision, undergoing rigorous development that involves the unique expertise of members from the professional technical community.

Readers’ feedback is a natural continuation of this process. If you have any comments regarding how we could improve the quality of this book, or otherwise alter it to better suit your needs, you can contact us through e-mail at feedback@ciscopress.com. Please make sure to include the book title and ISBN in your message.

We greatly appreciate your assistance.

Corporate and Government Sales

Cisco Press offers excellent discounts on this book when ordered in quantity for bulk purchases or special sales.

For more information, please contact: U.S. Corporate and Government Sales 1-800-382-3419
corpsales@pearsontechgroup.com

For sales outside the U.S., please contact: International Sales international@pearsoned.com

Publisher	John Wait
Editor-in-Chief	John Kane
Cisco Representative	Anthony Wolfenden
Cisco Press Program Manager	Jeff Brady
Production Manager	Patrick Kanouse
Development Editor	Jennifer Foster
Project Editor	Marc Fowler
Copy Editor	Bill McManus
Technical Editors	Niels Brunsgaard
	Mark Gallo
	Abderrahmane Mounir
	Gert Vanderstraeten
Team Coordinator	Tammi Barnett
Book and Cover Designer	Louisa Adair
Compositor	Mark Shirar
Indexer	Tim Wright



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

European Headquarters
Cisco Systems International BV
Haarlerbergpark
Haarlerbergweg 13-19
1101 CH Amsterdam
The Netherlands
www-europe.cisco.com
Tel: 31 0 20 357 1000
Fax: 31 0 20 357 1100

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
www.cisco.com
Tel: 408 526-7660
Fax: 408 527-0883

Asia Pacific Headquarters
Cisco Systems, Inc.
Capital Tower
168 Robinson Road
#22-01 to #29-01
Singapore 068912
www.cisco.com
Tel: +65 6317 7777
Fax: +65 6317 7799

Cisco Systems has more than 200 offices in the following countries and regions. Addresses, phone numbers, and fax numbers are listed on the

Cisco.com Web site at www.cisco.com/go/offices.

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

Copyright © 2003 Cisco Systems, Inc. All rights reserved. CCIP, CCSP, the Cisco Arrow logo, the Cisco *Powered* Network mark, the Cisco Systems Verified logo, Cisco Unity, Follow Me Browsing, FormShare, IQ Net Readiness Scorecard, Networking Academy, and ScriptShare are trademarks of Cisco Systems, Inc.; Changing the Way We Work, Live, Play, and Learn, The Fastest Way to Increase Your Internet Quotient, and iQuick Study are service marks of Cisco Systems, Inc.; and Aironet, ASIST, BPX, Catalyst, CCDA, CCDP, CCIE, CCNA, CCNP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, the Cisco IOS logo, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Empowering the Internet Generation, Enterprise/Solver, EtherChannel, EtherSwitch, Fast Step, GigaStack, Internet Quotient, IOS, IP/TV, iQ Expertise, the iQ logo, LightStream, MGX, MICA, the Networkers logo, Network Registrar, *Packet*, PIX, Post-Routing, Pre-Routing, RateMUX, Registrar, SlideCast, SMARTnet, StrataView Plus, Stratm, SwitchProbe, TeleRouter, TransPath, and VCO are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the U.S. and certain other countries.

All other trademarks mentioned in this document or Web site 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. (0303R)

Printed in the USA

About the Authors

Ramesh Kaza, CCIE No. 6207, is a technical leader in the World Wide Voice Practice Group (Customer Advocacy) at Cisco Systems. He has been with Cisco for five years. Ramesh has provided planning, design, and implementation support to many customers in deploying the Cisco IP Communications solutions. Prior to working on IP Communications, he was involved in validating the network designs for enterprise and service provider customers. He is a speaker at the Cisco Networkers event and has presented topics titled “Troubleshooting IPT Networks” and “Designing Large-Scale IPT Networks.” Prior to joining Cisco Systems, Ramesh worked for Software Technology Parks of India–Bangalore as a member of the technical staff, and he has played a major role in building the Internet backbone. Ramesh holds a bachelor’s degree in electronics and communications engineering.

Salman Asadullah, CCIE No. 2240, is a technical leader at Cisco Systems. As a recognized expert within Cisco and the industry, he has been designing and troubleshooting large-scale IP and multiservice networks for more than eight years. Salman represents Cisco in industry panel discussions and technical platforms such as NANOG, APRI-COT, SANOG, ASEAN, IETF, IPv6 Forum, Networkers, and so on. Salman influences technology directions and decisions with Cisco business units and the Internet community. He has produced several technical documents and white papers and is a coauthor of *Cisco CCIE Fundamentals: Network Design and Case Studies*. Salman has also developed CCIE exams for IP and multiservice technologies. He holds a bachelor’s degree in electrical engineering from The University of Arizona and a master’s degree in electrical engineering from Wichita State University.

About the Technical Reviewers

Niels Brunsgaard, CCIE No. 1544, has been with Cisco Systems as a consulting engineer since 1999, specializing in IP telephony. He has been involved in the planning, design, and implementation of a dozen IP telephony networks throughout Asia Pacific and North America. Niels holds a bachelor's degree in electro-mechanical engineering from the Denmark Technical University in Copenhagen, and a master's degree in telecommunications from the University of Colorado. He is a double CCIE, with certification in voice in addition to routing and switching.

Mark Gallo is a technical manager with America Online, where he leads a group of engineers responsible for the design and deployment of the domestic corporate intranet. His network certifications include Cisco CCNP and Cisco CCDP. He has led several engineering groups responsible for designing and implementing enterprise LANs and international IP networks. He has a BS in electrical engineering from the University of Pittsburgh. Mark resides in northern Virginia with his wife, Betsy, and son, Paul.

Abderrahmane Mounir, CCIE No. 4312, is a network consulting engineer at the Cisco Systems Advanced Services Group in San Jose. He has been working with large-scale IP telephony customers in planning, designing, implementing, and operating IP telephony networks since CallManager release 2.3. He has helped customers to successfully deploy and migrate large IP telephony deployments. He represents Cisco by presenting IPT end-to-end solutions and troubleshooting sessions at Networkers and other internal forums. He has also contributed to the creation and the design of the CCIE voice track. Abderrahmane holds a bachelor's degree in telecommunications engineering and a master's degree in electrical and computer engineering.

Gert Vanderstraeten has been working as a telecom/datacom engineer for companies such as Alcatel, Bell, and Lucent Technologies since 1993. Between 1998 and 2002, he was an independent contractor for the Cisco Systems IT department. During this period, his main focus was the implementation, maintenance, and design of VoIP, IP telephony, voice, and video applications, and the integration of Cisco AVVID technologies into large-scale solutions. In September 2002, he became a member of the technical staff and was operating until May 2004 within the Cisco Systems global enterprise architecture solutions team. Gert is currently working in the Advisory Services team as enterprise architect, where he takes on responsibility for large-scale customer deployments.

Dedications

For my wife for her tireless support and encouragement in this project. Also, for my daughter and son who sacrificed time with dad to make this book happen.

I also dedicate this book to my family for their never-ending support.

—Ramesh

I dedicate this book to:

The people around the world who are suffering and oppressed.

My affectionate parents, who gave me their best, and to my loving wife, for her support and encouragement.

—Salman

Acknowledgments

From Ramesh Kaza and Salman Asadullah:

There are many people who helped us to make this project successful. Please forgive us if we have inadvertently omitted the name of anyone who made such helpful contributions.

Thanks go to the following:

Himanshu Desai, senior manager, Advanced Services; Mike Quinn, VP, technical support; Kadir Koken, director, customer advocacy; and Khalid Raza, Cisco Distinguished Engineer, Cisco Systems, Inc., who encouraged us to write this book and supported us throughout this project.

Abderrahmane Mounir, network consulting engineer, Cisco Systems, Inc., for contributing to Chapter 6, verifying the configuration examples, reviewing the entire book, and providing valuable feedback.

Gert Vanderstraeten, enterprise architect for the Advisory Services team at Cisco Systems, Inc., for contributing to Chapter 7, reviewing the entire book, and providing valuable feedback.

Rajesh Ramarao, technical leader, Cisco Systems, Inc., for his contributions to parts of Chapter 9.

Jake Hartinger, technical leader, Cisco Systems, Inc., for humbly contributing to the valuable questionnaires in Appendixes B and C.

Niels Brunsgaard, technical leader, Cisco Systems, Inc., for reviewing parts of the book and providing valuable suggestions.

Mark Gallo, technical manager, America Online, for reviewing the entire book, helping in content rearrangement, and providing valuable feedback.

Thanks to all our colleagues and friends at Cisco Systems, Inc. whose work has helped us to complete this project. Especially, thanks to the members of the Advanced Services team: Hymed Besrou, Jine-Wen-Kou, Talal Siddiqui, Oludare Odunuga (Tola), Dave Turner, John Vosburg, Alvin Laguerta, Sanjay Jani, Imran Chaudhary, Kathy Decker, and Wesley Shuo.

Thanks to all the customers with whom we have worked over several years and in doing so acquired valuable knowledge and expertise that we have documented in this book.

We would like to express our special thanks to John Kane, editor in chief, for his expert guidance; Andrew Cupp and Jennifer Foster, development editors; Bill McManus, copy editor; Tammi Barnett, editorial assistant; and all other staff at Cisco Press for making this publication possible.

This Book Is Safari Enabled



The Safari® Enabled icon on the cover of your favorite technology book means the book is available through Safari Bookshelf. When you buy this book, you get free access to the online edition for 45 days.

Safari Bookshelf is an electronic reference library that lets you easily search thousands of technical books, find code samples, download chapters, and access technical information whenever and wherever you need it.

To gain 45-day Safari Enabled access to this book:

- Go to <http://www.ciscopress.com/safarienabled>
- Complete the brief registration form
- Enter the coupon code P7KR-KEMJ-SV5P-I4JV-ZZTV

If you have difficulty registering on Safari Bookshelf or accessing the online edition, please e-mail customer-service@safaribooksonline.com.

Contents at a Glance

	Foreword	xxi
	Introduction	xxii
Part I	Overview of Technology, Protocols, and the PDIOO Methodology	3
Chapter 1	Cisco IP Telephony Solution Overview	5
Chapter 2	Planning, Design, Implementation, Operation, and Optimization Overview	65
Part II	Large-Scale IPT and Voice-Mail Network	77
Chapter 3	Large-Scale Enterprise Requirements for IP Telephony	79
Chapter 4	Planning Phase	95
Chapter 5	Design Phase: Network Infrastructure Design	141
Chapter 6	Design of Call-Processing Infrastructure and Applications	179
Chapter 7	Voice-Mail System Design	279
Chapter 8	Implementation	377
Chapter 9	Operations and Optimization	437
Part III	Appendixes	505
Appendix A	Cisco IP Phone Models and Selection Criteria	507
Appendix B	IPT Planning Phase: Network Infrastructure Analysis Questionnaire	513
Appendix C	IPT Planning Phase: Telecom Infrastructure Analysis Questionnaire	541
Appendix D	IPT Design Phase: IP Phone Selection Questionnaire	561
Appendix E	IPT Design Phase: IPT Requirement Analysis Questionnaire	567
Appendix F	Ordering T1/E1 PRI from the Carrier Questionnaire	589
Appendix G	Voice-Mail Design Questionnaire	595
Appendix H	IP Implementation Checklist	611
Index		629

Contents

Foreword xxi

Introduction xxii

Part I Overview of Technology, Protocols, and the PDIOO Methodology 3

Chapter 1 Cisco IP Telephony Solution Overview 5

Legacy Voice and Data Networks 5

Next-Generation Multiservice Networks 6

Networks Based on Cisco AVVID 9

Signaling and Transport Protocols 11

Telco Signaling Protocols 12

Analog Signaling 12

Digital Signaling 12

VoIP Protocols 13

H.323 14

SIP 15

MGCP 18

SCCP 20

RTP/RTCP 20

IP Telephony Components 21

Network Infrastructure 22

Call Processing 22

CallManager Clustering 23

Device Weights 24

Dial Plan Weights 26

CallManager Directory Services 29

IP Telephony Endpoints 31

Cisco IP Phones 31

SoftPhones 32

Wireless IP Phones 34

Voice Gateways 34

Survivable Remote Site Telephony 35

Cisco CallManager Express 35

Call Admission Control 36

CallManager Locations-Based CAC 36

Gatekeeper CAC 37

Fax 37

Media Resources 38

Applications 38

Customer Response Solution 38

Cisco Unity 39

	Cisco Emergency Responder	40
	Cisco Conference Connection	41
	IP Phone Services	41
	IP Telephony Deployment Architectures	42
	Single-Site Deployment	43
	Centralized Call Processing with Remote Branches	44
	Distributed Call Processing Deployment	45
	Clustering over the IP WAN	46
	Local Failover Deployment Model	47
	Remote Failover Deployment Model	48
	Call-Flow Scenarios	49
	IP Phone-to-IP Phone Call	50
	Intracluster Call	52
	Intercluster Call	53
	Intercluster Call with the Gatekeeper	54
	Off-Net Calls	56
	Using MGCP Gateway	56
	Using H.323 Gateway	59
	Summary	62
Chapter 2	Planning, Design, Implementation, Operation, and Optimization Overview	65
	Planning Phase	66
	Design Phase	68
	Network Infrastructure Design	69
	Design of Call Processing Infrastructure and Applications	69
	Software Version Evaluation	70
	Design Validation	70
	Implementation Phase	71
	Operation and Optimization Phase	73
	Summary	74
Part II	Large-Scale IPT and Voice-Mail Network	77
Chapter 3	Large-Scale Enterprise Requirements for IP Telephony	79
	Customer Profile	80
	Data Network Architecture	80
	Voice Network Architecture	83
	Data Applications	83
	Directory and Messaging Architecture	84
	PBX and Voice-Mail System Features	84
	Customer Requirements	86
	System Architecture	86
	IP Phones	87

Integration and Replacement of Legacy PBX Systems	87
Integration and Replacement of Legacy Voice-Mail Systems	87
Voice Gateways	88
Quality of Service	88
Call Routing	88
Emergency Services	89
IPT Features and Applications	90
Security	91
Redundancy and High Availability	91
Network Management	92
Return on Investment	92
Summary	93

Chapter 4 Planning Phase 95

Getting Started	96
Network Infrastructure Analysis	97
Campus Network Infrastructure	98
Access Layer	99
Distribution Layer	104
Core Layer	105
Cabling Infrastructure	105
Common Guidelines	106
QoS in Campus Network Infrastructure	107
Data and Voice Traffic Characteristics	108
Oversubscription in Campus Networks	108
Network Trust Boundaries	109
IP Phone QoS	110
Inline Power for IP Phones	112
Wireless IP Phone Infrastructure	113
WAN Infrastructure	114
QoS in WAN Infrastructure	116
Minimizing Delay	117
Using Traffic Shaping	120
Provisioning WAN Bandwidth	121
Using Voice Compression	123
Network Services	126
DHCP	126
DNS	127
NTP	128
Directories and Messaging	128
Power and Environmental Infrastructure	129
Telecom Infrastructure Analysis	131
PBX Infrastructure and Migration	131
Telephony Numbering Plan	132

Voice-Mail Infrastructure and Migration	133
Emergency Services	133
Telephony Features and Applications	133
Business Continuity and Disaster Recovery	134
Securing IPT Infrastructure	134
Redundancy and High Availability	135
IPT Network Management System	137
Summary	138

Chapter 5 Design Phase: Network Infrastructure Design 141

Call-Processing Architecture	141
IP Phone Selection	143
Network Infrastructure Design Tasks	145
Designing IP Addressing and VLAN Scheme	145
Designing DHCP and TFTP Services	147
Central Site LAN Infrastructure	150
Central Site LAN QoS Design	150
Access Layer Catalyst 6500 QoS Configuration Guidelines	152
Distribution and Core Layer Catalyst 6500 QoS Configuration Guidelines	157
Remote-Site IPT Infrastructure	159
Remote-Site LAN QoS Design	161
Configuring the Remote-Site LAN Switches for QoS	162
Remote-Site WAN QoS Design	166
Perform DSCP-to-CoS Mappings	168
Map CoS-to-DSCP Mapping on Remote-Site Routers	169
Configure WAN Interface Queuing	170
Central Site WAN QoS Design	174
Summary	177

Chapter 6 Design of Call-Processing Infrastructure and Applications 179

High-Level IPT Design	179
Fax and Analog Terminals	179
Voice Gateways	180
Access to the PSTN	180
Access to the PBX	181
Media Resources	181
Conferencing and Transcoding	182
Music on Hold	183
IPT Applications	185
AutoAttendant	185
Interactive Voice Response	186
Call Center	186
Voice Messaging	186

Low-Level Design	187
CallManager Cluster Design	187
CallManager Scalability and Sizing	190
Customer Response Solution Server Scalability and Sizing	192
Sizing the Number of Agents	193
Sizing the Number of IVR Ports	195
Sizing the Gateway Trunks for the Call Center	196
CallManager Group Configuration	198
CallManager Date/Time Configuration	199
CallManager Region Configuration	200
CallManager Location Configuration	201
Device Pool Configuration	203
Media Resources Configuration	204
Conferencing	204
Transcoding	208
Music on Hold	211
Configuring the MRGs and MRGLs	216
Gateway Selection and Sizing	221
Dial Plan Architecture	224
Numbering Plan	225
Call-Routing Requirements	228
CallManager Route Plan	229
Partition Design	231
Calling Search Space Design	233
Route Groups	238
Route Lists	239
Route Patterns	241
Gatekeeper	256
Inbound Call Routing	258
Automated Alternate Routing	259
Survivable Remote Site Telephony	261
SRST for Seattle and Melbourne Remote Sites	262
Fax and Modem	269
Securing the IPT Infrastructure	272
Securing CallManager and Application Servers	273
Using a Firewall and ACLs	274
Securing the IPT Network from the Outside World	274
Securing IPT Endpoints	275
Securing Campus Network Devices	276
Securing Voice Gateways	276
Establishing Physical Security	277
Installing Host-Based Intrusion Detection	277
Summary	277

Chapter 7	Voice-Mail System Design	279
	Defining the Voice-Mail System Architecture	279
	Microsoft Active Directory and Exchange	281
	Active Directory Architecture	282
	Exchange 2000 Messaging Architecture	283
	Unity Deployment Model	284
	Physical Placement of Unity Servers	284
	High Availability	285
	Securing Unity Servers	285
	Backup of Unity Servers	285
	Voice-Mail Access Options	285
	Telephone User Interface	286
	Graphical User Interface	287
	Designing a Cisco Unity System	289
	Message Store Options and Sizing	290
	Sizing Unity Ports and Sessions	291
	Unity Server Hardware	292
	Data Protection	293
	Exchange Software Licensing	293
	Unity Software Licensing	293
	Extending the Schema for Unity and Unity Bridge	294
	Installing Cisco Unity	295
	Unity Installation Account	296
	End-User Interaction	296
	Integrating Voice Mail	296
	Unity Integration with CallManager	297
	Configuring Partitions and CSS in CallManager	297
	Changing Service Parameters in CallManager	298
	Defining MWI On and Off Numbers in CallManager	298
	Defining Voice-Mail Ports in CallManager	299
	Defining the Voice-Mail Pilot Number	301
	Defining the Voice-Mail Profile	302
	Reserving Ports for MWIs and Outcall Notifications in Unity	302
	Making Changes to the Octel Access Numbers	302
	Configuring the AutoAttendant functionality in Unity	303
	Octel Integration with CallManager	304
	SMDI Integration	304
	Integration Using VG248	305
	Digital Integration Using DPA	307
	Designing the Cisco Unity Networking	307
	Digital Networking	308
	Bridge Networking	308
	AMIS Networking	308
	VPIM Networking	309

Networking Octel and Unity	309
Deployment Architecture with Unity Bridge	310
Unity Bridge Software and Hardware	311
Configuring Unity Bridge	312
System Settings	313
Digital Networking	315
Unity Nodes	316
Octel Nodes	316
Unity Internet Voice Connector	318
Customizing the Cisco Unity System	319
Subscribers	321
Class of Service	321
Subscriber Template	327
Account Policy	339
Subscribers	340
Public Distribution Lists	346
Call Management	347
Call Handlers	347
Directory Handlers	352
Interview Handlers	355
Call Routing	355
Restriction Tables	356
Network	356
Primary Location	356
Delivery Locations	358
Bridge Options	360
System	361
Configuration	362
Schedules	364
Holidays	364
Licensing	365
Authentication	365
Integration	366
Ports	366
Multiple Directory Handlers	367
Improving the User Experience During Migration	373
Export Spoken Names from Octel to Unity	373
Pre-Enrollment Procedures	374
Summary	375

Chapter 8 Implementation 377

Complete Preimplementation Tasks	378
Perform Implementation Readiness Analysis	378
Site Readiness	379
Voice Network Readiness	379

Data Network Readiness	380
IP Telephony Readiness	380
Implement IPT Components	380
CallManager and Application Server Implementation	380
Operating System Installation	381
Installing CallManager and Other Applications	381
Installing Tools and Third-Party Applications	382
Implementing Voice Gateways	382
Implementing Catalyst T1 Voice Gateways Using the WS-X6608-T1 Module	383
Implementing a Catalyst T1/E1 Voice Gateway by Using a CMM Module	388
Troubleshooting Gateway Connectivity and Registration Issues	393
Implementing IP Phones	394
Implementation of IP Phones Using BAT	394
Physical Phone Installation	396
Implementing the Dial Plan	397
Dialed Number Analyzer	397
Implementing Cisco IP AutoAttendant	399
Configuration Steps for AA	402
Implementing IP ICD	406
Configuration Steps for IP ICD	409
Call Center Agent and Supervisor Login Options	415
Implementing IP IVR	415
Implementing IP Phone Services	416
Corporate Directory Access Through IP Phones	417
Troubleshooting IP Phone Services	423
Identify the Implementation Tools	425
Checking the CallManager OS Version	425
Checking the CallManager Version	426
Checking the SQL Version	426
Database Layer Tool to Check SQL Subscriptions	427
Checking Inconsistencies in the Software Versions Within the Cluster	429
Multi-Level Administration Tool	429
Functional Groups	430
User Groups	430
Access Levels	431
MLA Logs	431
Deploy IPT Solution Pilot	431
Implementation Acceptance Tests	431
Post-Implementation Documentation	432
Day 2 Support	432
Escalation Procedures	433

Training	433
End-User Training	434
Help Desk Staff Training	434
Voice Network Administration Staff Training	434
Voice Network Design/Architecture Staff Training	435
Summary	435

Chapter 9 Operations and Optimization 437

Software Upgrades	437
Operating System Upgrades	438
Subscribe to Notification Alerts	438
Stop Services	438
Use Recommended Server Access Methods to Perform Upgrades	439
Schedule the Upgrade	439
Document Registered Device Counts	439
Windows Operating System Upgrade	440
CallManager Software Upgrade	441
Upgrade Planning and Impacts	442
Failover Procedure	442
Recovery Methods	443
Application Software Upgrades	444
Upgrade Planning and Impacts	445
IP Phone and Gateway Upgrades	446
Upgrading the Firmware on a Few Cisco IP Phones or Gateways	446
Upgrade Planning and Impacts	448
Failover Procedures and Recovery Methods	449
BIOS Upgrades	449
Hardware Upgrades	449
Memory Upgrades	450
Server Hardware Upgrades	452
CallManager Operation and Monitoring Tools	452
Multilevel Administration	452
Quality Reporting Tool	452
QRT Viewer	454
Real-Time Monitoring Tool	454
Summary View	455
Server View	455
CallProcess View	456
Service View	457
Device View	458
CTI View	459
Perfmon View	459
RTMT Alerts	459
RTMT Reports	461

CallManager Traces	461
Trace Configuration	462
The Troubleshooting Trace Settings Page and Cisco CallManager Trace Collection Tool	463
Bulk Trace Analysis Tool	463
CDR Analysis and Reporting	464
User Reports	465
System Reports	465
Device Reports	465
Q.931 Translator	466
Alarm Configurations and Definitions	466
Backup and Restore System	467
Password-Changing Tools	468
Admin Utility	469
Event Viewer	472
Bulk Administration Tool	473
DHCP Management	473
Optimization Tips	474
Time Synchronization	475
CallManager Services	475
Name Resolution	475
IP Addressing	475
Subnetting and VLANs	476
Proactive Problem Identification and Resolution	476
Duplex and Speed Settings	477
Dial Plan Optimization	477
Route Pattern Design	477
Partition Rules	479
Calling Search Space Rules	479
Prefixing the Digits in Missed and Received Calls	480
Securing the Servers	480
Operating System Hardening	480
Cisco Security Agent	481
Service and Enterprise Parameter Fine-Tuning	481
Deployments Involving Shared Lines	486
Call Detail Records	486
CallManager Traces	487
Firmware Loads	487
Cluster Guidelines	487
Removing a Subscriber	487
Auto-Registration	487
Installing Third-Party Software Applications	489
Changing Session Timeout for CallManager	489
Cisco Unity Operations	490

Day 2 Monitoring and Management Tasks	490
CallManager Day-to-Day Monitoring Task List	491
CallManager Pre-Upgrade Task List	492
CallManager Post-Upgrade Task List	493
IPT Network Management Tools	495
CiscoWorks and IP Telephony Environment Monitor	495
Alerts and Activities	497
Active Partition Selector	498
Device Management	498
Notification Services	498
Fault History	499
Configuration	499
IP Phone Information Facility	500
SRST Monitoring Management	500
IP Phone Reachability Testing	500
IPT Security Displays	501
IP Phone Help Desk Utility	501
Gateway Statistics Utility	502
Summary	502

Part III Appendixes 505

Appendix A	Cisco IP Phone Models and Selection Criteria	507
Appendix B	IPT Planning Phase: Network Infrastructure Analysis Questionnaire	513
Appendix C	IPT Planning Phase: Telecom Infrastructure Analysis Questionnaire	541
Appendix D	IPT Design Phase: IP Phone Selection Questionnaire	561
Appendix E	IPT Design Phase: IPT Requirement Analysis Questionnaire	567
Appendix F	Ordering T1/E1 PRI from the Carrier Questionnaire	589
Appendix G	Voice-Mail Design Questionnaire	595
Appendix H	IP Implementation Checklist	611
Index		629

Foreword

In October, 1998, Cisco took a step forward in its entry into IP Telephony with the acquisition of Selsius Systems, a pioneer and innovator of next generation network PBX systems for high-quality telephony over IP networks. This began the revolution of converged data, voice and video networks rendering separate voice and data networks a thing of the past. Cisco is one of the front runners in changing the way enterprises and service providers deliver converging traditional voice, data, and video applications.

The overall IP communication industry has gained significant momentum. The original Selsius Systems product family acquired by Cisco has expanded and evolved at tremendous speed. Over four million IP phones and over three million Unity seats have been deployed.

In early 1999, I was asked to build a small team of network consulting engineers in order to help Cisco customers and partners with the planning, designing, implementation, operation and optimization (PDIOO) of IP communication networks by providing them with templates, tools and best practices. Salman Asadullah and Ramesh Kaza were among the first few senior engineers who I asked to help with this task. We began working with our customers and during this process we defined the PDIOO processes for core steps that are required for deploying IP communication solutions. These processes and best practices are being shared in this book using hypothetical customer scenarios in the form of a case study. As with any emerging technology, these processes and best practices change over the time, but the approach applied remain the same. Today, our team supports some of largest Cisco IP communication deployments, some with over with 10,000 IP phones. The team, which started with three network consulting engineers, has grown to over 30 engineers in the course of four years.

One day, Salman and Ramesh walked into my office and presented the idea of writing a book based on the experience we acquired on this roller coaster ride. With the strong technical background and experience they gained by working with the largest IP communications networks, it was a valuable idea.

While reviewing their final draft of the book I was impressed to see how beautifully they have made an excellent guide on how to approach the IP communication project using PDIOO life cycle for small-to-medium size deployment. I am confident that the reader will find this book highly valuable and practical because it can be used as a reference guide to create a framework for your IP communication convergence projects.

Regards,
Himanshu Desai
Senior Manager, Advanced Services
IP Communications Services Team

Introduction

IP telephony (IPT) technology has gained wide acceptance in the industry because it offers new ways to communicate and enables rich media communication capabilities. Recent studies have shown that deployment of IPT also helps improve employee productivity as a result of faster moves, adds, and changes; increased user mobility; and reduction in the time to set up telecommunication infrastructure for new office spaces. These are a few of the many benefits that are motivating organizations to move to IP-based PBX deployments.

Successful deployment of any new technology solution requires thorough understanding of the function of various components involved and the interaction among them. The architects and engineers who are tasked with implementing the IPT solution must ensure that the proposed architecture meets all the requirements and is also scalable in the future. To assist the architects and engineers in accomplishing this task, this book divides the deployment of IPT into planning, design, implementation, operation, and optimization (PDIOO) phases.

This book addresses the most important information that customers, network engineers, and architects should collect in each phase of the PDIOO methodology in deploying Cisco IPT solutions.

Goals and Methods

The goal of this book is to be a useful guide for network engineers and architects going through the various phases of planning and deploying a Cisco IPT solution. This book helps you to make the decisions that best suit a particular network scenario.

The major tasks involved in each phase of the PDIOO methodology are explained with the aid of a case study that includes the most commonly deployed Cisco IPT architectures, telephony features, and applications. You can use the questionnaires in the appendixes to collect details about the customer's current network and to gather IPT requirements to propose the most suitable IPT network architecture and a detailed design.

To keep this book concise, in-depth discussion of communication protocols is not included because this information is readily available in other books and in Requests for Comments (RFCs).

Target CallManager Release

The design principles and guidelines discussed in this book are applicable to Cisco CallManager version 3.3.3 and above. With the release of new versions of Cisco CallManager, you might find new features and scalability enhancements. However, the basic design rules and the PDIOO methodology remain the same.

How This Book Is Organized

This book is organized into three parts.

Part I, "Overview of Technology, Protocols, and the PDIOO Methodology," discusses the VoIP and IPT technology and related protocols, mechanisms, architectures, and basics. It also lays the foundation of the PDIOO methodology and discusses why the PDIOO methodology is critical for successful IPT network implementation. Part I includes the following:

- Chapter 1, "Cisco IP Telephony Solution Overview"
- Chapter 2, "Planning, Design, Implementation, Operation, and Optimization Overview"

Part II, "Large-Scale IPT and Voice-Mail Network," builds on the material discussed in Part I and provides a real-world example with technical details, examples, design tips, and configuration examples at each phase of the

PDIOO methodology on how to build a successful and efficient large-scale IPT network from scratch. Part II includes the following:

- Chapter 3, “Large-Scale Enterprise Requirements for IP Telephony”
- Chapter 4, “Planning Phase”
- Chapter 5, “Design Phase: Network Infrastructure Design”
- Chapter 6, “Design of Call-Processing Infrastructure and Applications”
- Chapter 7, “Voice-Mail System Design”
- Chapter 8, “Implementation”
- Chapter 9, “Operations and Optimization”

The final part includes eight appendixes that comprise questionnaires that enable you to collect the information that you need at different steps of the PDIOO methodology. This information is critical for a successful implementation of an IPT and voice-mail network. The appendixes are as follows:

- Appendix A, “IP Phone Models and Selection Criteria”
- Appendix B, “IPT Planning Phase: Network Infrastructure Analysis Questionnaire”
- Appendix C, “IPT Planning Phase: Telecom Infrastructure Analysis Questionnaire”
- Appendix D, “IPT Design Phase: IP Phone Selection Questionnaire”
- Appendix E, “IPT Design Phase: IPT Requirement Analysis Questionnaire”
- Appendix F, “Ordering T1/E1 PRI from the Carrier Questionnaire”
- Appendix G, “Voice-Mail Design Questionnaire”
- Appendix H, “IPT Implementation Checklist”

How to Read This Book

This book is organized logically with material advancing gradually. You can reference the various sections and chapters according to your needs and interests. If you have a good understanding of VoIP and IPT technology and tasks involved in PDIOO methodology, you might want to browse through Part I and spend more time on Part II. Part II references the appendix materials as appropriate, so you will have to refer to these appendixes quite often and will find them extremely useful.

This book provides several references and web links to useful material that is readily available and beyond the scope of this book.



Overview of Technology, Protocols, and the PDIOO Methodology

Chapter 1 Cisco IP Telephony Solution Overview

Chapter 2 Planning, Design, Implementation, Operation, and Optimization Overview



Cisco IP Telephony Solution Overview

This chapter provides a high-level overview of legacy networks and the Cisco Architecture for Voice, Video and Integrated Data (AVVID), including its components, underlying protocols, and technologies.

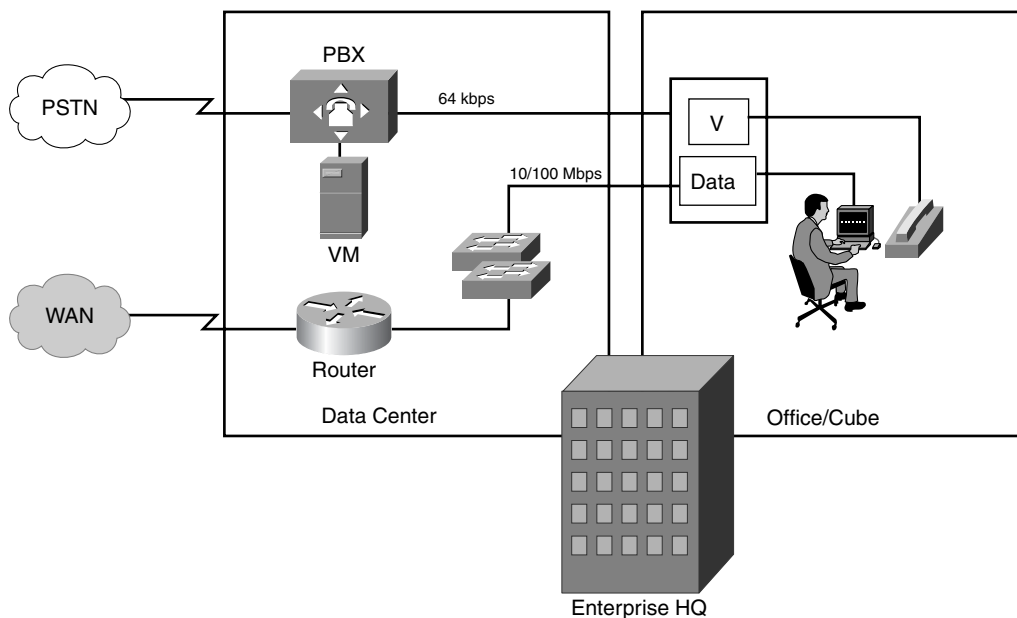
This chapter covers the following topics:

- Legacy voice and data networks and next-generation multiservice networks
- Signaling and transport protocols that are used to build Cisco IP telephony (IPT) networks
- IPT components, applications, and terms used in Cisco IPT solutions
- Components, applications, and terms used in Cisco IPT solutions
- Cisco IPT deployment architectures and the criteria used to choose the deployment model
- How various IPT components and protocols work together, including a look at various call-flow scenarios

The information that is presented in this chapter will help you to understand the operation of legacy voice networks and the evolution of IPT technology. You can use this while doing the planning, design, implementation, operation, and optimization (PDIOO) of Cisco IPT networks.

Legacy Voice and Data Networks

The term “legacy” refers to networks that have two separate infrastructures to support voice and data network services. A significant portion of many companies’ IT budget goes toward maintaining the distinct voice and data networks, which requires one staff dedicated to maintaining the legacy voice infrastructure, including PBXs and voice-mail systems, and another staff dedicated to supporting the data network infrastructure. Two other drawbacks associated with this approach is that these two separate infrastructures cannot share their resources with each other and have to be managed separately, both of which increase IT budgets. Figure 1-1 shows a common example of an enterprise that has separate data and voice networks.

Figure 1-1 *Separate Voice and Data Networks*

Next-Generation Multiservice Networks

The desire of industry to combine distinct voice and data networks led to the development of several new concepts and technologies, such as packetized voice. Packetized voice comprises several standards and protocols. Applications use these protocols and standards to provide value-added and cost-effective services to users.

Packetized voice enables a device to send voice traffic (for example, telephone and fax) over an IP/Frame Relay/ATM network. In case of Voice over IP (VoIP), the digital signal processor (DSP) that is located on the voice gateway segments the voice signal into frames. The voice gateway combines these frames to form an IP packet and sends the packet over the IP network. On the receiving end, a reverse action converts the voice information that is stored in the IP packet into the original voice signal.

Across the IP network, these voice packets are transported by using the Real-Time Transport Protocol (RTP) and RTP Control Protocol (RTCP) stack and by using the User Datagram Protocol (UDP) as a transport layer protocol. RTP provides timestamps and sequence numbers in each packet to help synchronize the voice frames at the receiving side. RTCP provides a feedback mechanism that informs session participants of the received quality of the voice call and includes information such as delay, jitter, and lost packets.

It is important to note that most of the real-time applications use UDP as the transport layer protocol rather than TCP, for the following reasons:

- TCP guarantees the retransmission of frames that are lost in the network, which is of no use in a packetized voice network because the late arrival of frames at the receiving end introduces delay. Hence, the capability of TCP to retransmit frames is not useful in packetized voice networks.
- TCP introduces unnecessary delay by waiting for acknowledgements for every packet. This delay is not noticeable in the data networks but causes poor voice quality in packetized voice networks.

In addition to using RTP/UDP/IP as the protocol stack to carry voice calls across the IP network, VoIP networks use VoIP signaling protocols to set up and tear down the calls, carry the information to locate the users/phones, and exchange capabilities such as compression algorithms to be used during the conversation. The commonly used signaling protocols in VoIP networks are H.323, Media Gateway Control Protocol (MGCP), Session Initiation Protocol (SIP), and Skinny Client Control Protocol (SCCP).

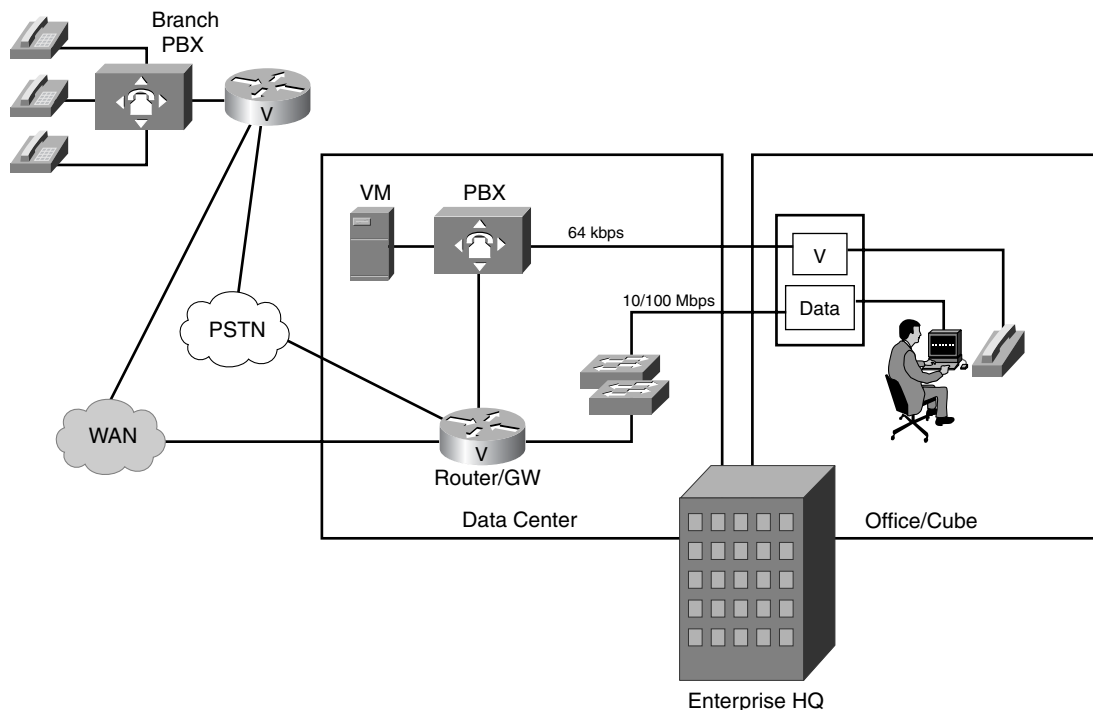
Introducing “packetized voice” capability into the router shown in Figure 1-1 turns the router into a voice gateway and enables the router to do the packetization just described along with the duties required as a regular data router. This change allows you to provide additional services such as toll bypass.

Toll bypass enables you to reduce the overall telephony expenditure by routing long-distance interoffice calls over existing packet-based WANs, thus avoiding interexchange carrier (IXC) toll charges. As shown in Figure 1-2, when you make phone calls between the enterprise headquarters and a branch location, you can send the voice calls via the WAN data circuit as opposed to using the Public Switched Telephone Network (PSTN). The connection from the PBX is now terminated on the gateway, allowing the gateway to receive both incoming and outgoing calls. This architecture also allows routing of a voice call over the internal network to the closest gateway to the destination of the call and then connects into the public network as a local phone call. This is called *Tail-End Hop-Off (TEHO)*. You need to be aware that TEHO is not allowed in all countries. Hence, when you are designing a VoIP network with toll bypass or TEHO, you need to check the local government regulations.

To ensure that the design of your toll-bypass application is effective, it must include a voice gateway that is able to support multiple types of call signaling as it interacts with the PSTN, WAN, and existing PBX systems. By maintaining a connection to the PSTN, as shown in Figure 1-2, the gateway can reroute calls to the PSTN if congestion or failure occurs within the packet network.

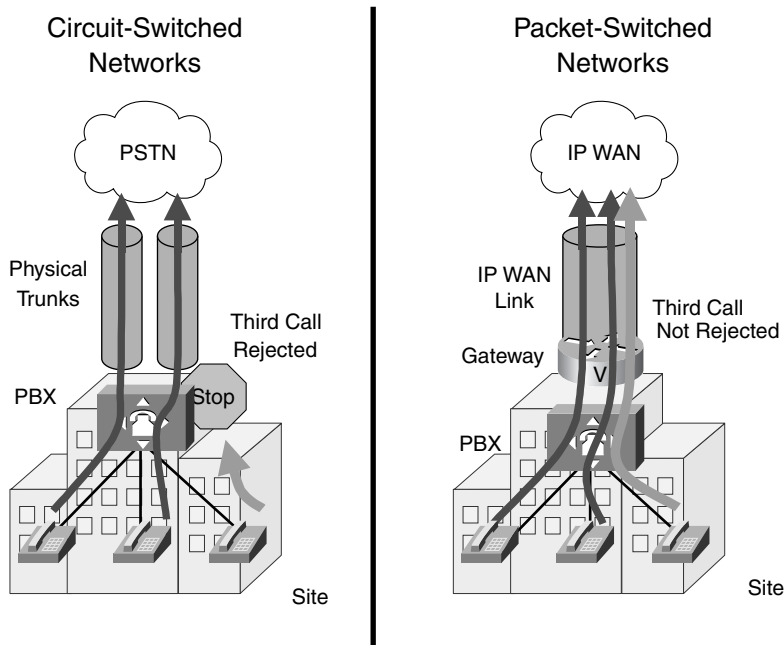
TIP

By having this voice gateway in the network, you eliminate the need to have a separate “tie line” for the voice-only traffic.

Figure 1-2 *Toll-Bypass Application*

The DSPs that are located on the voice gateways also have the capability to handle different types of compression algorithms, such as G.711, G.723.1, G.726, G.728, and G.729 traffic. These compression algorithms maximize the throughput on the packet network. Compression techniques on gateways, such as compressed RTP (cRTP), reduce the amount of bandwidth per voice call. You should be aware of the side effects of enabling cRTP on the voice gateways. cRTP processing on voice gateways essentially compresses all outgoing voice packets and decompresses the incoming compressed voice packets. Hence, if you have numerous voice calls across the WAN links, the router has to perform many cycles of this task, which can increase the amount of CPU resources consumed for cRTP, thus leaving less CPU cycles for the other tasks.

In traditional voice networks, each call consumes a fixed amount of bandwidth. The PBX does not place more calls than it can handle through the trunks connecting to the PSTN, as shown on the left side of Figure 1-3. In packetized networks, if bandwidth is available to make only two good-quality calls, in the absence of a call admission control (CAC) mechanism, the voice gateway allows the third call to go through, as shown on the right side of Figure 1-3. This third call degrades the quality of the existing two good voice calls. Hence, gatekeepers are deployed in the packetized networks to control the number of calls that can be sent over the WAN links. The CAC mechanism in the gatekeeper ensures that the gateway does not place the third call.

Figure 1-3 *Call Control in Circuit- and Packet-Switched Networks*

Gatekeepers perform CAC and bandwidth management in VoIP networks. Gatekeepers ensure that enough bandwidth is available before granting permission to a gateway to place a call across the IP WAN. After receiving permission from the gatekeeper, the originating gateway initiates a call setup with the terminating gateway over the packet network.

TIP

When you are using IP networks to carry packetized voice traffic, an optional but important consideration is to use proper admission and bandwidth control mechanisms.

Besides performing CAC and bandwidth management, gatekeepers can perform accounting, call authorization, authentication (via RADIUS), address lookup and resolution, and translation between E.164 numbers and the IP addresses.

Networks Based on Cisco AVVID

Networks no longer are limited to performing toll-bypass call routing. Today, many networks are replacing the legacy PBX systems with IP-based call-processing servers; replacing legacy voice-mail systems with IP-based voice-mail systems; replacing legacy phones with IP phones;

and replacing legacy video transmission with IP-based video transmission. This strategy is also the Cisco AVVID vision of truly converged voice, video, and data networks. In Cisco AVVID, IPT is one of the solutions. If three components of the legacy network previously shown in Figure 1-2 are replaced as described in the following list, the network evolves into the network shown in Figure 1-4:

- Legacy PBXs are replaced by IP-based call-processing servers, such as Cisco CallManager
- Legacy voice-mail systems are replaced by IP-based voice-mail systems such as Cisco Unity
- Legacy phones are replaced by Cisco IP Phones

The migration shown in Figure 1-4 is a big change from a legacy network. These types of migrations have been done on hundreds of networks around the world. Several organizations currently run and manage true IP-based networks for their data and voice traffic or are in the process of migrating to IPT solutions.

Figure 1-5 shows the high-level network architecture of an organization that has transitioned to a Cisco IPT solution. The IPT solution replaced all the legacy PBXs, voice-mail systems, and phones with a true end-to-end IP-based solution. This network supports thousands of users located in different parts of world, using IP-based devices communicating over IP infrastructure. To reach this goal, you have to follow a structured approach; the rest of the chapters in this book discuss the use of PDIOO methodology to build such an end-to-end IP-based telephony network.

Figure 1-4 *Today's Multiservice Networks*

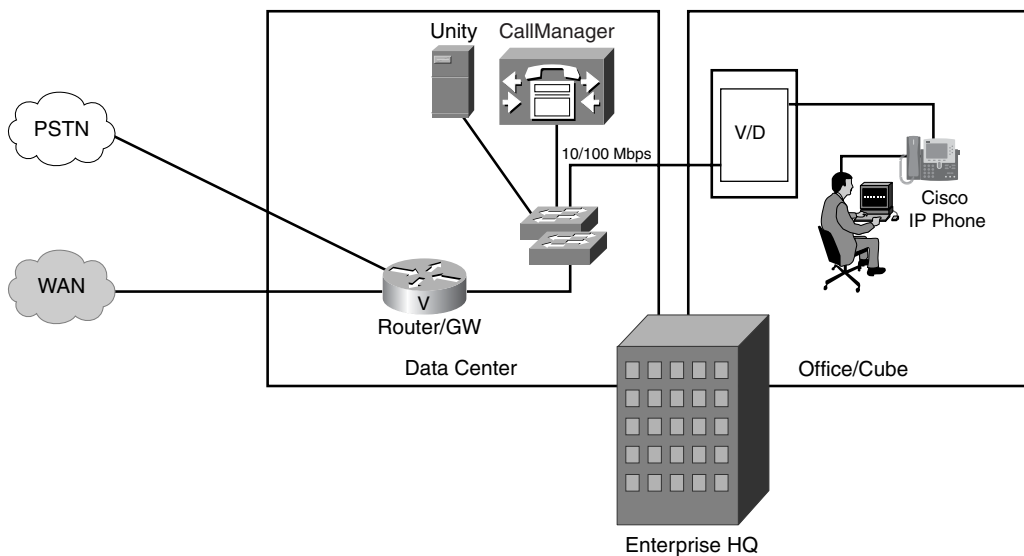
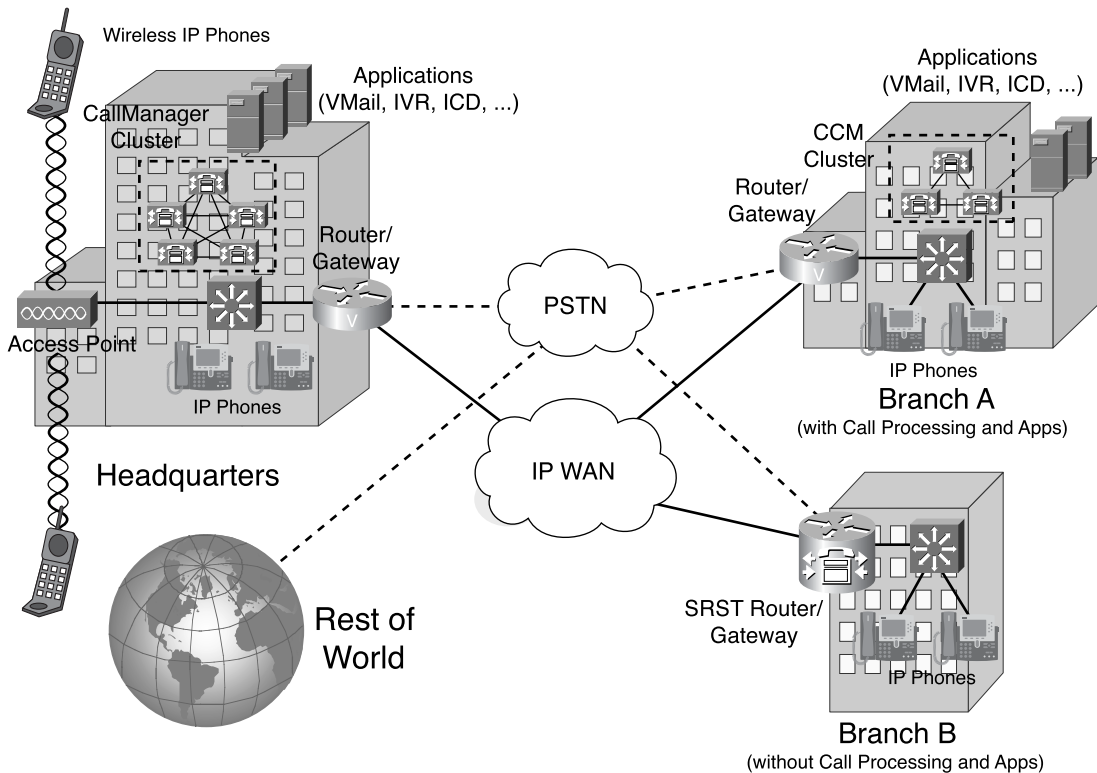


Figure 1-5 *End-to-End IPT Network*



Signaling and Transport Protocols

Now that you have a good understanding of the evolution of integrated voice and data networks, this section briefly discusses the concepts of different signaling and transport protocols used in IPT solutions.

Today, organizations use a PBX system or a key system as customer premises equipment (CPE) to provide voice services. Key systems are less expensive than PBX systems, but they typically support fewer users and do not have the rich functionality and feature sets available in PBX systems. If there are large numbers of users on the PBX system, it is not possible to forklift the PBX systems and replace them with IP-based call-processing servers. In these scenarios, the IPT solution should provide the integration with the existing PBX or key systems. Knowing the type of interfaces and signaling protocols supported on the PBX or key systems allows you to choose the right hardware and software components on the IPT solution so that the PBX or key systems can coexist with the IPT solution until migration to IPT is completed.

Telco Signaling Protocols

Conceptually, the signaling protocols that are used in the telco networks can be divided into three categories:

- **Subscriber-to-network signaling**—Used by end users to request the network to set up a call. The telephone companies (telcos) treat these interfaces as subscriber interfaces.
- **Intranetwork signaling**—Used between switches in the telco network to set up and tear down calls between telco switches.
- **Network-to-network signaling**—Used between two networks to set up and disconnect calls and to exchange billing and other related information. The types of network-to-network signaling are not new signaling types but rather are variants of the intranetwork signaling types.

Signaling is further divided into two types: analog and digital.

Analog Signaling

By definition, analog signals are sent over wires or through air and carry information through some combination of frequency, phase, and amplitude. You can find trunks that use analog signaling in small offices or in offices where the telco switch does not support digital signaling. Analog signaling types usually fall under the subscriber-to-network signaling category. The three common analog trunk types are loop start, ground start, and ear and mouth (E&M).

Loop-start and ground-start trunks use the same wire pair for both audio and signaling. Most of the telephone connections to households around the world use loop-start signaling. E&M uses separate wire pairs for audio and signaling. You can find E&M signaling trunks in older PBX/central office switches.

The telephone system usually uses dual-tone multifrequency (DTMF) or dial pulse/digit transmission methods to transmit the digits that the subscriber dials. DTMF, which is the most popular method, uses two simultaneous voice-band tones for dialing, such as touch-tones. Dial pulse, which is an older method, uses a series of make and brake pulses to represent digits. In pulse dialing, an off-hook state is represented by a make state of the pulse, and an on-hook state is represented by a break state of the pulse.

Digital Signaling

Analog trunks require a physical set of wires per trunk and thus might not be the best method when provisioning a large number of trunks. Hence, higher-density digital trunks are used in larger organizations that have higher call volumes. There are two varieties of digital signaling trunk types: T1 and E1 circuits. When a network supports voice on T1 and E1 circuits (also used for data transmission), two types of signaling mechanisms are used:

Channel-associated signaling (CAS)

Common channel signaling (CCS)

CAS falls into the subscriber-to-network and CCS into intranetwork signaling.

CAS

In CAS, signaling information is carried in-band. This means that actual voice conversation travels along with the signaling information on the same circuit. One example of a CAS signaling system is Robbed Bit Signaling (RBS). RBS gets its name from the nature of its operation, in which some of the bits from the payload in each time-division multiplexing (TDM) slot are robbed and reused for signaling.

In the E1 facility, the signaling bits are arranged in time slot 16. CAS on the E1 facility also uses R1 (MF) and R2 (MF Compelled) types of signaling methods.

CCS

CCS separates signaling information from user data. Two examples of protocols in which you can find CCS signaling are ISDN and Q.SIG.

ISDN permits telephone networks to carry data, voice, and other types of traffic. ISDN has two types of variants:

- **Basic Rate Interface (BRI)**—Composed of two B (bearer) channels (used to carry data and voice traffic) and one D (data) channel (used for signaling), referred to as 2B+D. Each B channel provides 64 kbps, and the D channel provides 16 kbps for signaling. Two B channels combined can provide 128 kbps of bandwidth. Although the signaling is in a separate channel, it travels along with data.
- **Primary Rate Interface (PRI)**—Composed of 23 B channels and one D channel (23B+D) when using a T1 facility, and 30 B channels and a single 64-kbps D channel (30B+D) when using an E1 facility. Each B channel is 64 kbps.

The other example signaling standard that uses CCS, Q.SIG, has many variations in its feature implementations. Q.SIG is used in many PBX systems and in PBX internetworking.

VoIP Protocols

This section provides a brief overview of the operation of VoIP protocols and explains how these protocols play a role in IPT networks.

Two types of VoIP protocols exist:

- Protocols that provide the call control and signaling
- Protocols that carry voice payload (RTP, RTCP, UDP, and IP)

The job of the call-control and signaling protocols is to set up and tear down the connection between two or more endpoints in a VoIP network. The following is a list of the call-control and signaling protocols commonly found in IPT networks:

- **H.323**—(peer-to-peer model)
- **Session Initiation Protocol (SIP)**—(peer-to-peer model)
- **Media Gateway Control Protocol (MGCP)**—(client/server model)
- **Skinnny Client Control Protocol (SCCP)**—(a lighter-weight Cisco proprietary protocol that uses the client/server model)

After the call setup process is complete, the source and destination endpoints can transmit and receive data by using the RTP/RTCP/IP/UDP protocol stack. A typical VoIP network uses any one or a combination of these protocols, depending on the endpoints involved. These protocols are needed at different points in an IPT network. As mentioned before, the gateway is an interface between the IP telephony network and the PSTN or a PBX. On one side, the gateway supports the signaling protocols needed to interface with the PSTN or a PBX. On the other side, the gateway supports the signaling and control protocols needed to interface with the IPT network via the CallManager. The CallManager also acts as a protocol translator. On one hand, the CallManager could be communicating with an IP phone using SCCP, and on the other hand, it could be communicating to the gateway using MGCP, H.323.

The following sections discuss briefly some basic functionality of the call control and signaling protocols that carry voice payload.

H.323

H.323 is an International Telecommunication Union (ITU) specification to carry real-time voice traffic such as telephone calls, video, and data over an IP network. The H.323 protocol specification describes how a session between two H.323 endpoints is created and maintained. The following are the main components of H.323:

- **H.225**—Scaled-down version of Q.931 to set up an IP connection between two H.323 endpoints.
- **H.245**—Allows H.323 endpoints to negotiate their capabilities (such as codecs available) with each other.
- **RAS**—H.323 endpoints use this protocol to communicate with H.323 gatekeepers to Manage Registration/Administration/Status.

The preceding three components use TCP for transport. The H.323 standard has gone through many revisions. The current standard is H.323 Version 4. Cisco CallManager 4.0 is compliant with H.323 Version 2 standards.

The “Call-Flow Scenarios” section later in this chapter discusses the call flow sequence between the IP phone and a voice gateway using the H.323 protocol.

SIP

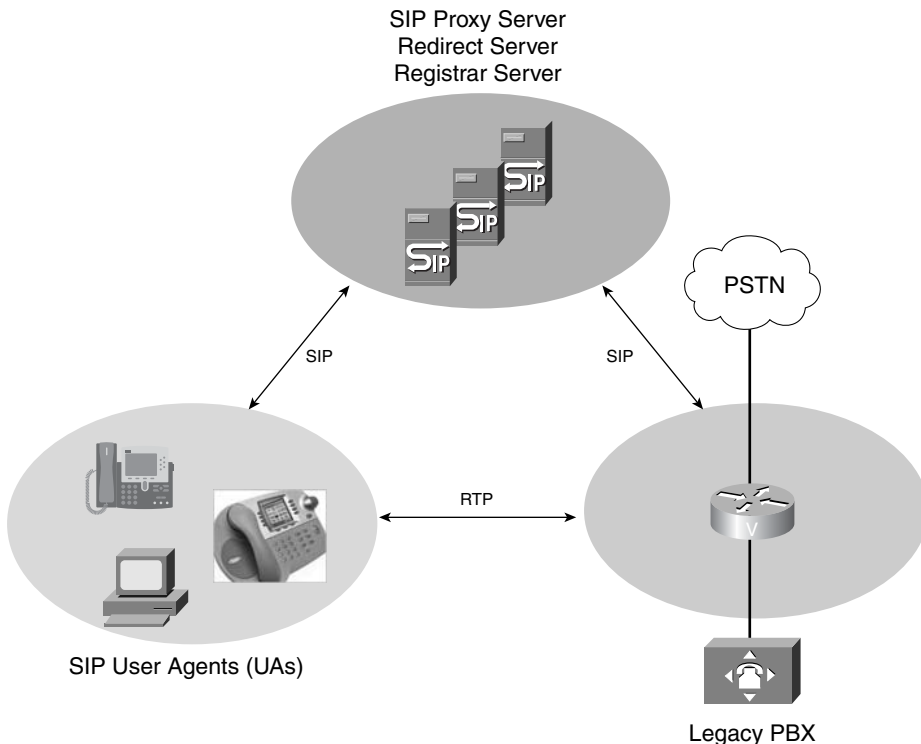
SIP is an RFC standard (RFC 3261) from the Internet Engineering Task Force (IETF), the body responsible for administering and developing the mechanisms that comprise the Internet. SIP is one of the most talked about protocols these days because of its wide interoperability with other products.

SIP is a peer-to-peer protocol. The peers in a session are called user agents (UAs). A user agent can function in one of the following roles:

- **User agent client (UAC)**—A client application that initiates the SIP request
- **User agent server (UAS)**—A server application that contacts the user when a SIP request is received and returns a response on behalf of the user

Typically, a SIP endpoint is capable of functioning as both a UAC and a UAS, but it functions only as one or the other per transaction. Whether the endpoint functions as a UAC or a UAS depends on the UA that initiated the request. From an architectural standpoint, the physical components of a SIP network can be grouped into two categories: clients (endpoints) and servers. Figure 1-6 shows the SIP architecture.

Figure 1-6 *SIP Architecture*



In Figure 1-6, the SIP clients are phones such as Cisco SIP phones (7960, 7940, and ATA-18x can be configured as SIP phones by loading SIP firmware) and SoftPhones that are loaded on the user's PC/laptop. The routing entities within the SIP architecture are called SIP servers. The following are the three types of SIP servers:

- **SIP proxy server**—An intermediate device that receives SIP requests from a client and then forwards the requests on the client's behalf. Basically, proxy servers receive SIP messages and forward them to the next SIP server in the network. Proxy servers can provide functions such as authentication, authorization, network access control, routing, reliable request retransmission, and security. The role of a SIP proxy server is similar to that of a gatekeeper in an H.323 network.
- **Redirect server**—Provides the client with information about the next hop or hops that a message should take, after which the client contacts the next hop server or UAS directly.
- **Registrar server**—Processes requests from UACs for registration of their current location. Registrar servers are often co-located with a redirect or proxy server.

SIP uses six main messages for its basic functionality:

- **Register message**—Sent by the UAs to tell the network where they can be located. The location could be one or more addresses.
- **Invite message**—Sent by a UA to initiate a session.
- **ACK message**—Used to acknowledge that a successful session has been initiated.
- **Bye message**—Used to terminate a session that is already in progress and established.
- **Cancel message**—Used to terminate a session that is not yet established (for example, phone is still ringing).
- **Options message**—Used for an out-of-band mechanism to determine the capabilities of another UA.

Users in the SIP network are identified by a unique SIP address such as an e-mail ID. Figure 1-7 shows the basic call setup diagram of a successful call when a SIP proxy server is present in the network.

Figure 1-7 SIP Call Flow Using SIP Proxy Server

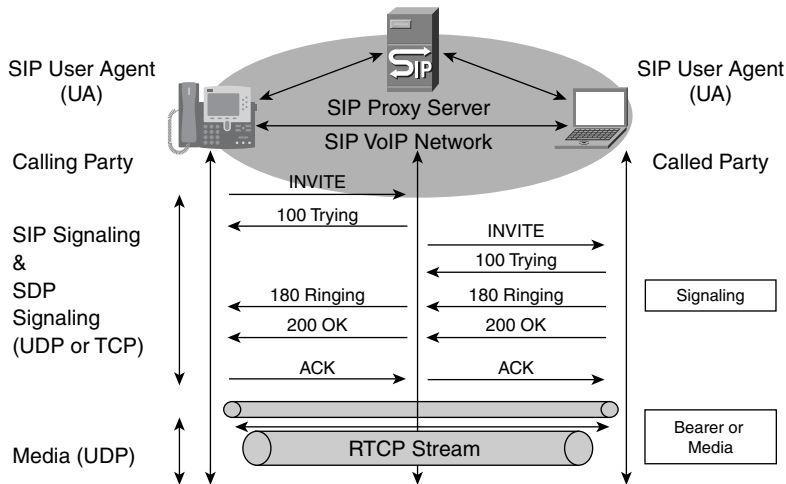


Figure 1-7 shows the following sequence of events:

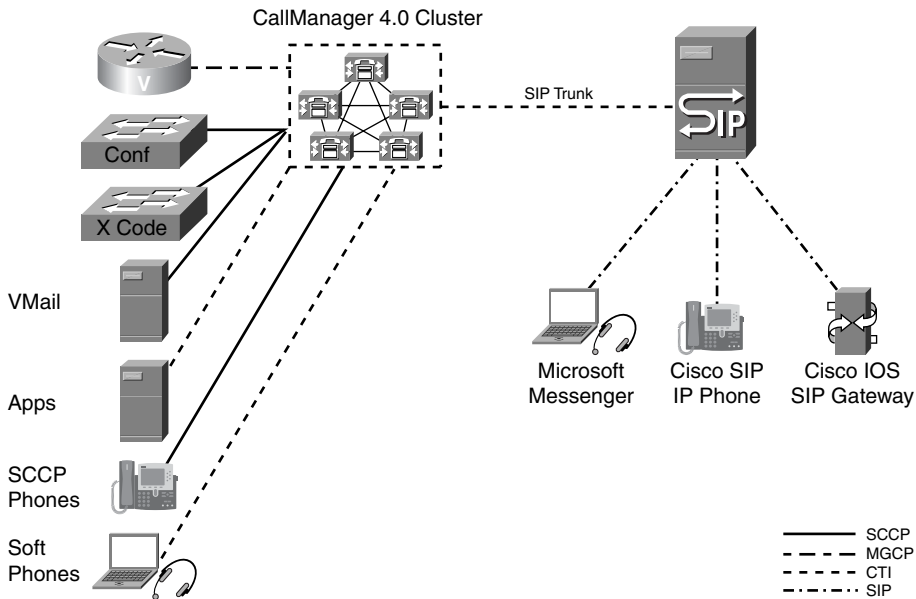
- 1 The calling party sends an Invite message to the called party.
- 2 The SIP proxy server responds to the calling party with the informational response “100 Trying.”
- 3 At the same time, the SIP proxy server sends an Invite message to the called party on behalf of the calling party.
- 4 The called party responds with two informational responses: “100 Trying” and then “180 Ringing.”
- 5 The SIP proxy server passes the informational response “180 Ringing” to the calling party.
- 6 The called party responds with the response “200 OK” if the call is successful.
- 7 The SIP proxy server passes the success response “200 OK” to the calling party.
- 8 The calling party sends an ACK message.
- 9 The SIP proxy server passes the ACK message to the called party.

After SIP successfully completes the signaling, a media path between the two endpoints is established.

Starting with CallManager 4.0, CallManager can communicate with SIP endpoints (SIP IP phones, SIP gateways) via SIP Proxy server. This feature, referred to as “SIP Trunk” and shown in Figure 1-8, allows any CallManager-controlled device to communicate with a SIP network.

Future releases of CallManager might include the direct support of SIP so that CallManager can talk to the SIP endpoints directly without the need for a SIP proxy server.

Figure 1-8 *SIP Support in CallManager*



MGCP

As previously discussed, H.323 and SIP are based on the peer-to-peer model, whereas MGCP is based on a client/server model. As defined in RFC 2705, “MGCP is designed as an internal protocol within a distributed system that appears to the outside as a single VoIP gateway.”

MGCP uses the Session Description Protocol (SDP, RFC 2327) to describe and negotiate media capabilities, which is also used in SIP. SDP functionality is similar to H.245 capability in H.323.

There are two main components of MGCP:

- **Media gateway (MG)**—Bridges networks that use different media types, such as circuit-switched, analog, and IP networks. An MG is also referred to as an endpoint (EP). An MG is an interface between a telephony network or a PBX and a VoIP network. Examples of Cisco media gateway products include 26xx/36xx/37xx series routers, Catalyst gateways such as WS-X-6608-T1/E1, and WS-6624-FXS gateways.

- **Media gateway controller (MGC)**—Controls the parts of the call state that relate to connection control for media channels in one or more media gateways. An MGC is also referred to as a call agent (CA) or as the industry term Softswitch. In the IPT networks, CallManager acts as a CA that provides call-processing functions and feature logic and controls the MG.

MGCP messages are sent over UDP/IP between the CA and MG. The client/server relationship is maintained between the CA and MG. Voice traffic (bearer channels) is carried over RTP/UDP/IP or other transmission media (e.g., ATM). MGCP is independent of transport media and can be used to control ATM or circuit-switched gateways.

Similar to H.323, MGCP has undergone several revisions. As of CallManager 4.0, support for MGCP 0.1 is included. The current revision of MGCP is 1.0.

MGCP uses very simple commands in the negotiation process between the MG and CA and uses UDP as a transport layer protocol. The default port is UDP 2427, although it is configurable in the CallManager. Examples of the commands are **CRCX (CreateConnection)**, **MDCX (ModifyConnection)**, etc., and every command requires an acknowledgement. The following list describes commonly used MGCP commands, and Figure 1-8 shows the usage of these commands:

- **CRCX**—The CA can use the **CreateConnection** command to create a connection that terminates in an endpoint inside the MG.
- **MDCX**—The CA can use the **ModifyConnection** command to change the parameters associated with a previously established connection.
- **DLCX**—The MG can also use the **DeleteConnection** command to delete an existing connection. The MG can also use the **DeleteConnection** command. This command indicates that a connection can no longer be sustained.
- **RQNT**—The CA can issue a **NotificationRequest** command to a gateway to instruct the gateway to watch for specific events such as hook actions or DTMF tones on a specified endpoint.
- **NTFY**—The MG can use the **Notify** command to inform the CA when the requested events occur.
- **AUEP and AUCX**—The CA can use the **AuditEndpoint** and **AuditConnection** commands to audit the status of an endpoint and any connections associated with it.
- **RSIP**—The MG can use the **RestartInProgress** command to notify the CA that the MG, or a group of endpoints managed by the MG, is being taken out of service or is being placed back in service.

Table 1-1 shows the directions of the signaling messages exchanged between the CA and the endpoint or MG.

Table 1-1 *MGCP Message Types and Flows*

MGCP Command Code	MGCP Command Verb	Direction of the Command Flow
Endpoint Configuration	EPCF	CA -> EP
Creation Connection	CRCX	CA -> EP
ModifyConnection	MDCX	CA -> EP
DeleteConnection	DLCX	CA <-> EP
Notification Request	RQNT	CA -> EP
Notify	NTFY	CA <- EP
AuditEndpoint	AUEP	CA -> EP
AuditConnection	AUCX	CA -> EP
RestartIn Progress	RSIP	CA <- EP

The “Call-Flow Scenarios” section later in this chapter discusses the call-flow sequence between the IP phone and a voice gateway using the MGCP protocol.

SCCP

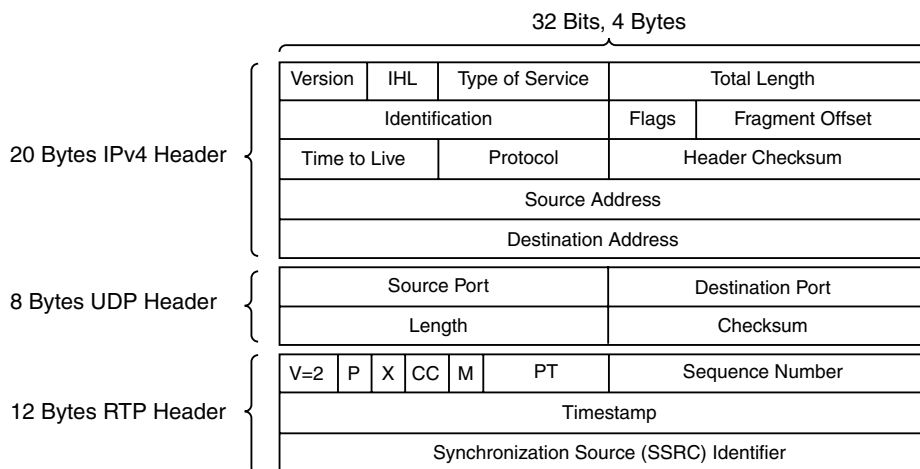
SCCP is a “lightweight” Cisco proprietary protocol that is based on a client/server model. In this model, all the intelligence is built into the server, which is a CallManager in the Cisco IPT solution. The client, which is a Cisco IP Phone, has minimal intelligence. In other words, the Cisco IP Phones have to do less work, thus requiring less memory and processing power. The CallManager, being the intelligent server, learns client capabilities, controls call establishment, clears calls, sends notify signals (i.e. message waiting indication (MWI), reacts to signals from the client (after the user presses the directory button on the phone), and so forth. CallManager communicates with the IP phones using SCCP and, if the call has to go through a gateway, communicates with the gateway using H.323 or MGCP.

RTP/RTCP

By now you should have a good operational understanding of signaling protocols such as H.323, SIP, MGCP, and SCCP. These protocols provide call-signaling and control functionality and are responsible for setting up and tearing down the connection between the endpoints. After the connection is set up between the two endpoints, the source and destination endpoints can transmit and receive data by using RTP/RTCP. As discussed in the “Next-Generation Multiservice Networks” section earlier in this chapter, RTP/RTCP uses UDP for transport.

Figure 1-9 shows the IP packet header information that transports the RTP/RTCP packets. As you can see, the IPv4 header is 20 bytes, the UDP header is 8 bytes, and the RTP header is 12 bytes, which means that a total of 40 bytes of header information is required to transport the single RTP packet. After this 40 bytes of IP header information, two 10-byte frames (10 bytes per frame for G.729 codec voice samples) of real voice payload are carried, for a total of 20 bytes of voice payload. (The Cisco implementation puts two frames into one packet.) A simple math calculation shows that the header has twice the number of bytes that are in the real payload. To address this particular issue, you can use RTP header compression technique on point-to-point links. You must apply the RTP header compression on a link-by-link basis. When enabled on a gateway, you can use the RTP header compression technique compresses the 40-byte header into 2 or 4 bytes. However, enabling compression increases the load of the CPU on the router. You need to make a decision based on the number of calls that you need to send out through that gateway.

Figure 1-9 RTP, UDP, and IP Protocol Headers



IP Telephony Components

So far this chapter has focused on analyzing how legacy networks are migrating to integrated voice and data networks and on describing the various protocols used in the new multiservice networks. This section discusses the main components of Cisco AVVID and some of the key areas to look for when deploying the Cisco IPT solution. Key areas include the following:

- Network infrastructure
- Call processing

- CallManager Directory Services
- IPT endpoints
- Call admission control
- Fax
- Media resources
- Applications

Understanding the features and capabilities of these components will help you to design the network that meets the targeted organization's requirements.

Network Infrastructure

Network infrastructure plays a key role in building multiservice networks such as Cisco AVVID. Integration of data and voice traffic puts strong requirements on packet loss, delay, and jitter (variable delay). When designing IPT networks, you should choose network infrastructure components in the LAN and WAN that support QoS mechanisms, in addition to faster convergence in case of network failures to avoid the delay, jitter, and so forth.

The addition of voice traffic on top of the existing data traffic increases the bandwidth requirements in both LANs and WANs. The bandwidth within the LAN is not a challenging issue because of the availability of the high-speed LAN switching technologies. However, when transporting the voice traffic across the WAN links, you need to ensure that adequate bandwidth is available to support the additional bandwidth required to transport voice calls. If the WAN links do not have adequate bandwidth, you need to increase their bandwidth to support the additional voice traffic. After the bandwidth is available, you can use QoS mechanisms to prioritize the voice traffic and reserve the bandwidth.

Chapter 4, "Planning Phase," discusses the infrastructure requirement analysis in depth.

Call Processing

CallManager software is the main component of the Cisco IPT solution. CallManager handles all the call-processing requests received from various clients in the IPT network. CallManager software runs on the Microsoft Windows 2000 Server/Windows 2000 Advanced Server operating systems.

CallManager is installed on the Cisco Media Convergence Server (MCS). The selection of the hardware platforms depends on the size of the network in which they are going to be deployed, including its high-availability and performance requirements. Table 1-2 lists the maximum number of devices supported per server platform.

Table 1-2 *Maximum Number of Devices per Server Platform*

Server Platform	Maximum Number of Devices per Server
Cisco MCS-7845	7500
Cisco MCS-7835	2500
Cisco MCS-7825	1000
Cisco MCS-7815	300

CallManager Clustering

CallManager servers are grouped to form clusters to support more devices (IP phones, gateways, and so forth). Starting with CallManager Version 3.3, a CallManager cluster can have up to eight CallManager servers running the CallManager service.

In addition to eight call-processing servers, the cluster can have servers such as a publisher server, a Trivial File Transfer Protocol (TFTP) server, and a Music on Hold (MoH) server. A publisher server has the read/write database of Microsoft SQL that stores the CallManager configuration information. There can be only one publisher server in a cluster. All other servers in the cluster, referred to as subscribers, have the read-only database. Subscribers pull their up-to-date subscriptions from the publisher server. During normal operating conditions, when the publisher server is available, the subscriber database is not used.

If a publisher is offline, you cannot perform updates such as adding new devices, changing user passwords, speed dials, or any other features that require a write operation on the database, because it is the only server that has the read-write database. However, the phones and other devices will continue to function normally.

CallManager stores the configuration of the IP phones in the TFTP server. (The default is to store it in the memory. You can change this default by modifying the service parameters. Chapter 9, “Operations and Optimization,” discusses these techniques.) The configuration information is stored in the XML format. The configuration file contains information such as device pool associations, directory URLs, authentication URLs, language-specific information, and so forth. IP phones and many other endpoints in the Cisco IPT network download the firmware and configuration information from the TFTP server.

Failure of a TFTP server is not an issue for the devices that were already configured and functioning before the failure. The devices store the previously loaded configuration and firmware in memory and use the same if they fail to contact the TFTP server during the reboot. However, an update to a phone’s configuration information that is stored in the TFTP configuration file will fail if the TFTP server is unavailable. In addition, provisioning of new devices fails if a TFTP server is not available.

For networks that require high availability, you can deploy two TFTP servers to provide redundancy and load balancing in the network. Cisco IP Phones and other Cisco IPT endpoints

receive the TFTP server information via the DHCP server in the custom option 150. You can configure an array of IP addresses for option 150 in the DHCP server, instead of one IP address, to communicate to the Cisco IPT endpoints the existence of the secondary TFTP server.

TIP

In a large IPT deployment, the recommendation is to have a dedicated publisher server that does not participate in the call processing and a separate server that provides TFTP services.

Device Weights

The devices in the IPT network consume different amounts of memory and CPU resources on the CallManager servers. Based on the amount of resource consumption, Cisco has assigned a weight to each device, as shown in Table 1-3. This information is based on CallManager Version 3.3.(3).

Table 1-3 *Base Device Weights*

Device Type	Weight per Session/ Voice Channel	Session/DS0 per Device	Cumulative Device Weight
IP phone	1	1	1
Analog MGCP ports	3	Varies	3 per DS0
Analog SCCP ports	1	Varies	1 per DS0
CTI route point	2	Varies	Varies ¹
CTI client port	2	1	2
CTI server port	2	1	2
CTI third-party control ²	3	1	3
CTI agent phone ²	6	1	6
H.323 client	3	Varies	3 per call
Intercluster trunk gateway	3	Varies	3 per call
H.323 gateway	3	Varies	3 per call
Digital MGCP T1 gateway ports	3	24	72 per T1
Digital MGCP E1 gateway ports	3	30	90 per E1
MoH stream	10	20	200 ³
Transcoding resource	3	Varies	3 per session

Table 1-3 *Base Device Weights (Continued)*

Device Type	Weight per Session/ Voice Channel	Session/DS0 per Device	Cumulative Device Weight
Media Termination Point (MTP) (software)	3	24	72 ⁴
Conference resource (hardware)	3	Varies	3 per session
Conference resource (software)	3	24	72 ⁴

1. Cumulative weight of the CTI (Computer Telephony Integration) route point depends on the associated CT ports used by the application.
2. Includes the associated IP phone.
3. When MoH is installed on the same server as CallManager, the maximum number of media streams is 20.
4. When installed on the same server as CallManager, the maximum number of conference sessions is 24.

The devices that are registered with CallManager consume additional server resources during transactions, which are in the form of calls. A device that makes only 6 calls per hour consumes fewer resources than a device that makes 12 calls per hour. The device weights that are assigned to the devices in Table 1-3 are based on the assumption that the device makes 6 or fewer calls during the busy hour call attempts (BHCA).

BHCA is the number of call attempts made during the busiest hour of the day. Before deploying a Cisco IPT solution, you must determine the busiest hour of the day for an organization and then scale the type of devices that are going to be deployed within the Cisco IPT solution. The BHCA varies from organization to organization and depends on the type of business (which can vary by season) and on the sales/promotional periods. A thorough network audit or analysis of historical call detail records is required to determine an organization's BHCA.

Each device that requires more than six BHCA has a multiplier applied to its base weight. Based on the BHCA multiplier table, Table 1-4, if an IP phone is making 16 BHCA, its multiplier is 3. The total weight of the IP phone with 16 BHCA is equal to its base weight 1 (refer to Table 1-3) multiplied by 3. The multiplier is applied only to station/client devices and not to devices that are a media resource or gateway.

Table 1-4 *BHCA Multiplier*

BHCA	0–6 BHCA	7–12 BHCA	13–18 BHCA	19–24 BHCA	25–30 BHCA
Multiplier	1	2	3	4	5
Example IP phone	1	2	3	4	5
Example CTI client port	2	4	6	8	10

The total number of device units that a single CallManager can control depends on the server platform. Table 1-2 gives the details of the maximum number of devices per platform based on CallManager Version 4.0. You have to deploy multiple CallManager clusters if the number of IP phones plus other devices exceeds the device weights limit supported by a single cluster.

TIP

In Table 1-2, the number provided in the Maximum Number of IP Phones per Server column is based on the assumption that all phones are configured with a single directory number. If the network that you are deploying is complex and involves multiple lines/directory numbers per IP phone or dial plan that includes numerous route patterns and translational patterns, you have to understand the concept of dial plan weights, as discussed in the following section.

Dial Plan Weights

Device weights determine the maximum number of physical devices that can be registered to a CallManager subscriber. Some IP phone models support multiple lines (directory numbers or line appearances). Many IPT deployments have directory numbers that are shared across multiple IP phones and a large number of dial plan entries that include route patterns; translational patterns require an extra amount of resources (CPU, memory) on the CallManager.

Dial plan weights provide the limit on the number of such dial plan entries configured in a CallManager subscriber. Dial plan weight calculations provide guidelines to size the cluster. Two types of dial plan weights are available:

- Subscriber dial plan weights (include line appearances)
- Global dial plan weights (include route patterns and translational patterns)

In larger IPT deployments, you should register all the endpoints to the subscribers and none to the publisher server. That way, you can prevent the publisher server from doing call-processing activity. Subscriber dial plan weights consist of the following main types:

- **IP phone weight**—Associated with the subscriber server to which the IP phone is normally registered. This weight is for the base device. The dial plan weight of an IP phone is independent of its device weight. (See Table 1-3.)
- **Line weight (unique or shared appearance)**—Associated with the subscriber server to which the device is normally registered.
- **Reachability weight**—Associated with all other subscribers in the cluster that have to be able to reach (call) a given line. Consider a CallManager cluster with two CallManager servers: CCM1 and CCM2. An IP phone ‘A’ is registered to CCM1. Even though the IP phone is registered to CCM1, the CCM2, which is part of the same cluster, needs to know how to reach the phone ‘A.’ CCM2 keeps this information in the memory. *Reachability Weight* accounts for this memory utilization on CCM2.
- **Global dial plan weights**—Consist of route pattern and translation pattern weights.

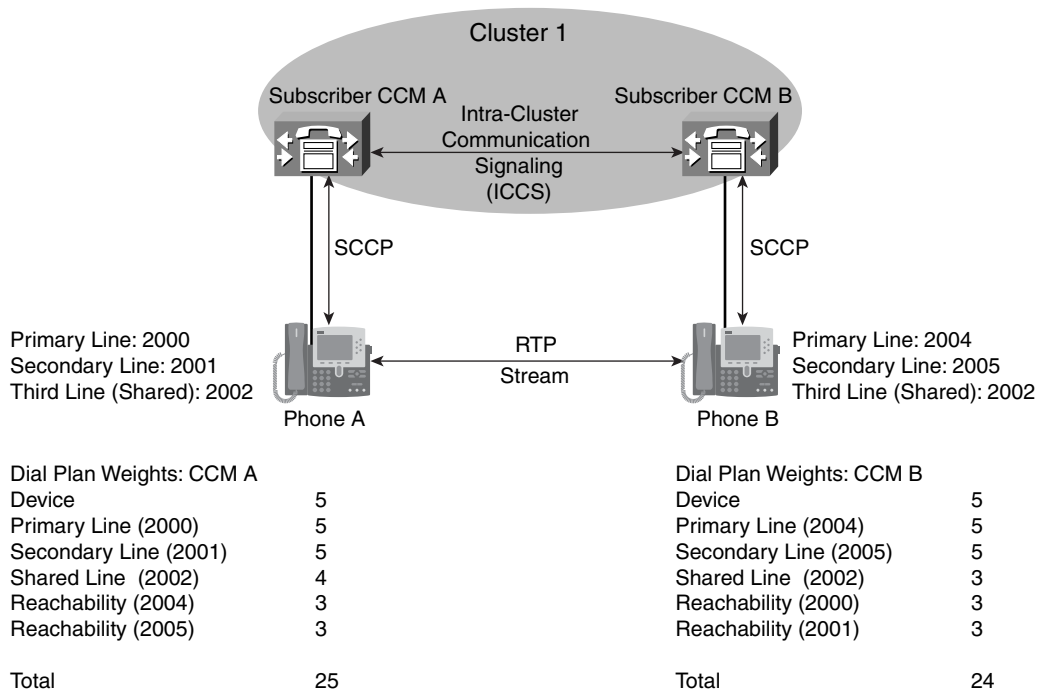
In summary, dial plan components contribute the weights outlined in Table 1-5.

Table 1-5 *Base Dial Plan Weights*

Subscriber Dial Plan Components	Dial Plan Weight
IP phone device (excluding line appearances)	5
Unique line appearance	5
Shared line appearance	4
Reachability per line appearance	3
Global Dial Plan Components	
Route pattern	2
Translational pattern	1

To understand more about the dial plan weight calculations, consider Figure 1-10. When IP phone A (primary extension 2000), which is a unique line appearance, is registered with subscriber CCM A, the dial plan weight on subscriber CCM A is 10 units (5 units for the IP phone and 5 units for the unique line appearance (primary extension 2000)). Subscriber CCM B in cluster 1 has a dial plan reachability weight of 3 units to reach extension 2000 on subscriber CCM A.

Figure 1-10 *Dial Plan Weight Calculations*



The secondary unique line appearance on IP phone A (secondary extension 2001) adds a dial plan weight of 5 units to subscriber CCM A and 3 units to subscriber CCM B located in cluster 1. Each shared line appearance (shared extension 2002) on IP phone A adds a dial plan weight of 4 units to subscriber CCM A and 3 units to subscriber CCM B located in cluster 1. A line appearance is called “shared” when the same unique line appears on multiple devices in the same partition.

Figure 1-10 also shows IP phone B with primary extension 2004, secondary extension 2005, and shared extension 2002, registered with subscriber CCM B in cluster 1. Note that shared extension 2002 has a dial plan weight of 4 units on subscriber CCM A and 3 units on subscriber CCM B, since the shared extension 2002 is primarily controlled by subscriber CCM A, thus requiring more resources.

In each cluster, the global dial plan weights apply to all subscriber servers. For example, a route pattern of 9.1xxxxxxxxxxx adds a dial plan weight of 2 units to each subscriber server in the cluster (refer to Table 1-5).

Table 1-6 lists guidelines for how much physical memory to install on a subscriber server, based on the number of phones, number of line appearances, and complexity of the dial plan that is configured on that server.

Table 1-6 *Server Memory Requirements for Dial Plan Weights*

Total Dial Plan Weight on a Subscriber	Server Memory Requirements
Up to 15,000	512 MB of RAM
Up to 35,000	768 MB of RAM
Up to 70,000	1 GB of RAM
Up to 140,000	2 GB of RAM
Up to 220,000	4 GB of RAM

TIP When determining the server hardware and number of servers in the cluster, you should choose a server based on the size of the network, performance, and high-availability requirements. A properly sized cluster must satisfy both the device weight and dial plan weight requirements.

Starting with CallManager 4.0, Cisco has introduced a Cisco CallManager Capacity Tool to size the CallManager clusters. This is a web-based tool and is currently not available on Cisco Connection Online (CCO). In the back end, the tool uses device weights, dial plan weights, and the BHCA multipliers concept to calculate cluster sizing. The device weights and BHCA factors could change from one version of CallManager to another, but the concept remains the same.

CallManager Directory Services

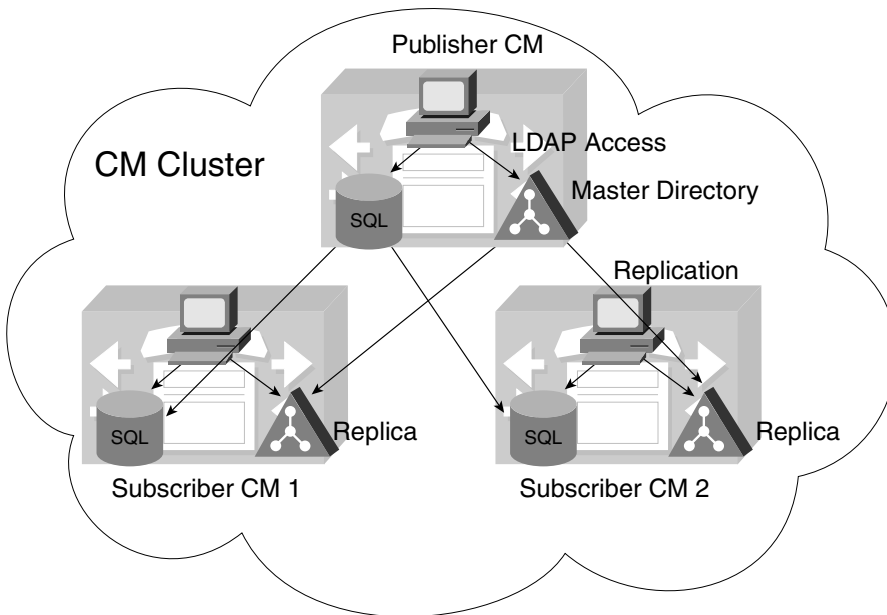
CallManager is bundled with a Lightweight Directory Access Protocol (LDAP) compliant directory called DC Directory (DCD). DCD is a Cisco OEM product from Data Connection Limited.

CallManager stores system and device configurations in a Microsoft SQL database. The application scripts and the following information are stored in DCD:

- User authentication and authorization
- Extension Mobility profiles
- Personal Assistant profiles
- Internationalization information
- Personal Address Book (PAB)
- Spoken name
- Fast dial
- Call Forward All information

The DCD process replicates the information among the members of the cluster, as shown in Figure 1-11. This process is similar to Microsoft SQL replication.

Figure 1-11 DC Directory Replication Within a Cluster



Many organizations have already deployed LDAP-based directories to store the user-related information, such as user ID, password, authentication information, authorization information, e-mail ID, phone number, and address. There are two possible deployment scenarios for the CallManager directory:

- Use the embedded DCD, which is part of CallManager
- Use corporate directory integration, which allows CallManager to store the user-related information in a centralized, existing directory, instead of using DCD. CallManager supports the directory integration with Microsoft Active Directory 2000/2003, Netscape 4.x, iPlanet 4.x, or SunOne 5.x Server.

You do not need to perform additional planning or design tasks when using the embedded DCD. The publisher server stores the master copy of the directory database, and the subscribers have the replica of the publisher server's directory database.

However, if you are considering integration of CallManager with an existing corporate directory, you must take extra care to achieve successful integration and functioning of the CallManager cluster. Corporate directory integration requires schema extensions to the existing corporate directory schema structure. The schema extension creates new objects and attributes in the existing corporate directory schema structure to store CallManager-specific information in the directory. The CallManager schema extensions use official object identifiers (OIDs) that are approved by the Internet Assigned Numbers Authority (IANA).

Many other Cisco IPT applications, such as Cisco Unity, IPCC Express, Personal Assistant (PA), and Cisco Emergency Responder (CER), support directory integration with external directories. Cisco Unity requires a special set of schema extensions when integrated with an external directory, and other applications create special directory trees and attributes in the corporate directory.

NOTE

The IPT planning team must consult the corporate directory team to discuss the effects of this schema extension and to determine the effects of the extra size of the directory database because of the addition of new objects and attributes. Note that the directory schema extension process requires higher user privileges.

CallManager integration with the corporate directory includes the following benefits:

- You do not need to maintain two separate directories (one for the corporate directory and another for the CallManager directory), which results in minimal administration overhead
- When deploying multiple CallManager clusters, you do not need to provide different services to look up users in different clusters.
- Moves, adds, and changes are centralized.

IP Telephony Endpoints

In a Cisco IPT network, endpoints are the devices that accept or initiate a VoIP session. This section introduces the following endpoints that are used in a Cisco IPT network.

- Cisco IP Phones
- SoftPhones
- Wireless IP Phones
- Voice gateways
- Survivable Remote Site Telephony (SRST)
- CallManager Express (CME)

Cisco IP Phones

IP phones are one of the endpoints in Cisco AVVID. Various IP phone models are available, the selection of which depends on the end-user requirements and the overall budget for the project. Appendix A, “IP Phone Models and Selection Criteria,” provides a list of currently available IP phone models and selection criteria.

IP phones keep the connection to the primary and standby CallManager servers. CallManager redundancy groups (device pools) that are configured on the CallManager administration page provide this feature. Each CallManager redundancy group consists of more than one CallManager. The first CallManager listed in the CallManager redundancy group has the highest priority. IP phones attempt to register with the higher priority CallManager.

Just like any other networking device, IP phones require an IP address, subnet mask, default gateway, DNS server, and TFTP server information to communicate with CallManager. By default, IP phones are configured to obtain the IP address and the other network settings via the Dynamic Host Configuration Protocol (DHCP). This allows mobility and improves IP address manageability. The only downside is that critical IP address allocation information for many nodes is stored within one file or database on the DHCP server. You should have adequate support for DHCP services and treat the DHCP data as highly critical data.

TIP

Best practice is to keep the DHCP databases mirrored or backed up on a continual basis. In addition, have a plan in case DHCP services fail. In large deployments, separate the DHCP and TFTP server functionality to achieve stability and reliability.

If an organization has an existing DHCP server, it can extend the services to IPT endpoints, such as IP Phones. The only requirement is that the DHCP servers should also support adding custom

option 150 or 66 for IP phone provisioning. The DHCP server uses one of these option fields to forward to the IP phones information about the TFTP server or array of TFTP servers.

Only option 150 supports specifying an array of IP addresses. Hence, if you are planning to use more than one TFTP server, you should use option 150. Specifying more than one TFTP server allows the endpoints to use the secondary server if the primary server fails. Also, you can achieve load balancing by configuring these TFTP servers in different orders in the DHCP scopes.

The DHCP and TFTP services can be collocated on the CallManager publisher server in a small IPT deployment. However, for larger deployments, separating these services from the publisher server provides greater performance.

TIP

To build a standalone TFTP server, you simply need to install the CallManager software, as you would do with any other subscriber, but activate only the TFTP and DataBase Layer (DBL) monitor services on that server.

Domain Name Service (DNS) is not mandatory in IPT environments. IP phones can use IP addresses to communicate with CallManager. However, DNS is useful for managing the overall network environment and provides redundancy/load balancing for the IP phones that require access to the application servers.

SoftPhones

SoftPhones are software-based applications that turn your computer into a full-featured Cisco IP Phone, allowing you to place, receive, and otherwise handle calls. These types of applications are useful for telecommuters or users who move within the campus. With the wireless connectivity to the PC, users can freely move to any location within the reach of the wireless and thus carry the phone with them.

Two types of soft phone applications are available:

- Cisco IP SoftPhone
- Cisco IP Communicator

Cisco IP SoftPhone is a Telephony Application Programming Interface (TAPI) application that communicates with CallManager via the Computer Telephony Interface (CTI), whereas Cisco IP Communicator communicates with CallManager via SCCP. The user interface for the Communicator phone looks like a Cisco 7970G IP Phone.

Table 1-7 lists the major differences between Cisco IP SoftPhone and Cisco IP Communicator.

Table 1-7 *Differences Between Two Cisco SoftPhone Products*

Feature	Cisco IP SoftPhone	Cisco IP Communicator
User interface	PC application look and feel	Cisco IP Phone 7970G look and feel
Communication protocol with CallManager	CTI	SCCP
Provisioning	Requires creation of CTI port and user association	Just like any other Cisco IP phone
Call-control features	Features are limited to the capability of CTI APIs	All features supported in the 7970G Phone, such as multiple lines and access to Cisco IP Phone services, are supported

As Table 1-7 indicates, Cisco IP SoftPhone uses CTI to communicate with CallManager. When deploying Cisco IP SoftPhone, you need to note the limitations on the number of CTI devices that can be provisioned on the CallManager depending on the hardware platform. Table 1-8 shows the CTI device limitations for CallManager 4.0 and assumes that the Cisco IP SoftPhones are configured with one line appearance, and no more than six BHCAs are made from the Cisco IP SoftPhones.

The maximum CTI limits are shown in Table 1-8 and include any other provisioned CTI devices such as IP-IVR or third-party CTI-enabled applications.

Table 1-8 *CTI Device Limitations on CallManager*

Hardware Platform	Number of CTI Devices per Server	Number of CTI Devices per Cluster
MCS-7825, MCS-7835	800	3200
MCS-7845	2500	10,000

Because Cisco IP Communicator uses SCCP, it is treated like any other Cisco IP Phone; hence, you can deploy Cisco IP Communicator phones up to the maximum allowed IP phone device limits per server.

Both Cisco IP SoftPhone and Cisco IP Communicator mark the voice and signaling packets (0xB8/EF for media and 0x60/CS3 for signaling). These applications run on the user's laptop/PC connected to the PC port that is on the back of the IP Phone. Because the packets coming from the PC port on the IP phone are not trusted, when deploying these applications, you need to create the access lists on the access or distribution switches to identify and mark with proper Differentiated Services Code Point (DSCP) values the signaling and media packets coming from these applications. Chapter 4 discusses the QoS and markings in detail.

Wireless IP Phones

Cisco Wireless IP Phone 7920 works in conjunction with CallManager and Cisco Aironet 1200, 1100, and 350 Series Wi-Fi (IEEE 802.11b) access points.

The planning procedures for deploying wireless voice are different from those used to deploy wired IP phones. Wireless IP phone deployment involves the following major tasks:

- Preparing a site survey to do the following:
 - Determine the location of the access points
 - Identify and eliminate the sources of interference
 - Determine the power levels of the access points
 - Identify and eliminate the rogue access points
- Determining the number of access points required
- Configuring QoS policy on access points
- Configuring security

Voice Gateways

Voice gateways connect the IPT network to the PSTN or a PBX. CallManager supports a variety of voice gateways. Selection of the gateway depends on the specific site requirements. Geographical placement of the voice gateways determines the type of interfaces and link layer protocol selection.

CallManager communicates with gateways using any of the following protocols:

- MGCP
- H.323
- SIP

MGCP-based gateways provide call survivability and do not require a local dial plan. All the dial plan configurations are required to be made on the CallManager, whereas with H.323 gateways, you need to configure the local dial plan on the router by configuring the voice dial peers.

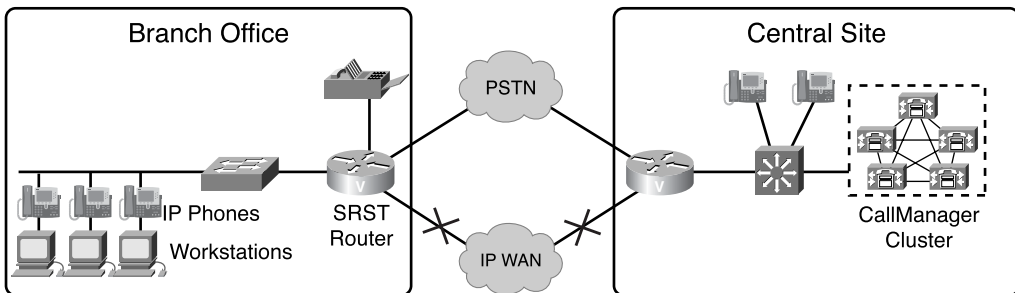
Cisco offers a variety of voice gateways, which are essentially the routers and switch modules with interfaces that can connect to the PSTN or a PBX. These routers and switch modules support two types of signaling interfaces: analog and digital. Analog signaling interfaces use Foreign eXchange Office (FXO), Foreign eXchange Station (FXS), and E&M signaling protocols. Digital signaling interfaces use T1/E1 Primary Rate Interface (PRI), ISDN Basic Rate Interface (BRI), or T1 CAS. Most of the Cisco IOS voice gateways support H.323, MGCP, and SIP, whereas the majority of the Catalyst voice gateways support MGCP.

Survivable Remote Site Telephony

Survivable Remote Site Telephony (SRST) provides the fallback support for the IP phones that are connected behind a router running the Cisco IOS software version that supports SRST. This feature enables you to deploy the IPT at small branch offices with a centralized call-processing model. Figure 1-12 depicts a branch office deployment with SRST.

During normal operation, when the CallManager is active and the WAN link is available, IP phones at the branch behave the same way as the IP phones at the central site. The SRST feature on the router becomes active as soon as the IP Phones detect the failure of the WAN link. (The IP Phones miss three consecutive acknowledgements from the CallManager.) The IP phones attempt to register with the other CallManagers in the redundancy group before attempting the registration with the SRST router. So, the fallback process to the SRST router could take longer if other CallManagers are in the IP phone's redundancy group. SRST provides the basic call handling and minimal features to the IP phones during the WAN failure. Without this feature, the IP phone users at these locations would not be able to make outside calls.

Figure 1-12 *SRST Operation in a Branch Office*



When the WAN link comes back online, IP phones detect the keep-alive acknowledgements from the CallManager and attempt to re-home back to the CallManager servers.

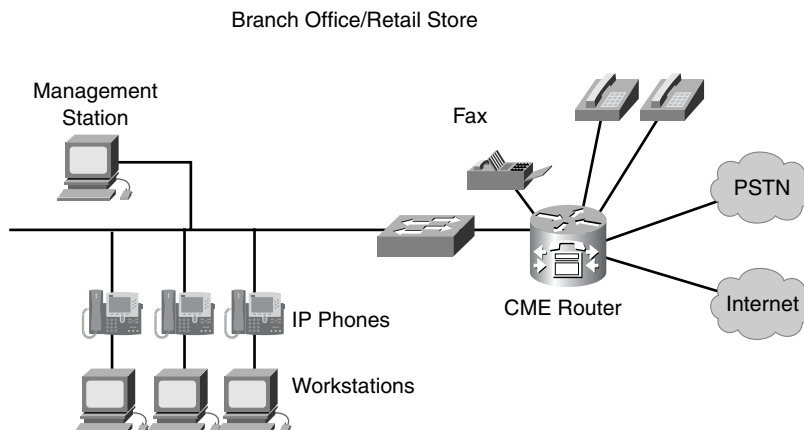
The number of IP phones supported in the SRST mode depends on the router platform, the Cisco IOS version, and the amount of memory. You have to choose the appropriate router model and amount of memory based on the number of phones being deployed at the branch office.

Cisco CallManager Express

Cisco CallManager Express (CME) is the new name given to the feature formerly known as IOS Telephony Services (ITS) on the Cisco IOS routers. CME is a licensed feature of Cisco IOS software that is available on many router hardware platforms. CME delivers key system functionality for small and midsize branch offices. In the CME solution, IP phones are registered to the CME router all the time. As shown in Figure 1-13, for a branch office/retail store that operates independently, the CME-based solution provides flexibility. Like SRST, the number of phones supported by

the CME gateway depends on the router hardware, the Cisco IOS version, and the amount of memory.

Figure 1-13 *CME Operation in a Branch Office*



Call Admission Control

In VoIP networks, CAC does the bandwidth management. CAC ensures that enough bandwidth is available before granting permission to a gateway for placing the call across the IP WAN. When deploying IPT solutions with multiple locations, you have two choices for implementing the CAC:

- CallManager locations-based CAC
- Gatekeeper CAC

CallManager Locations-Based CAC

CallManager locations-based CAC is one mechanism to limit the calls sent across an IP WAN in a single CallManager cluster deployment. Locations are configured in the CallManager and assigned a maximum bandwidth. The bandwidth assigned per location depends on the number of calls that are allowed to be made to a particular location and the type of codec used for that location. Before placing a new call, CallManager checks its location tables to determine if enough bandwidth is available to place the new call. If enough is available, the call is allowed and CallManager updates the available bandwidth for that location. Locations-based CAC is ideal for centralized call-processing deployments with a hub-and-spoke topology.

CallManager locations-based CAC is not scalable for multicluster CallManager deployments; gatekeeper CAC, discussed next, is recommended for such deployments.

Gatekeeper CAC

A Cisco IOS gatekeeper in Cisco AVVID networks provides call admission and call routing between the CallManager clusters in distributed call processing deployments. Gatekeeper CAC is suited for deployments that follow the hub-and-spoke topology and does not work with the meshed topologies. The following are some of the advantages of using the gatekeeper:

- It simplifies the dial plan management by enabling you to quickly add or remove routes and devices.
- It provides CAC between calls from different clusters, ensuring that the WAN bandwidth allocation is strictly enforced.
- It reduces configuration overhead by eliminating the need to configure a separate H.323 device for each remote CallManager that is connected to the IP WAN.
- It offers a choice of protocols for communicating with CallManager or H.225 gateways.
- It can perform basic call routing in addition to call admission control.

You have two choices of deploying a gatekeeper with CAC:

- Gatekeepers deployed with the Hot Standby Router Protocol (HSRP)
- Gatekeeper clustering

Gatekeepers in HSRP mode do not share the CAC information, whereas gatekeeper clustering enables true redundancy and load balancing. Gatekeepers that are deployed in a cluster mode exchange the CAC information via the gatekeeper Update Protocol (GUP) and are the recommended deployment method.

Fax

One of the most important pieces in the transition to converged networks is support for fax communication. As network implementations increasingly provide for e-mail attachments and web-downloadable documents, fax communication nonetheless is still a significant method of immediate document delivery worldwide. Studies have shown that a large portion of long-distance minutes is fax traffic.

The frequent use and customer expectations of fax functionality and reliability demand a support for reliable fax transmissions across a converged network. Most Cisco voice gateways currently support three methods to transmit fax traffic across the IP network:

- **Fax Pass-Through**—In Fax Pass-Through mode, the gateways do not distinguish a fax call from a voice call
- **Cisco Fax Relay**—In Cisco Fax Relay mode, the gateways terminate the T.30 fax signaling.
- **T.38 Fax Relay**—This standard provides standards-based Fax Relay.

Fax Relay mode is the preferred method to transmit fax traffic. Because the T.38 Fax Relay protocol is standards-based, fax gateways that use this protocol can interoperate with third-party T.38-enabled gateways and gatekeepers in a mixed-vendor network. As of CallManager 4.0, T.38 Fax Relay is not supported. When deploying the fax over IP by using the CallManager, Cisco Fax Relay or Fax Pass-Through are the only choices that you can use on the gateways.

Similar to voice traffic, fax traffic is also sensitive to delay, jitter (variable delay), and packet loss. Hence, the network must be QoS enabled.

Media Resources

The function of media resource devices is to mix the multiple streams into a single output stream, converting the data stream from one compression type to another, and so forth. Examples of media resources are conferencing, transcoding, and MoH.

The media resources can be hardware or software. CallManager has built-in software media resources for conferencing, transcoding, and media termination. The limitation of software media resources is that they can't combine the streams that use different compression techniques.

Hardware media resources have the same features as software media resources with an additional advantage of mixing the streams that use different compression types. Hardware media resources offer good performance and quality because the processing is done in the hardware.

MoH is another example of a media resource. MoH is an application that is installed by default on the CallManager servers (or you can install a standalone MoH server on a dedicated server for large deployments). As the name implies, MoH provides music or announcements when the users are put on hold.

When you are designing the IPT network, one of the tasks is to size the media resources and determine their placement within the network.

Applications

Cisco has a wide range of applications that can be deployed in an IPT network. These applications are optional, and their deployment adds more features and capabilities to the overall IPT network. Design and deployment of the applications, such as CRS and IP phone services, are discussed in Chapters 6, "Design of Call Processing Infrastructure and Applications," and 7, "Voice-Mail System Design."

Customer Response Solution

The Customer Response Solution (CRS) platform provides interactive telephony and multimedia services. It provides a multimedia (voice, data, and web) IP-enabled customer-care

application environment. The CRS platform uses VoIP technology, so an organization's telephony network can share resources with the data network.

The CRS platform uses an open architecture that supports industry standards. This enables application designers to integrate applications with a wide variety of technologies and products.

The CRS platform includes the following applications:

- Cisco IP Auto Attendant (IP AA)
- Cisco Interactive Voice Response (IP IVR)
- Cisco IP Contact Center (IPCC) Express (formerly known as Integrated Contact Distribution, or ICD)

CRS has add-on components, including Automatic Speech Recognition (ASR) and Text-to-Speech (TTS).

IVR

IVR queues the callers, accepts the input, and does a database lookup based on the input. The open standards-based design of the CRS platform supports connectivity to various databases, such as Microsoft SQL, Oracle, Sybase, and IBM DB2 via Open DataBase Connection (ODBC) interface.

IPCC Express

Cisco IPCC Express provides enterprises with a contact management solution that is ideal to implement a small-scale contact center or internal help desk. IPCC Express provides Automated Call Distribution (ACD), IVR, and CTI functionality. The ACD queues and distributes incoming calls that are destined for groups of CallManager users. The IVR gathers caller data and classifies incoming calls based on user-entered information. IPCC Express includes a web-based real-time reporting system that monitors the system performance, Contact Service Queue (CSQ), and resource performance.

A Java Telephony API (JTAPI) connection manages communication between the CRS engine and CallManager Computer Telephony Integration Manager (CTIM) service.

The sizing of the CRS platform depends on the organization's call volume.

Cisco Unity

CallManager integrates with many existing voice-mail systems that use the Simplified Message Desk Interface (SMDI) standard and other voice-mail systems from Lucent, Avaya, or Nortel that use proprietary protocols. CallManager uses the Cisco Digital PBX Adapter (DPA) 7630 to integrate with Lucent or Avaya voice-mail systems and DPA 7610 to integrate with Nortel voice-mail systems.

Cisco Unity is a voice-mail/unified messaging solution that delivers powerful unified messaging (e-mail, voice, and fax messages sent to one inbox) for Microsoft Exchange or Lotus Domino environments. Cisco Unity can integrate with CallManager and with many legacy PBXs. Cisco Unity communicates with CallManager via SCCP.

Likewise, CallManager server has guidelines on the maximum number of devices that can be registered; Cisco Unity server has guidelines on the number of subscriber accounts per Unity server. The capacity depends on the hardware platforms.

Redundancy is achieved in an IPT network by deploying the CallManagers in cluster configuration. To build the redundancy for Cisco Unity deployment, two Unity servers are deployed. Unlike CallManager, where the load can be shared on all the servers in the cluster, the Cisco Unity servers deployed in the failover model do not share the load. Only one server is active at a time.

Cisco Emergency Responder

An IPT network provides flexibility to move the IP phones from one location to another location without the involvement of an administrator. This is attractive to many organizations and network administrators because it reduces the cost.

However, careful planning is required, which varies depending on the country where the telephony system is deployed and local government rules and regulations for routing emergency calls.

In the United States and Canada, users dial 911 (in other countries, this number varies) to make emergency calls to get the services of police, ambulance, and fire personnel. In a regular 911 system, also called a Basic-9-1-1 system, the emergency calls are sent to a public safety answering point (PSAP). No mechanism ensures that the call is sent to the correct PSAP, and the PSAP does not receive information about the location of the 911 caller. Enhanced 9-1-1, or E-9-1-1, sends 911 calls to the correct PSAP based on the location of the caller, and it ensures that the PSAP knows where the 911 caller is located (even without the caller providing directions). The location is determined by querying an Automatic Location Information (ALI) database that maps the phone number of the 911 caller to the caller's physical location.

Large organizations that maintain their own phone systems (e.g. key systems, PBXs, and Cisco CallManagers) are responsible for maintaining the ALI database information and providing the updates to the ALI database to the local exchange carrier (LEC) from time to time.

Cisco Emergency Responder (CER) is designed to address the E-9-1-1 functionality requirements for multiline telephone systems (MLTSs) deployed in North America. CER dynamically tracks the device (IP phone or SoftPhone) movements and routes the emergency calls to the right PSAP based on the device's current physical location.

Consider a case in which an employee in New York office location 1 moves the phone to New York office location 2. Assume that these two offices are served by different PSAPs. After the employee moves the phone to New York office location 2, if a user makes an emergency call, the call is routed to the PSAP for location 1. Because the user's phone number originally registered with New York office location 1, the PSAP for location 1 dispatches emergency staff to New York office location 1, and the user at location 2 waits indefinitely for the help.

CER in an IPT network enables emergency agencies to identify the location of callers and eliminates the need for administration when phones or people move from one location to another.

The phone's location is dynamically tracked by CER based on the switch ports to which the phone is attached. CER polls the switches via the Simple Network Management Protocol (SNMP) and updates the location database. Thus, in the previous example, when the phone is moved to New York office location 2, CER detects that the phone is now in New York office location 2, because it is connected to a switch that is in New York office location 2, and it routes the emergency calls to the PSAP that services New York office location 2.

Cisco Conference Connection

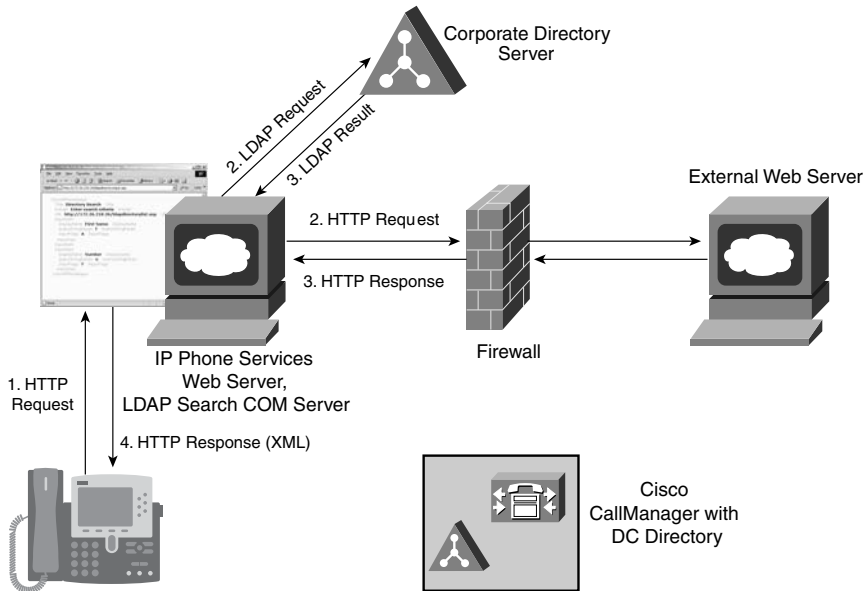
Cisco Conference Connection (CCC) is an application that allows users to schedule conferences. Users can schedule conferences via a simple web-based interface. Conference participants call in to a central number, enter a meeting identification, and are then placed into the conference.

IP Phone Services

You can provide additional services such as those listed here to the end users from their IP phones:

- Calendar
- Weather information
- Airline information
- Corporate directory lookup
- Stock quotes

Offering these services on the IP phones requires a connection through an external web server such as Microsoft Internet Information Server (IIS) or Apache, as shown in Figure 1-14. The IP phone sends the requests in the HTTP packet to the web server. The request could be to get the latest stock quote, flight arrival/departure information, or some other information. The IP Phone services web server contacts the external web servers and sends the response in XML format back to the IP phones. IP phones parse the information contained within the XML tags and display it on the phone.

Figure 1-14 *IP Phone Services***NOTE**

In the Figure 1-14, "Step 2. HTTP Request" and "Step 3. HTTP Response" are used when accessing the IP phone services that require connection to the external web server. Examples of such services are stock quote and airline information.

The preceding concept can be extended to provide IP phone service to do a corporate directory lookup from the IP phone. The following steps explain how this service works:

- 1 The IP phone user selects a corporate lookup directory service on the IP phone.
- 2 The IP phone sends an HTTP request to the IP phone services web server.
- 3 The IP phone services web server sends an LDAP request to the corporate LDAP server.
- 4 The IP phone services web server passes the returned LDAP result to the IP phone in XML format.
- 5 The IP phone parses the information and displays the search results on the IP phone.

For more information on providing such services, refer to the IP phone services Software Development Kit (SDK) documentation, available at http://www.cisco.com/pcgi-bin/dev_support/access_level/product_support.

IP Telephony Deployment Architectures

By using CallManager, organizations can eliminate PBX and replace it with IPT over a converged network. CallManager provides call-control functionality and, when used in conjunction with IP phone sets or a soft phone application, it can provide PBX functionality in

a distributed and scalable fashion. Cisco IPT solution deployment models fall into one of the following categories:

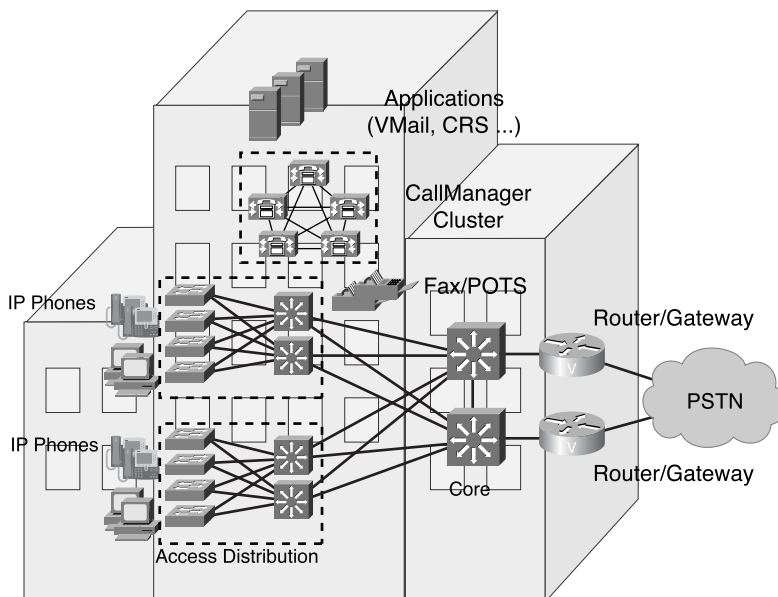
- Single-site deployment
- Centralized call processing with remote branches
- Distributed call-processing deployment
- Clustering over the IP WAN

Selection of the deployment model depends on the organization's requirements, such as the size of the network, features, and availability of the WAN bandwidth. This section provides information on various deployment models at a high level. To get detailed information on the benefits and limitations, refer to the *IP Telephony Solution Reference Network Design for Cisco CallManager 4.0* on Cisco.com, available for download at <http://www.cisco.com/go/srnd>.

Single-Site Deployment

In this deployment model, shown in Figure 1-15, CallManager applications such as voice mail, IP-IVR, AutoAttendant (AA), Transcoding, and conferencing resources are located at the same physical location. All the IP phones are located within this single site. The PSTN is used to route the off-net calls.

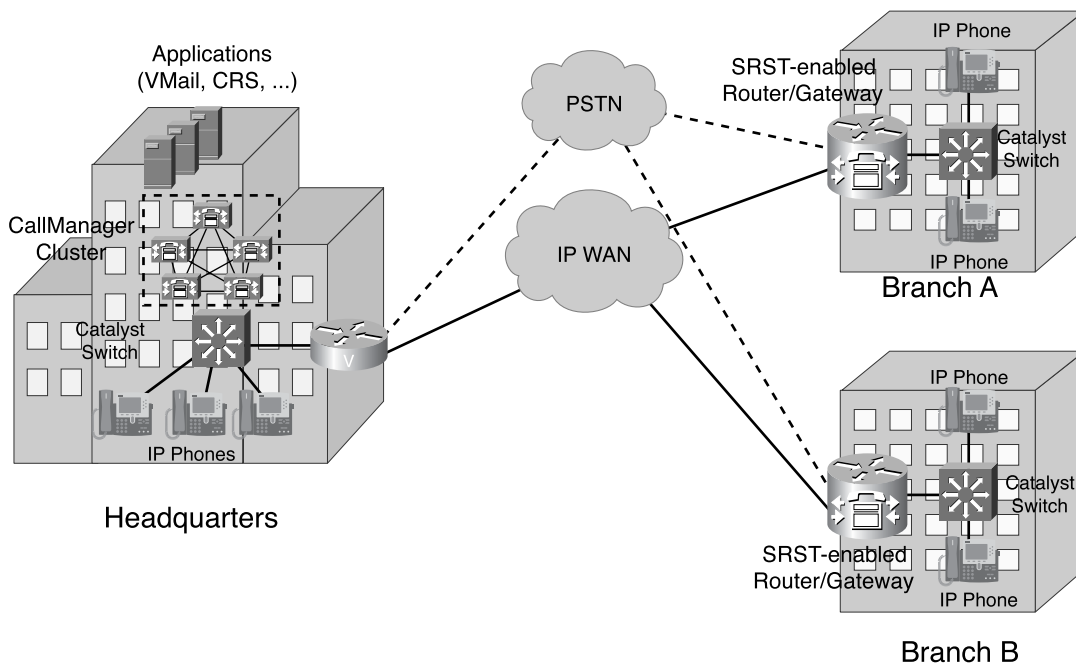
Figure 1-15 *Single-Site Deployment Model*



Centralized Call Processing with Remote Branches

Figure 1-16 shows the centralized call-processing deployment with remote branches. All the call processing is done at the central site. This is suitable for organizations in which the majority of the workforce is concentrated at a single site and small numbers of employees work at the remote branches.

Figure 1-16 *Centralized Call-Processing Model*



At each remote branch, SRST routers ensure that call processing is preserved in case of WAN link failure. The voice traffic travels via the IP WAN and falls back to the PSTN if not enough bandwidth is available across the WAN link, by using the Automated Alternate Routing (AAR) feature available in the CallManager.

You can avoid the oversubscription of the WAN bandwidth by using the locations-based CAC feature in the CallManager. This feature works for hub-and-spoke topologies. For example, as shown in Figure 1-16, the hub site is the headquarters and the branches are spokes. Each branch is defined as a location in CallManager, and maximum bandwidth is assigned to each location along with the codec to be used when placing calls between two locations. CallManager maintains the current state of the utilized bandwidth and checks the bandwidth availability before placing a new call to the locations.

With this deployment model, you can use the G.711 codec within the LAN. However, when placing the voice calls between the headquarters site and the branch sites or between the branch sites, you can use lower-bandwidth codecs such as G.729. The amount of bandwidth required per voice call depends on the type of codec chosen between the central and remote sites. Remote branch routers running Cisco IOS software along with the CallManager software can provide transcoding and conferencing functions locally. QoS configurations are required on the WAN links between the central site and each of the remote sites to prioritize the traffic. The traffic that requires priority includes the call-control traffic between the IP phones and the CallManager, the gateway signaling protocol (H.323, MGCP) traffic between the remote gateways and the CallManager, and the actual voice traffic.

This deployment model is cost effective and provides many benefits, such as a unified dial plan, less administrative overhead, and potential savings on communications costs as intersite calls use the IP WAN as first choice. The only limitation is that the remote sites will have limited features available if a WAN failure occurs while you are operating in the SRST mode.

Distributed Call Processing Deployment

In a distributed call-processing deployment, CallManager and applications are located at each site. Device weights and dial plan weight calculations determine the number of IP phones supported at each site.

Figure 1-17 depicts a distributed call-processing model in which headquarters and branch A IP phones are served by separate CallManager clusters and branch B is served by the Cisco CallManager Express (CME) feature that is enabled on the router. CME solution is suitable for a small branch.

Intercluster Trunks link CallManager clusters. The Cisco IOS gatekeeper ensures that only a permitted number of calls are sent across the IP WAN between the CallManager clusters. PSTN connections on the gateways route the local off-net calls from each location and serve as a backup connection to IP WAN when insufficient bandwidth is available to support additional calls.