



Official Cert Guide

Advance your IT career with hands-on learning

CCNP Collaboration Cloud and Edge Solutions

CLCEI 300-820

ciscopress.com

Jason Ball, CCSI® No. 33717
TJ Arneson, CCSI® No. 35208

FREE SAMPLE CHAPTER

SHARE WITH OTHERS



CCNP Collaboration Cloud and Edge Solutions CLCEI 300-820 Official Cert Guide

JASON BALL, CCSI No. 33717

TJ ARNESON, CCSI No. 35208

Cisco Press

CCNP Collaboration Cloud and Edge Solutions CLCEI 300-820 Official Cert Guide

Jason Ball and TJ Arneson

Copyright© 2022 Cisco Systems, Inc.

Published by:
Cisco Press

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.

ScoutAutomatedPrintCode

Library of Congress Control Number: 2021944062

ISBN-13: 978-0-13-673372-0

ISBN-10: 0-13-673372-7

Warning and Disclaimer

This book is designed to provide information about the CCNP CLCEI 300-820 exam. 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 author 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.

Special Sales

For information about buying this title in bulk quantities, or for special sales opportunities (which may include electronic versions; custom cover designs; and content particular to your business, training goals, marketing focus, or branding interests), please contact our corporate sales department at corpsales@pearsoned.com or (800) 382-3419.

For government sales inquiries, please contact governmentsales@pearsoned.com.

For questions about sales outside the U.S., please contact intlcs@pearson.com.

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 email at feedback@ciscopress.com. Please make sure to include the book title and ISBN in your message.

We greatly appreciate your assistance.

Editor-in-Chief: Mark Taub

Copy Editor: Bill McManus

Alliances Manager, Cisco Press: Arezou Gol

Technical Editor(s): Daniel Ball
Jeffrey Hubbard

Director, ITP Product Management: Brett Bartow

Editorial Assistant: Cindy Teeters

Executive Editor: Nancy Davis

Cover Designer: Chuti Prasertsith

Managing Editor: Sandra Schroeder

Composition: codeMantra

Development Editor: Ellie Bru

Indexer: Erika Millen

Senior Project Editor: Tonya Simpson

Proofreader: Donna Mulder



Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

Asia Pacific Headquarters
Cisco Systems (USA) Pte. Ltd.
Singapore

Europe Headquarters
Cisco Systems International BV Amsterdam,
The Netherlands

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

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: www.cisco.com/go/trademarks. Third party trademarks mentioned 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. (1110R)

About the Authors

Anyone who has worked with **Jason Ball** or has sat in one of his classes knows that his enthusiasm for collaboration is matched only by his engaging zeal for teaching. Jason's current position as a solution readiness engineer in Collaboration for Cisco awards him with the opportunity to create and provide training to Cisco partners on new, innovative collaboration solutions as Cisco releases them. He has been operating as a collaboration engineer for more than 11 years and holds 19 different certifications, including a CCNP Collaboration certification and a Cisco Certified Systems Instructor (CCSI) certification. He has been teaching Cisco Voice, Video, and Collaboration certification courses for as many years as he has been involved with Cisco.

Some of the accomplishments that Jason has achieved include serving as a subject matter expert (SME) for two certification courses Cisco has developed: the TVS Advanced Services Course and the CIVND2 certification course for the former CCNA Collaboration certification. He also wrote the Video Infrastructure Implementation (VII) Advanced Services course for Cisco, coauthored *CCNA Collaboration CIVND 210-065 Official Cert Guide* (Cisco Press, 2015), and was the sole author of *CCNP and CCIE Collaboration Core CLCOR 350-801 Official Cert Guide* (Cisco Press). Jason currently resides in Raleigh, North Carolina, with his wife and two children.

TJ Arneson is a Cisco Certified Systems Instructor (CCSI) who has had a history with Cisco products since his enlistment days in the U.S. Army. He has obtained both the CCNP Routing & Switching and Collaboration certifications. TJ's current position is a Customer Success Specialist for Cisco Systems, where he is enabling and empowering customers through the Customer Experience (CX) team under the Service Provider theater. TJ currently resides in sunny Tampa, Florida. When he is not working, he is either fishing in Tampa Bay or grinding levels in video games with his wife.

About the Technical Reviewers

Jeff Hubbard, CCNP Collaboration, CCSI No. 34456, is an engineering project manager with Cisco focusing on training products in the Cloud Collaboration segment. He has been in the technology industry for more than 30 years in a wide variety of roles, and devoted himself solely to Cisco products beginning in 2008, when he started working as a Cisco Certified Systems Instructor with an emphasis on video and voice solutions. In his free time Jeff is an avid motorcyclist and spends most of his time exploring the less-traveled dirt roads of Colorado's Rocky Mountains.

Daniel Ball is a leader in Cisco Collaboration technologies, with a strong background in higher education. He is currently a senior training specialist for PCH Collaboration, focusing on programmability and API integrations. Daniel also maintains a growing YouTube channel called Collab Crush, which is dedicated to promoting quality training for the Cisco Collaboration solution. Daniel received a Bachelor of Arts degree from the University of Texas at Austin and a Master of Science degree in Education from Shenandoah University. His Cisco certifications include CCNA Route/Switch, CCNA Collaboration, and CCNP Collaboration. Currently, Daniel lives in Kobe, Japan, with his wife, Miki, and two daughters, Midori and Hana.

Dedications

I would like to dedicate my contribution in this book to my wife of 24 years. The love, encouragement, and support she has offered have been the strength that has sustained me throughout this endeavor. Every accomplishment I have achieved has been encouraged by her cheering for me from the sidelines. She is the best partner and friend anyone could ask for.

—*Jason*

I would like to dedicate my half of this book to my wife of 8 years as she has been through deployments, heavy travel for work, and the strain of working on her own career on top of that. Jessica has always been a best friend and has grown into a partner in the journey of life.

—*TJ*

Acknowledgments

TJ and I want to acknowledge and thank the technical editors who have also contributed greatly to this book. Jeff Hubbard, it is unfathomable to think about how much both of us have been through, and how much we have learned in the nine and a half years we have worked together and formed our friendship. You have helped challenge and shape me as much as I have done the same for you. Daniel Ball, you are more than a brother to me. Obviously, we have gone through a lifetime of experiences together, but the last 15 years of our lives have proven to be the most formative to our bond. You helped me take that leap into the world of technology, and I would not be where I am without your inspiration.

We would also like to express our gratitude to Eleanor Bru, development editor of this book. We were so incredibly lucky to work with her on this text. She has always been a strong professional who takes the time to ensure the job gets done correctly the first time. Without her, this book would not have been possible, as she worked patiently with us to make this book a reality.

The perceptiveness and expertise of project editor, Tonya Simpson, were integral and vital to this book. Her keenness of insight, understanding, and intuition enabled us to produce quality material. We are thankful for her expertise as we could not accomplish this without her.

Finally, we would like to acknowledge Nancy Davis. You, too, have been a huge part of the success of this book. You constantly had to stay on top of TJ and me to ensure we met our deadlines, and you offered great feedback in the chapters that helped shape the final version of this book. You were always professional, yet gentle and easy to work with. We have enjoyed working with you and would love the opportunity to work with you again.

Contents at a Glance

Introduction xx

Part I Key Concepts

- Chapter 1 Introduction to the Cisco Expressway Solution 2
- Chapter 2 Configure Key Cisco Expressway Settings 24
- Chapter 3 Initial Configuration Settings on the Cisco Expressway 46
- Chapter 4 Regular Expressions on the Cisco Expressway 62
- Chapter 5 Security Overview on the Cisco Expressway 68

Part II Cisco Expressway Configurations

- Chapter 6 Registration on Cisco Expressway 92
- Chapter 7 Cisco Expressway Call Processing Order 114
- Chapter 8 Bandwidth Management 134
- Chapter 9 Multisite Collaboration Solutions 148
- Chapter 10 Multisite and Business-to-Business (B2B) Collaboration Solutions 178
- Chapter 11 Clustering Expressways 208
- Chapter 12 Troubleshooting a Business-to-Business (B2B) Collaboration Solution 218

Part III Mobile and Remote Access

- Chapter 13 Introduction to Mobile and Remote Access (MRA) 238
- Chapter 14 Configure an MRA Solution 248
- Chapter 15 Troubleshoot an MRA Solution 284

Part IV Cisco Webex Technologies

- Chapter 16 Introduction to Cisco Cloud Collaboration 298
- Chapter 17 Configure Webex Hybrid Directory Service 316
- Chapter 18 Configure Webex Hybrid Calendar Service 342
- Chapter 19 Configure Webex Hybrid Message Service 380

Chapter 20	Webex Edge Solutions	404
Chapter 21	Cisco Jabber for Cloud and Hybrid Deployments with Cisco Webex Messenger	444
Chapter 22	Final Preparation	454
Appendix A	Answers to the “Do I Know This Already?” Quizzes and Review Questions	460
Appendix B	CCNP Implementing Cisco Collaboration Cloud and Edge Solutions (CLCEI) 300-820 Exam Updates	486
	Glossary of Key Terms	489
	Index	504

Online Elements

Appendix C	Memory Tables
Appendix D	Memory Tables Answer Key
Appendix E	Study Planner
	Glossary of Key Terms

Contents

Introduction xx

Part I Key Concepts

Chapter 1 Introduction to the Cisco Expressway Solution 2

“Do I Know This Already?” Quiz 2
Foundation Topics 4
VCS to Expressway Migration 4
SIP on the Expressway 5
H.323 on the Expressways 8
Describe Expressway Licensing 11
 Option Keys 15
 Release Key 16
 License Consumption 17
Exam Preparation Tasks 21
Review All Key Topics 21
Complete Tables and Lists from Memory 22
Define Key Terms 22
Q&A 23

Chapter 2 Configure Key Expressway Settings 24

“Do I Know This Already?” Quiz 25
Foundation Topics 26
Cisco Expressway Deployment on VM 26
Service Setup Wizard Through Web Interface 28
Expressway System Configuration 34
Expressway Backup and Restore Procedure 42
Exam Preparation Tasks 44
Review All Key Topics 44
Complete Tables and Lists from Memory 45
Define Key Terms 45
Q&A 45

Chapter 3 Initial Configuration Settings on the Cisco Expressway 46

“Do I Know This Already?” Quiz 46
Foundation Topics 48
H.323 Settings 48
SIP and Domain Settings 51
Protocol Interworking on the Cisco Expressway 55

	Verifying Registration on the Cisco Expressway	57
	Exam Preparation Tasks	59
	Review All Key Topics	59
	Complete Tables and Lists from Memory	59
	Define Key Terms	60
	Q&A	60
Chapter 4	Regular Expressions on the Cisco Expressway	62
	“Do I Know This Already?” Quiz	62
	Foundation Topics	64
	Overview and Use Cases for Regular Expressions	64
	Verifying Regular Expression Using the Check Pattern Tool	66
	Exam Preparation Tasks	67
	Review All Key Topics	67
	Complete Tables and Lists from Memory	67
	Define Key Terms	67
	Q&A	67
Chapter 5	Security Overview on the Cisco Expressway	68
	“Do I Know This Already?” Quiz	68
	Foundation Topics	70
	Describe SIP Media Encryption Mode	70
	Certificates	72
	Configuring Certificate-Based Authentication	73
	<i>Enabling Certificate-Based Authentication</i>	73
	<i>Authentication Versus Authorization</i>	73
	<i>Obtaining the Username from the Certificate</i>	74
	<i>Emergency Account and Certificate-based Authentication</i>	74
	Managing the Trusted CA Certificate List	74
	Managing the Expressway Server Certificate	75
	<i>Using the ACME Service</i>	75
	<i>Server Certificates and Clustered Systems</i>	76
	Managing Certificate Revocation Lists	76
	<i>Certificate Revocation Sources</i>	76
	<i>Automatic CRL Updates</i>	77
	<i>Manual CRL Updates</i>	77
	<i>Online Certificate Status Protocol</i>	78

<i>Configuring Revocation Checking for SIP TLS Connections</i>	78
Administrator Authentication	80
Configuring SSH	81
Advanced Security	81
<i>HTTP Methods</i>	81
<i>Enabling Advanced Account Security</i>	83
<i>Expressway Functionality: Changes and Limitations</i>	83
<i>Disabling Advanced Account Security</i>	84
Configuring FIPS140-2 Cryptographic Mode	84
<i>Enable FIPS140-2 Cryptographic Mode</i>	85
<i>Managing Domain Certificates and Server Name Indication for Multitenancy</i>	87
<i>Managing the Expressway's Domain Certificates</i>	88
Exam Preparation Tasks	90
Review All Key Topics	90
Complete Tables and Lists from Memory	91
Define Key Terms	91
Q&A	91

Part II Cisco Expressway Configurations

Chapter 6 Registration on Cisco Expressway 92

“Do I Know This Already?” Quiz	92
Foundation Topics	94
Registration Conflict Policy	94
Registration Restriction Policy	96
Registration Authentication	101
Subzones and Membership Rules	106
Exam Preparation Tasks	112
Review All Key Topics	112
Complete Tables and Lists from Memory	113
Define Key Terms	113
Q&A	113

Chapter 7 Cisco Expressway Call Processing Order 114

“Do I Know This Already?” Quiz	114
Foundation Topics	116
Transforms	116
Call Policy	122

User Policy	128
Search History and the Locate Tool	131
Exam Preparation Tasks	133
Review All Key Topics	133
Complete Tables and Lists from Memory	133
Define Key Terms	133
Q&A	133

Chapter 8 Bandwidth Management 134

“Do I Know This Already?” Quiz	134
Foundation Topics	136
Subzone Bandwidth Management	136
Links and Pipes Bandwidth Management	140
Call Control Using Pipes	145
Exam Preparation Tasks	147
Review All Key Topics	147
Complete Tables and Lists from Memory	147
Define Key Terms	147
Q&A	147

Chapter 9 Multisite Collaboration Solutions 148

“Do I Know This Already?” Quiz	149
Foundation Topics	151
Dial Plan Elements	151
Zones	151
Search Rules	154
Simple Video Network with a Flat Dial Plan	157
Complex Video Network with a Flat Dial Plan	158
Complex Video Network with a Structured Dial Plan	161
Hierarchical Video Network with a Structured Dial Plan	162
Configuring Neighbor Zones	165
Expressway to Expressway Neighbor Zones	166
Expressway to Cisco Unified CM Neighbor Zone	169
Exam Preparation Tasks	176
Review All Key Topics	176
Complete Tables and Lists from Memory	177
Define Key Terms	177
Q&A	177

Chapter 10 Multisite and Business-to-Business (B2B) Collaboration Solutions 178

- “Do I Know This Already?” Quiz 179
- Foundation Topics 181
- Firewall Issues in a Collaboration Environment 181
- NAT Issues in a Collaboration Environment 182
- Purpose of STUN, TURN, and ICE 183
 - STUN 183
 - TURN 184
 - ICE 186
- Expressway Media Traversal 187
 - Assent and H.460.18/19 188
 - Configuring Traversal Zones on Expressway Core and Edge 189
 - Deployment Scenarios for Traversal Zones 196
- DNS Zones 199
- Exam Preparation Tasks 205
- Review All Key Topics 205
- Complete Tables and Lists from Memory 206
- Define Key Terms 206
- Q&A 206

Chapter 11 Clustering Expressways 208

- “Do I Know This Already?” Quiz 208
- Foundation Topics 210
- Clustering Requirements 210
- DNS and Clustering 213
- Zones and Clustering 214
- Exam Preparation Tasks 216
- Review All Key Topics 216
- Complete Tables and Lists from Memory 216
- Define Key Terms 217
- Q&A 217

Chapter 12 Troubleshooting a Business-to-Business (B2B) Collaboration Solution 218

- “Do I Know This Already?” Quiz 219
- Foundation Topics 220
- Troubleshooting Registration Issues 220
- Troubleshooting Calling Issues 225

Troubleshooting DNS Issues	230
Troubleshooting Certificate Issues	232
Client Certificate Testing Tool	232
Server Traversal Test Tool	233
Other Troubleshooting Tools	234
Exam Preparation Tasks	237
Review All Key Topics	237
Complete Tables and Lists from Memory	237
Define Key Terms	237
Q&A	237

Part III Mobile and Remote Access

Chapter 13 Introduction to Mobile and Remote Access (MRA) 238

“Do I Know This Already?” Quiz	238
Foundation Topics	240
Purpose of MRA	240
Components of MRA	241
Considerations for MRA Deployment	242
Exam Preparation Tasks	246
Review All Key Topics	246
Complete Tables and Lists from Memory	246
Define Key Terms	246
Q&A	246

Chapter 14 Configure an MRA Solution 248

“Do I Know This Already?” Quiz	249
Foundation Topics	251
DNS Records	251
Certificates	254
TLS Verify Requirements	255
Cisco Expressway Certificates	259
Cisco Unified CM Certificates	260
Creating Certificates for MRA	261
Cisco Unified CM Settings for MRA	266
Unified Communications Configuration on Expressways	270
HTTP Allow List	274
Unified Communications Traversal Zones	278
Exam Preparation Tasks	281

- Review All Key Topics 281
- Complete Tables and Lists from Memory 282
- Define Key Terms 282
- Q&A 282

Chapter 15 Troubleshoot an MRA Solution 284

- “Do I Know This Already?” Quiz 285
- Foundation Topics 287
- MRA Troubleshooting General Techniques 287
- Registration and Certificate Issues 291
- Cisco Jabber Sign-In Issues 292
- Other Specific Issues 294
- Exam Preparation Tasks 296
- Review All Key Topics 296
- Complete Tables and Lists from Memory 297
- Define Key Terms 297
- Q&A 297

Part IV Cisco Webex Technologies

Chapter 16 Introduction to Cisco Cloud Collaboration 298

- “Do I Know This Already?” Quiz 298
- Foundation Topics 300
- Cloud Collaboration Solutions 300
 - Cisco Hosted Collaboration Solution 300
 - Cisco Webex 303
 - Cisco Unified Communications Manager Cloud* 303
- Cisco Webex Components 306
 - Webex Meetings 306
 - Webex Messaging 308
 - Webex Calling 309
- Cisco Webex Hybrid Services 310
 - Hybrid Calendar Service 311
 - Hybrid Directory Service 311
 - Hybrid Call Service 311
 - Hybrid Message Service 312
 - Hybrid Data Security Service 312
 - Hybrid Meeting Service (Video Mesh) 312
- Exam Preparation Tasks 313
- Review All Key Topics 313

Complete Tables and Lists from Memory 314

Define Key Terms 314

Q&A 314

Chapter 17 Configure Webex Hybrid Directory Service 316

“Do I Know This Already?” Quiz 316

Foundation Topics 318

Deployment Model 318

Deployment Requirements 319

Infrastructure Requirements 321

Active Directory Configuration and Synchronization 326

Webex User Service Assignment 338

Exam Preparation Tasks 340

Review All Key Topics 340

Complete Tables and Lists from Memory 340

Define Key Terms 340

Q&A 341

Chapter 18 Configure Webex Hybrid Calendar Service 342

“Do I Know This Already?” Quiz 342

Foundation Topics 344

Calendar Service Operation 344

Expressway-Based Calendar Connector 345

 Cisco Expressway-C Connector Host Preparation 345

 Hybrid Calendar Service Deployment 354

Google Calendar Deployment in the Cloud 362

Office 365 368

One Button to Push (OBTP) 374

Exam Preparation Tasks 377

Review All Key Topics 377

Complete Tables and Lists from Memory 378

Define Key Terms 378

Q&A 378

Chapter 19 Configure Webex Hybrid Message Service 380

“Do I Know This Already?” Quiz 380

Foundation Topics 382

Deployment Models 382

Deployment Requirements	385
Expressway Requirements	388
Certificates	392
Register Expressway Connector to the Cisco Webex Cloud	392
IM and Presence Configuration	394
Manage Hybrid Message Service	396
Exam Preparation Tasks	402
Review All Key Topics	402
Complete Tables and Lists from Memory	402
Define Key Terms	402
Q&A	402

Chapter 20 Webex Edge Solutions 404

“Do I Know This Already?” Quiz	404
Foundation Topics	406
Webex Edge for Devices	406
Webex Edge for Calling	414
Webex Edge Audio	416
Webex Edge Connect	417
Webex Video Mesh	418
Exam Preparation Tasks	442
Review All Key Topics	442
Complete Tables and Lists from Memory	442
Define Key Terms	443
Q&A	443

Chapter 21 Cisco Jabber for Cloud and Hybrid Deployments with Cisco Webex Messenger 444

“Do I Know This Already?” Quiz	444
Foundation Topics	445
Deployment Requirements	445
Cisco Unified CM Requirements	450
Exam Preparation Tasks	452
Review All Key Topics	452
Complete Tables and Lists from Memory	452
Define Key Terms	452
Q&A	453

Chapter 22	Final Preparation	454
	Getting Ready	454
	Tools for Final Preparation	455
	Pearson Test Prep Practice Test Engine and Questions on the Website	455
	<i>Accessing the Pearson Test Prep Software Online</i>	455
	<i>Accessing the Pearson Test Prep Software Offline</i>	455
	Customizing Your Exams	456
	Updating Your Exams	457
	<i>Premium Edition</i>	457
	Chapter-Ending Review Tools	457
	Suggested Plan for Final Review/Study	458
	Summary	458
Appendix A	Answers to the “Do I Know This Already?” Quizzes and Review Questions	460
Appendix B	CCNP Implementing Cisco Collaboration Cloud and Edge Solutions (CLCEI) 300-820 Exam Updates	486
	Glossary of Key Terms	489
	Index	504
Online Elements		
Appendix C	Memory Tables	
Appendix D	Memory Tables Answer Key	
Appendix E	Study Planner	
	Glossary of Key Terms	

Introduction

The Implementing Cisco Collaboration Cloud and Edge Solutions v1.0 (CLCEI 300-820) exam is a 90-minute exam associated with the CCNP Collaboration and Cisco Certified Specialist – Collaboration Cloud & Edge Implementation certifications. This exam tests a candidate's knowledge of collaboration cloud and edge solutions, Expressway configurations, and Cisco Webex Teams hybrid and emerging technologies. The course, Implementing Cisco Collaboration Cloud and Edge Solutions, helps candidates to prepare for this exam.

TIP You can review the exam blueprint from the Cisco website at <https://learningnetwork.cisco.com/s/clcei-exam-topics>.

This book gives you the foundation and covers the topics necessary to start your CCNP Collaboration or CCIE Collaboration journey.

The CCNP Collaboration Certification

The CCNP Collaboration certification is one of the industry's most-respected certifications. To earn the CCNP Collaboration certification, you must pass two exams: the CLCOR exam covered in *CCNP and CCIE Collaboration Core CLCOR 350-801 Official Cert Guide*, and one Collaboration concentration exam of your choice, so you can customize your certification to your technical area of focus.

TIP The CLCOR core exam is also the qualifying exam for the CCIE Collaboration certification. Passing this exam is the first step toward earning both of these certifications.

The following are the CCNP Collaboration concentration exams:

- Implementing Cisco Collaboration Applications (CLICA 300-810)
- Implementing Cisco Advanced Call Control and Mobility Services (CLACCM 300-815)
- Implementing Cisco Collaboration Cloud and Edge Solutions (CLCEI 300-820)
- Implementing Cisco Collaboration Conferencing (CLCNF 300-825)
- Automating and Programming Cisco Collaboration Solutions (CLAUTO 300-835)

TIP CCNP Collaboration now includes automation and programmability to help you scale and customize your Collaboration infrastructure. If you pass the Automating and Programming for Cisco Collaboration Solutions (CLAUTO 300-835) exam, the Implementing and Operating Cisco Collaboration Core Technologies (CLCOR 350-801) exam, and the Developing Applications Using Cisco Core Platforms and APIs (DEVCOR 350-901) exam, you will achieve the CCNP Collaboration and DevNet Professional certifications with only three exams. Every exam earns an individual Specialist certification, allowing you to get recognized for each of your accomplishments, instead of waiting until you pass all the exams.

There are no formal prerequisites for CCNP Collaboration. In other words, you do not have to pass the CCNA Collaboration or any other certifications in order to take CCNP-level exams. The same goes for the CCIE exams. On the other hand, CCNP candidates often have three to five years of experience in IT and Collaboration.

Cisco considers ideal candidates to be those who possess the following:

- Working knowledge of fundamental terms of computer networking, including LANs, WANs, switching, and routing
- Basics of digital interfaces, public switched telephone networks (PSTNs), and Voice over IP (VoIP)
- Fundamental knowledge of converged voice and data networks and Cisco Unified Communications Manager deployment

The CCIE Collaboration Certification

The CCIE Collaboration certification is one of the most admired and elite certifications in the industry. The CCIE Collaboration program prepares you to be a recognized technical leader. To earn the CCIE Collaboration certification, you must pass the Implementing and Operating Cisco Collaboration Core Technologies (CLCOR 350-801) exam and an eight-hour, hands-on lab exam. The lab exam covers very complex Collaboration network scenarios. These scenarios range from designing through deploying, operating, and optimizing Collaboration solutions.

Cisco considers ideal candidates to be those who have five to seven years of experience with designing, deploying, operating, and optimizing Collaboration technologies and solutions prior to taking the exam. Additionally, candidates will need to possess the following:

- Understand capabilities of different technologies, solutions, and services
- Translate customer requirements into solutions
- Assess readiness to support proposed solutions
- Deploy a Cisco Collaboration solution
- Operate and optimize a Cisco Collaboration solution

The Exam Objectives (Domains)

The Implementing Cisco Collaboration Cloud and Edge Solutions v1.0 (CLCEI 300-820) exam is broken down into four major domains. The contents of this book cover each of the domains and the subtopics included in them as illustrated in the following descriptions.

The following table breaks down each of the domains represented in the exam:

Domain	Percentage of Representation in Exam
1: Key Concepts	25%
2: Initial Expressway Configurations	25%
3: Mobile and Remote Access	25%
4: Cisco Webex Technologies	25%

The following topics are general guidelines for the content likely to be included on the exam; however, other related topics may also appear on any specific delivery of the exam. To better reflect the contents of the exam and for clarity purposes, the following guidelines might change at any time without notice. Here are the details of each domain and where the exam objectives are covered in the book:

Domain 1: Key Concepts	Chapter Where This Is Covered
1.1 Describe the complications of NAT in a Collaboration environment	Chapter 10
1.2 Describe the purpose of ICE, TURN, and STUN	Chapter 10
1.3 Describe Expressway media traversal	Chapter 10
1.4 Describe protocol interworking on the Expressway	Chapter 3
1.4.a SIP < > H.323	Chapter 3
1.4.b IPv4 and IPv6	Chapter 3
1.5 Describe Expressway Licensing	Chapter 1
1.5.a Option keys	Chapter 1
1.5.b Release key	Chapter 1
1.5.c License consumption	Chapter 1
1.6 Describe SIP media encryption mode	Chapter 5
1.6.a Auto	Chapter 5
1.6.b Force encrypted	Chapter 5
1.6.c Force unencrypted	Chapter 5
1.6.d Best effort	Chapter 5
1.7 Describe Expressway Core dial plan elements	Chapter 7
1.7.a Transforms	Chapter 7
1.7.b Search rules	Chapter 9
1.7.c Zones	Chapter 9
1.7.d Regular expressions	Chapter 4
1.7.e Pipes and links	Chapter 8
1.8 Describe key Expressway settings	Chapter 2
1.8.a DNS	Chapter 2
1.8.b Network interfaces	Chapter 2

Domain 1: Key Concepts		Chapter Where This Is Covered
1.8.c	<i>Certificates</i>	Chapter 5
1.8.d	<i>QoS</i>	Chapter 2
1.8.e	<i>Clustering</i>	Chapter 11
1.8.f	<i>Network firewall rules</i>	Chapter 2
1.9	Describe Expressway backup and restore procedure (standalone and cluster)	Chapter 2
Domain 2: Initial Expressway Configurations		
2.1	Configure key Expressway settings	Chapter 2
2.1.a	<i>DNS</i>	Chapter 2
2.1.b	<i>Network interfaces</i>	Chapter 2
2.1.c	<i>Certificates</i>	Chapter 5
2.1.d	<i>QoS</i>	Chapter 2
2.1.e	<i>Clustering</i>	Chapter 11
2.1.f	<i>Network firewall rules</i>	Chapter 2
2.2	Configure Expressway Core dial plan elements	Chapter 7
2.2.a	<i>Transforms</i>	Chapter 7
2.2.b	<i>Search rules</i>	Chapter 4
2.2.c	<i>Zones</i>	Chapter 9
2.2.d	<i>Regular expressions</i>	Chapter 4
2.2.e	<i>Pipes and links</i>	Chapter 8
2.3	Configure toll fraud prevention on Expressway series (no custom CPL scripts)	Chapter 7
2.4	Configure a Business to Business (B2B) collaboration solution	Chapter 12
2.4.a	<i>DNS records (focus on Microsoft DNS)</i>	Chapter 10
2.4.b	<i>Certificates (focus on Microsoft CA)</i>	Chapter 5
2.4.c	<i>Traversal Zones</i>	Chapter 10
2.4.d	<i>Neighbor Zones</i>	Chapter 9
2.4.e	<i>Transforms</i>	Chapter 7
2.4.f	<i>Search rules</i>	Chapter 9
2.4.g	<i>SIP trunk integration with Cisco Unified Communications Manager</i>	Chapter 9
2.5	Troubleshoot a Business to Business (B2B) collaboration solution	Chapter 12
2.5.a	<i>DNS records (focus on Microsoft DNS)</i>	Chapter 12
2.5.b	<i>Certificates (focus on Microsoft CA)</i>	Chapter 12
2.5.c	<i>Traversal Zones</i>	Chapter 12
2.5.d	<i>Neighbor Zones</i>	Chapter 12

Domain 1: Key Concepts	Chapter Where This Is Covered
2.5.e <i>Transforms</i>	Chapter 12
2.5.f <i>Search rules</i>	Chapter 12
2.5.g <i>SIP trunk integration with Cisco Unified Communications Manager</i>	Chapter 12
Domain 3: Mobile and Remote Access	
3.1 <i>Configure a Mobile and Remote Access (MRA) solution</i>	Chapter 14
3.1.a <i>DNS records types (not platform-specific)</i>	Chapter 14
3.1.b <i>Certificates (not platform specific, covers Unified Communications Manager, IM&P, Expressways, Unity Connection)</i>	Chapter 14
3.1.c <i>Unified Communications traversal zones</i>	Chapter 14
3.1.d <i>Unified Communications configuration on Expressway</i>	Chapter 14
3.1.e <i>HTTP allow list</i>	Chapter 14
3.1.f <i>SIP trunk security profile on Cisco Unified Communications Manager</i>	Chapter 14
3.2 <i>Troubleshoot a Mobile and Remote Access (MRA) solution</i>	Chapter 15
3.2.a <i>DNS records (focus on Microsoft DNS)</i>	Chapter 15
3.2.b <i>Certificates (focus on Microsoft CA, covers Unified Communications Manager, IM&P, Expressways, Unity Connection)</i>	Chapter 15
3.2.c <i>Unified Communications traversal zones</i>	Chapter 15
3.2.d <i>Unified Communications configuration on Expressway</i>	Chapter 15
3.2.e <i>HTTP allow list</i>	Chapter 15
3.2.f <i>SIP trunk security profile on Cisco Unified Communications Manager</i>	Chapter 15
Domain 4: Cisco Webex Technologies	
4.1 <i>Describe the signaling and media flows used in a Cisco Webex Video Mesh deployment</i>	Chapter 20
4.2 <i>Configure Webex Hybrid Services/Connector</i>	Chapter 16
4.2.a <i>Calendar Service (Office 365, Microsoft Exchange, One Button to Push)</i>	Chapters 16 and 18
4.2.b <i>Message Service (Deployment requirements; Expressway requirements, certificates, CallManager prerequisites, IM&P prerequisites, deployment models)</i>	Chapters 16 and 19

Domain 1: Key Concepts	Chapter Where This Is Covered
4.2c <i>Directory Services (Deployment requirements; deployment models, infrastructure requirements, active directory configuration, synchronization, Webex user service assignment)</i>	Chapters 16 and 17
4.2.d <i>Video Mesh (Deployment requirements including: bandwidth, clustering, endpoint support, video call capacity, ports and protocols, deployment models)</i>	Chapters 16 and 20
4.3 Describe Cisco Jabber for Cloud and Hybrid deployments with Cisco Webex Messenger	Chapter 21

Steps to Becoming a CCNP Collaboration Certified Engineer

To become a CCNP Collaboration Certified Engineer, you must first take and pass the CLCOR 350-801 exam. Passing this exam alone will automatically earn the Cisco Certified Specialist – Collaboration certification. You will then need to pass one of the collaboration specialization exams of your choosing, such as the CLCEI 300-820 exam. Passing these two exams will earn you the CCNP Collaboration certification. All Cisco certification exams are managed by the Pearson Vue testing organization. Use the following steps to sign up for your Cisco exam.

Signing Up for the Exam

The steps required to sign up for the CCNP Collaboration CLCEI 300-820 exam are as follows:

1. Navigate to <https://home.pearsonvue.com/cisco>.
2. To schedule a Cisco exam, you must first have a CCO ID you created on the Cisco website. Then you must create a Pearson VUE login and link it to the CCO ID. After all this is created, you must sign in to the Pearson VUE site to schedule the exam. Click **Sign In** from the column on the right side of the screen and enter your login credentials.
3. Once signed in click on the View exams button.
4. In the Find an Exam box, enter **300-820** and then click the **300-820: Implementing Cisco Collaboration Cloud and Edge Solutions** name when it appears. Click **Go** to proceed to the next screen.
5. Select either the **At a test center** or the **Online at my home or office** option for where you want to take the exam, read through the information on the screen related to your choice, then click on the next button at the bottom of the screen.
6. Continue to follow the steps on the screen. The options will vary based on your selection from the previous step. You will also need to provide payment for the exam you're scheduling. The CLCEI 300-820 exam costs \$300 USD.

Facts About the Exam

The exam is a computer-based test. It consists of multiple-choice questions only. To take the test, you must bring two forms of ID; one must be a government-issued identification card with a photo. The second can be any official ID with your name on it, such as a Social Security card, employee ID card, or credit card, as long as it has your signature on it.

About the CCNP CLCEI 300-820 Official Cert Guide

Although this book does not map sequentially to the topic areas of the exam, all topic areas on the exam are covered in this book. This book cannot contain the personal experience and hands-on exposure to the equipment needed to answer some of the questions that may be asked in the exam. However, it was our intent to write this book in a manner that provides a slow buildup to the technologies that are being tested so that you will not only be better prepared to pass the test but also develop a solid understanding of the underlying technologies examined in this book. This book also uses a number of features to help you understand the topics and prepare for the exam.

Objectives and Methods

This book uses several key methodologies to help you discover the exam topics on which you need more review, help you fully understand and remember those details, and help you prove to yourself that you have retained your knowledge of those topics. This book does not try to help you pass the exam only by memorization; it seeks to help you to truly learn and understand the topics. This book is designed to help you pass the CCNP CLCEI 300-820 exam by using the following methods:

- Helping you discover which exam topics you have not mastered
- Providing explanations and information to fill in your knowledge gaps
- Supplying exercises that enhance your ability to recall and deduce the answers to test questions
- Providing practice exercises on the topics and the testing process via test questions on the companion website

Book Features

To help you customize your study time using this book, the core chapters have several features that help you make the best use of your time:

- **Foundation Topics:** These are the core sections of each chapter. They explain the concepts for the topics in that chapter.
- **Exam Preparation Tasks:** After the “Foundation Topics” section of each chapter, the “Exam Preparation Tasks” section lists a series of study activities that you should do at the end of the chapter:
- **Review All Key Topics:** The Key Topic icon appears next to the most important items in the “Foundation Topics” section of the chapter. The Review All Key

Topics activity lists the key topics from the chapter, along with their page numbers. Although the contents of the entire chapter could be on the exam, you should definitely know the information listed in each key topic, so you should review these areas.

- **Define Key Terms:** Although the CCLEI exam may be unlikely to ask a question such as “Define this term,” the exam does require that you learn and know a lot of terminology. This section lists the most important terms from the chapter, asking you to write a short definition and compare your answer to the glossary at the end of the book.
- **Complete Memory Tables:** Open Appendix C from the book’s website and print the entire thing or print the tables by major part. Then complete the tables.
- **Review Questions:** Confirm that you understand the content that you just covered by answering these questions and reading the answer explanations.
- **Web-Based Practice Exam:** The companion website includes the Pearson Test Prep practice test engine that enables you to take practice exam questions. Use it to prepare with a sample exam and to pinpoint topics where you need more study.

How This Book Is Organized

This book contains 21 core chapters. Chapter 22 includes preparation tips and suggestions for how to approach the exam. Each core chapter covers a subset of the topics on the CLCEI 300-820 exam. The core chapters map to the CLCEI 300-820 exam topic areas and cover the concepts and technologies that you will encounter on the exam. Refer to the exam objective/chapter mapping table as a reference to see which objectives are covered in which chapters. Also, each chapter includes a list of objectives covered in that chapter for easy reference.

The Companion Website for Online Content Review

All the electronic review elements, as well as other electronic components of the book, exist on this book’s companion website.

To access the companion website, which gives you access to the electronic content with this book, start by establishing a login at the Cisco Press website and registering your book. To do so, simply go to <https://www.ciscopress.com/register> and enter the ISBN of the print book: **9780136733720**. After you have registered your book, go to your account page and click the **Registered Products** tab. From there, click the **Access Bonus Content** link to get access to the book’s companion website.

Note that if you buy the Premium Edition eBook and Practice Test version of this book from Cisco Press, your book will automatically be registered on your account page. Simply go to your account page, click the **Registered Products** tab, and select **Access Bonus Content** to access the book’s companion website.

Please note that many of our companion content files can be very large, especially image and video files.

If you are unable to locate the files for this title by following the preceding steps, please visit <https://www.pearsonITcertification.com/contact> and select the **Site Problems/Comments** option. Our customer service representatives will assist you.

How to Access the Pearson Test Prep Practice Test Software

You have two options for installing and using the Pearson Test Prep software: a web app and a desktop app. To use the Pearson Test Prep software, start by finding the registration code that comes with the book. You can find the code in these ways:

- **Print book:** Look in the cardboard sleeve in the back of the book for a piece of paper with your book's unique PTP code.
- **Premium Edition:** If you purchase the Premium Edition eBook and Practice Test directly from the Cisco Press website, the code will be populated on your account page after purchase. Just log in at <https://www.ciscopress.com>, click **Account** to see details of your account, and click the **Digital Purchases** tab.
- **Amazon Kindle:** For those who purchase a Kindle edition from Amazon, the access code will be supplied directly from Amazon.
- **Other Bookseller eBooks:** Note that if you purchase an eBook version from any other source, the practice test is not included because other vendors to date have not chosen to vend the required unique access code.

NOTE Do not lose the activation code, because it is the only means with which you can access the QA content with the book.

Once you have the access code, to find instructions about both the PTP web app and the desktop app, follow these steps:

- Step 1.** Open this book's companion website, as shown earlier in this Introduction under the heading "The Companion Website for Online Content Review."
- Step 2.** Click the **Practice Exams** button.
- Step 3.** Follow the instructions listed there both for installing the desktop app and for using the web app.

Note that if you want to use the web app only at this point, just navigate to <https://www.pearsonstestprep.com>, establish a free login if you do not already have one, and register this book's practice tests using the registration code you just found. The process should take only a couple of minutes.

NOTE Amazon eBook (Kindle) customers: It is easy to miss Amazon's email that lists your PTP access code. Soon after you purchase the Kindle eBook, Amazon should send an email. However, the email uses very generic text and makes no specific mention of PTP or practice exams. To find your code, read every email from Amazon after you purchase the book. Also do the usual checks for ensuring your email arrives, such as checking your spam folder.

NOTE Other eBook customers: As of the time of publication, only the publisher and Amazon supply PTP access codes when you purchase their eBook editions of this book.

Customizing Your Exams

Once you are in the exam settings screen, you can choose to take exams in one of three modes:

- **Study mode:** Allows you to fully customize your exams and review answers as you are taking the exam. This is typically the mode you would use first to assess your knowledge and identify information gaps.
- **Practice Exam mode:** Locks certain customization options, as it is presenting a realistic exam experience. Use this mode when you are preparing to test your exam readiness.
- **Flash Card mode:** Strips out the answers and presents you with only the question stem. This mode is great for late-stage preparation when you really want to challenge yourself to provide answers without the benefit of seeing multiple-choice options. This mode does not provide the detailed score reports that the other two modes do, so you should not use it if you are trying to identify knowledge gaps.

In addition to these three modes, you will be able to select the source of your questions. You can choose to take exams that cover all of the chapters, or you can narrow your selection to just a single chapter or the chapters that make up specific parts in the book. All chapters are selected by default. If you want to narrow your focus to individual chapters, simply deselect all the chapters and then select only those on which you wish to focus in the Objectives area.

You can also select the exam banks on which to focus. Each exam bank comes complete with a full exam of questions that cover topics in every chapter. You can have the test engine serve up exams from all test banks or just from one individual bank by selecting the desired banks in the exam bank area.

There are several other customizations you can make to your exam from the exam settings screen, such as the time of the exam, the number of questions served up, whether to randomize questions and answers, whether to show the number of correct answers for

multiple-answer questions, and whether to serve up only specific types of questions. You can also create custom test banks by selecting only questions that you have marked or questions on which you have added notes.

Updating Your Exams

If you are using the online version of the Pearson Test Prep practice test software, you should always have access to the latest version of the software as well as the exam data. If you are using the Windows desktop version, every time you launch the software while connected to the Internet, it checks whether there are any updates to your exam data and automatically downloads any changes that were made since the last time you used the software.

Sometimes, due to many factors, the exam data may not fully download when you activate your exam. If you find that figures or exhibits are missing, you may need to manually update your exams. To update a particular exam you have already activated and downloaded, simply click the **Tools** tab and click the **Update Products** button. Again, this is an issue only with the desktop Windows application.

If you wish to check for updates to the Pearson Test Prep exam engine software, Windows desktop version, simply click the **Tools** tab and click the **Update Application** button. This ensures that you are running the latest version of the software engine.

This page intentionally left blank

Initial Configuration Settings on the Cisco Expressway

This chapter covers the following topics:

H.323 Settings: Explains the H.323 settings for the Cisco Expressway.

SIP and Domain Settings: Explains how to apply required SIP and domain settings for the Cisco Expressway.

Protocol Interworking on the Cisco Expressway: Focuses on interworking of H.323 and SIP signaling protocols via the Cisco Expressway.

Verifying Registration on the Cisco Expressway: Spotlights the registration process and verification of registration to the Cisco Expressway.

This chapter focuses on the initial configurations needed for the Cisco Expressway. It covers both the H.323 and SIP settings and includes interworking on the Expressway. You will also confirm these settings with the verification of registration.

This chapter covers the following objectives from the Implementing Cisco Collaboration Cloud and Edge Solutions (CLCEI) exam 300-820:

- 1.4.a Describe protocol interworking on the Expressway: SIP <-> H.323
- 1.4.b Describe protocol interworking on the Expressway: IPv4 and IPv6

“Do I Know This Already?” Quiz

The “Do I Know This Already?” quiz enables you to assess whether you should read this entire chapter thoroughly or jump to the “Exam Preparation Tasks” section. If you are in doubt about your answers to these questions or your own assessment of your knowledge of the topics, read the entire chapter. Table 3-1 lists the major headings in this chapter and their corresponding “Do I Know This Already?” quiz questions. You can find the answers in Appendix A, “Answers to the ‘Do I Know This Already?’ Quizzes and Review Questions.”

Table 3-1 “Do I Know This Already?” Section-to-Question Mapping

Foundation Topics Section	Questions
H.323 Settings	1
SIP and Domain Settings	2
Protocol Interworking on the Cisco Expressway	3–4
Verifying Registration on the Cisco Expressway	5–6

CAUTION The goal of self-assessment is to gauge your mastery of the topics in this chapter. If you do not know the answer to a question or are only partially sure of the answer, you should mark that question as wrong for purposes of the self-assessment. Giving yourself credit for an answer you correctly guess skews your self-assessment results and might provide you with a false sense of security.

1. Registration, Admission, and Status (RAS), which is used between an H.323 endpoint and a gatekeeper to provide address resolution and admission control services, uses which ITU-T recommendation?
 - a. H.320
 - b. H.225.0
 - c. H.245
 - d. H.264
2. Which of the following is considered a SIP URI? (Choose three.)
 - a. username@domain
 - b. 123username
 - c. username @domain.com
 - d. 8088675309
 - e. +18088675309
 - f. username@172.16.0.50
3. Which of the following is *not* an H.323 <-> SIP Interworking Mode setting on the Cisco Expressway?
 - a. Off
 - b. On
 - c. Registered only
 - d. Gateway
4. Calls that utilize the interworking functionality are considered what type of call?
 - a. Registered
 - b. Rich Media Session
 - c. B2B
 - d. Audio-only
5. When registering an endpoint to the Cisco Expressway, what functions are the devices registering to? (Choose two.)
 - a. SIP registrar
 - b. SIP AOR
 - c. H.323 gateway
 - d. H.323 gatekeeper
 - e. H.320 gatekeeper

6. Which of the following are able to register to the Cisco Expressway? (Choose three.)
- H.323 ID
 - SIP ZRTP
 - E.164 number
 - SIP URI
 - H.320 URI

Foundation Topics

H.323 Settings

As we move into the essential functions of the Cisco Expressway, we begin with the multi-media communications over the packet-based network. Deriving from the ITU Telecommunication Standardization Sector (ITU-T) **H.320** that was utilized over **Integrated Services Digital Network (ISDN)**-based networks, **H.323** was published by the **International Telecommunications Union (ITU)** in November 1996 with an emphasis on enabling videoconferencing capabilities over a local-area network (LAN), but was quickly adopted by the industry as a means of transmitting voice communication over a variety of IP networks, including wide-area networks (WANs) and the Internet. H.323 also provides a framework that uses other protocols to describe the actual protocol:

- **H.225.0: Registration, Admission, and Status (RAS)**, which is used between an H.323 **endpoint** and a **gatekeeper** to provide address resolution and admission control services
- **H.225.0**: Call signaling, which is used between any two H.323 entities to establish communication based on Q.931
- **H.245**: Control protocol for multimedia communication, describes the messages and procedures used for capability exchange, opening and closing logical channels for audio, video, data, and various control and indication signals
- **Real-time Transport Protocol (RTP)/Real-time Transport Control Protocol (RTCP)**: Protocols for sending or receiving multimedia information (voice, video, or text) between any two entities

The Cisco Expressway supports the H.323 protocol and it is also an H.323 gatekeeper. As an H.323 gatekeeper, the Expressway accepts registrations from H.323 endpoints and provides call control functions such as address translation and admission control. For an endpoint to use the Expressway as its H.323 gatekeeper or **SIP registrar**, the endpoint must first register with the Expressway.

To enable the Expressway as an H.323 gatekeeper, ensure that the H.323 Mode setting is set to On (**Configuration > Protocols > H.323**), as shown in Figure 3-1. H.323 mode is a powerful option that enables or disables functionality of the Cisco Expressway as an H.323 gatekeeper.

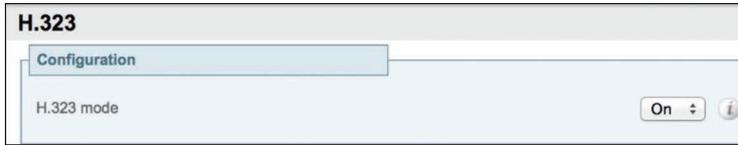


Figure 3-1 H.323 Mode

There are two ways an H.323 endpoint can locate an Expressway with which to register: manually or automatically. The option is configured on the endpoint itself under the Gatekeeper Discovery setting:

- If the mode is set to automatic, the endpoint tries to register with any Expressway it can find. It does this by sending out a Gatekeeper Discovery Request, to which eligible Expressways will respond.
- If the mode is set to manual, you must specify the IP address or the **fully qualified domain name (FQDN)** of the Expressway with which you want your endpoint to register, and the endpoint will attempt to register with that Expressway only.

You can prevent H.323 endpoints from being able to register automatically with the Expressway by disabling Auto Discovery on the Expressway (**Configuration > Protocols > H.323**).

While you are on the Configuration > Protocols > H.323 page, you can also configure the H.323 settings on the Expressway to fit your organization by utilizing Table 3-2 as a reference.

Table 3-2 H.323 Settings

Field	Description	Usage Tips
H.323 mode	Enables or disables H.323 on the Expressway. H.323 support is set to Off by default.	You must enable H.323 mode if you are clustering the Expressway, even if there are no H.323 endpoints in your deployment.
Registration UDP port	The listening port for H.323 UDP registrations.	The default Expressway configuration uses standard port numbers so you can use H.323 services out of the box without having to first set these up. The default port is 1719.
Registration conflict mode	Determines how the system behaves if an endpoint attempts to register an alias currently registered from another IP address. Reject: Denies the new registration. This is the default.	An H.323 endpoint may attempt to register with the Expressway using an alias that has already been registered on the Expressway from another IP address. The reasons for this could include: Two endpoints at different IP addresses are attempting to register using the same alias.

Field	Description	Usage Tips
	<p>Overwrite: Deletes the original registration and replaces it with the new registration.</p>	<p>A single endpoint has previously registered using a particular alias. The IP address allocated to the endpoint then changes, and the endpoint attempts to re-register using the same alias.</p> <p>Reject is useful if your priority is to prevent two users registering with the same alias.</p> <p>Overwrite is useful if your network is such that endpoints are often allocated new IP addresses, because it will prevent unwanted registration rejections.</p> <p>Note that in a cluster, a registration conflict is only detected if the registration requests are received by the same peer.</p>
Call signaling TCP port	The listening port for H.323 call signaling.	Default port: 1720.
Call signaling port range start and end	Specifies the port range used by H.323 calls after they are established.	The call signaling port range must be great enough to support all the required concurrent calls. Default start and end: 15000–19999.
Time to live	The interval (in seconds) at which an H.323 endpoint must re-register with the Expressway to confirm that it is still functioning. The default is 1800.	<p>Some older endpoints do not support the ability to periodically re-register with the system. In this case, and in any other situation where the system has not had a confirmation from the endpoint within the specified period, it will send an IRQ to the endpoint to verify that it is still functioning.</p> <p>Note that by reducing the registration time to live too much, you risk flooding the Expressway with registration requests, which will severely impact performance. This impact is proportional to the number of endpoints, so you should balance the need for occasional quick failover against the need for continuous good performance.</p>

Field	Description	Usage Tips
Call time to live	The interval (in seconds) at which the Expressway polls the endpoints in a call to verify that they are still in the call. The default is 120.	If the endpoint does not respond, the call is disconnected. The system polls endpoints in a call, whether the call type is traversal or non-traversal.
Auto discover	Determines whether the Expressway responds to Gatekeeper Discovery Requests sent out by endpoints. The default is On.	To prevent H.323 endpoints being able to register automatically with the Expressway, set Auto Discover to Off. This means that endpoints can only register with the Expressway if their Gatekeeper Discovery setting is Manual and they have been configured with the Expressway's IP address or FQDN.
Caller ID	Specifies whether the prefix of the ISDN gateway is inserted into the caller's E.164 number presented on the destination endpoint.	Including the prefix allows the recipient to directly return the call.

SIP and Domain Settings

Session Initiation Protocol (SIP) is an ASCII-based, application-layer control protocol that can be used to establish, maintain, and terminate calls between two or more endpoints. SIP is an alternative protocol developed by the Internet Engineering Task Force (IETF) for multimedia conferencing over IP. SIP was originally standardized with IETF **Request for Comments (RFC)** 2543, “SIP: Session Initiation Protocol,” published in March 1999. The current RFC 3261 (July 2002) makes the original RFC 2543 obsolete and has had many updates. The Cisco SIP implementation enables supported Cisco platforms to signal the setup of voice and multimedia calls over IP networks. SIP can be carried by several transport layer protocols including **Transmission Control Protocol (TCP)** and **User Datagram Protocol (UDP)**. SIP clients typically use TCP or UDP on port numbers 5060 or 5061 for SIP traffic to servers and other endpoints. Port 5060 is commonly used for nonencrypted signaling traffic, whereas port 5061 is typically used for traffic encrypted with Transport Layer Security (TLS). Normally SIP over UDP is not recommended because SIP messages for video systems are too large to be carried on a packet-based (rather than stream-based) transport.

Like other **Voice over IP (VoIP)** protocols, SIP is designed to address the functions of signaling and session management within a packet telephony network. Signaling allows call information to be carried across network boundaries. Session management provides the ability to control the attributes of an end-to-end call.

The Cisco Expressway supports SIP. It can act as a SIP registrar, as a SIP proxy, and as a SIP Presence Server. The Expressway can also provide **interworking** between SIP and H.323, translating between the two protocols to enable endpoints that only support one of the protocols to call each other.

To support SIP:

- SIP mode must be enabled.
- At least one of the SIP transport protocols (UDP, TCP, or TLS) must be active. Note that the use of UDP is not recommended for video because SIP message sizes are frequently larger than a single UDP packet.

For a SIP endpoint to be contactable via its alias, it must register its Address of Record (AOR) and its location with a SIP registrar. The SIP registrar maintains a record of the endpoint's details against the endpoint's AOR. The AOR is the alias through which the endpoint can be contacted; it is a SIP Uniform Resource Indicator (URI) and always takes the form *username@domain*. When a call is received for that AOR, the SIP registrar refers to the record to find its corresponding endpoint. (Note that the same AOR can be used by more than one SIP endpoint at the same time, although to ensure that all endpoints are found, they must all register with the same Expressway or Expressway cluster.)

A SIP registrar only accepts registrations for domains for which it is authoritative. The Expressway can act as a SIP registrar for up to 200 domains. To make the Expressway act as a SIP registrar, you must configure it with the SIP domains for which it will be authoritative. It will then handle registration requests for any endpoints attempting to register against that domain. Note that the Expressway will also accept registration requests where the domain portion of the AOR is either the FQDN or the IP address of the Expressway. Whether or not the Expressway accepts a registration request depends on its registration control settings.

In a Cisco Unified Communications deployment, endpoint registration for SIP devices may be provided by **Cisco Unified Communications Manager (Unified CM)**. In this scenario, the Expressway provides secure firewall traversal and line-side support for Unified CM registrations. When configuring a domain, you can select whether Unified CM or Expressway provides registration and provisioning services for the domain.

There are two ways a SIP endpoint can locate a registrar with which to register: manually or automatically. The option is configured on the endpoint itself under the SIP Server Discovery option (consult your endpoint user guide for how to access this setting; it may also be referred to as Proxy Discovery).

- If the Server Discovery mode is set to automatic, the endpoint sends a REGISTER message to the SIP server that is authoritative for the domain with which the endpoint is attempting to register. For example, if an endpoint is attempting to register with a URI of *john.smith@example.com*, the request will be sent to the registrar that is authoritative for the domain *example.com*. The endpoint can discover the appropriate server through a variety of methods including DHCP, Domain Name System (DNS), or provisioning, depending upon how the video communications network has been implemented.
- If the Server Discovery mode is set to manual, the user must specify the IP address or FQDN of the registrar (Expressway or Expressway cluster) with which the user wants to register, and the endpoint will attempt to register with that registrar only.

The Expressway is a SIP server and a SIP registrar:

- If an endpoint is registered to the Expressway, the Expressway will be able to forward inbound calls to that endpoint.
- If the Expressway is not configured with any SIP domains, the Expressway will act as a SIP server. It may proxy registration requests to another registrar, depending upon the SIP Registration Proxy Mode setting.

The Expressway acts as a SIP proxy server when SIP mode is enabled. The role of a proxy server is to forward requests (such as REGISTER and INVITE) from endpoints or other proxy servers on to further proxy servers or to the destination endpoint. If the Expressway receives a registration request for a domain for which it is not acting as a registrar (the Expressway does not have that SIP domain configured), then the Expressway may proxy the registration request onwards. This depends on the SIP Registration Proxy Mode setting, as follows:

- **Off:** The Expressway does not proxy any registration requests. They are rejected with a “403 Forbidden” message.
- **Proxy to known only:** The Expressway proxies the request in accordance with existing call processing rules, but only to known neighbor, traversal client, and traversal server zones.
- **Proxy to any:** This is the same as Proxy to Known Only but for all zone types (i.e., it also includes ENUM and DNS zones).

If the Expressway receives a proxied registration request, in addition to the Expressway’s standard registration controls, you can also control whether the Expressway accepts the registration depending upon the zone through which the request was received. You do this through the Accept Proxied Registrations setting when configuring a zone. Proxied registrations are classified as belonging to the zone they were last proxied from. This is different from non-proxied registration requests, which are assigned to a subzone within the Expressway.

The Expressway, as a SIP Presence Server, supports the SIP-based SIMPLE protocol. It can act as a Presence Server and Presence User Agent for any of the SIP domains for which it is authoritative. The Presence Server can manage the presence information for locally registered endpoints whose information has been received via a SIP proxy (such as another Expressway).

The SIP page (**Configuration > Protocols > SIP**) is used to configure SIP settings on the Expressway, including:

- SIP functionality and SIP-specific transport modes and ports
- Certificate revocation checking modes for TLS connections
- Registration controls for standard and outbound registrations

Table 3-3 outlines the configurable settings for enabling SIP functionality and for configuring the various SIP-specific transport modes and ports.

Table 3-3 SIP Settings

Field	Description	Usage Tips
SIP mode	Enables and disables SIP functionality (SIP registrar and SIP proxy services) on the Expressway. The default is Off.	This mode must be enabled to use either the Presence Server or the Presence User Agent.
SIP protocols and ports	The Expressway supports SIP over UDP, TCP, and TLS transport protocols. Use the Mode and Port settings for each protocol to configure whether incoming and outgoing connections using that protocol are supported and, if so, the ports on which the Expressway listens for such connections. The default modes are <ul style="list-style-type: none"> ■ UDP mode: Off ■ TCP mode: Off ■ TLS mode: On ■ Mutual TLS mode: Off 	At least one of the transport protocol modes must be set to On to enable SIP functionality. If you use both TLS and MTLS, Cisco recommends that you enable them on different ports. If you must use port 5061 for MTLS, you should avoid engaging the B2BUA, by switching Media Encryption mode to Auto on all zones in the call path.
TCP outbound port start/end	The range of ports the Expressway uses when TCP and TLS connections are established.	The range must be sufficient to support all required concurrent connections.
Session refresh interval	The maximum time allowed between session refresh requests for SIP calls. The default is 1800 seconds.	This is the time period after processing a request for which any session-stateful proxy must retain its state for this session.
Minimum session refresh interval	The minimum value the Expressway will negotiate for the session refresh interval for SIP calls. Default is 500 seconds.	This is the time period after processing a request for which any session-stateful proxy must retain its state for this session.
TLS handshake timeout	The timeout period for TLS socket handshake. The default is 5 seconds.	You might want to increase this value if TLS server certificate validation is slow (e.g., if OCSP servers do not provide timely responses) and thus cause connection attempts to timeout.
Certificate revocation checking mode	Controls whether revocation checking is performed for certificates exchanged during SIP TLS connection establishment.	Cisco recommends enabling revocation checking.

The Domains page (**Configuration > Domains**) lists the SIP domains managed by this Expressway. A domain name can comprise multiple levels. Each level's name can only contain letters, digits, and hyphens, with each level separated by a period (dot). A level name cannot start or end with a hyphen, and the final level name must start with a letter. An example valid domain name is *100.example-name.com*. You can configure up to 200 domains. (Note that you cannot configure domains on an Expressway-E.)

When the Expressway-C has been enabled for Unified Communications mobile and remote access, you must select the services that each domain will support. The options are as follows:

- **SIP registrations and provisioning on Expressway:** The Expressway is authoritative for this SIP domain. The Expressway acts as a SIP registrar for the domain (and Presence Server in the case of Video Communication Server (VCS) systems) and accepts registration requests for any SIP endpoints attempting to register with an alias that includes this domain. The default is On.
- **SIP registrations and provisioning on Unified CM:** Endpoint registration, call control, and provisioning for this SIP domain are serviced by Unified CM. The Expressway acts as a Unified Communications gateway to provide secure firewall traversal and line-side support for Unified CM registrations. The default is Off.
- **IM and Presence Service:** Instant messaging and presence services for this SIP domain are provided by the Unified CM **Instant Messaging and Presence (IMP)** service. The default is Off.
- **XMPP federation:** Enables **Extensible Messaging and Presence Protocol (XMPP)** federation between this domain and partner domains. The default is Off.
- **Deployment:** Associates the domain with the selected deployment, if there are multiple deployments. This setting is absent if there is only one deployment (there is always at least one).

Any domain configuration changes, when one or more existing domains are configured for IM and Presence services on Unified CM or XMPP federation, will result in an automatic restart of the **Universal Measurement and Calibration Protocol (XCP)** router on both Expressway-C and Expressway-E.

Protocol Interworking on the Cisco Expressway

The Interworking page (**Configuration > Protocols > Interworking**) lets you configure whether or not the Expressway acts as a gateway between SIP and H.323 calls. The translation of calls from one protocol to the other is known as *interworking*.

By default, the Expressway acts as a SIP–H.323 and H.323–SIP gateway but only if at least one of the endpoints that are involved in the call is locally registered. You can change this setting so that the Expressway acts as a SIP–H.323 gateway regardless of whether the endpoints involved are locally registered. You also have the option to disable interworking completely.

The options for the H.323 <-> SIP Interworking Mode setting are as follows:

- **Off:** The Expressway does not act as a SIP–H.323 gateway.
- **Registered only:** The Expressway acts as a SIP–H.323 gateway but only if at least one of the endpoints is locally registered.
- **On:** The Expressway acts as a SIP–H.323 gateway regardless of whether the endpoints are locally registered.



Cisco recommends that you leave this setting as Registered Only. Unless your network is correctly configured, setting it to On (where all calls can be interworked) may result in unnecessary interworking, for example, where a call between two H.323 endpoints is made over SIP, or vice versa.

Calls for which the Expressway acts as a SIP to H.323 gateway are **Rich Media Session (RMS)** calls. The Expressway always takes the media for SIP–H.323 interworked calls so that it can independently negotiate payload types on the SIP and H.323 sides, and Expressway will rewrite these as the media passes. Also, in a SIP SDP negotiation, multiple codec capabilities can be agreed (more than one video codec can be accepted) and the SIP device is at liberty to change the codec it uses at any time within the call. If this happens, because Expressway is in the media path, it will close and open logical channels to the H.323 device as the media changes (as required) so that media is passed correctly.

When searching a zone, the Expressway first performs the search using the protocol of the incoming call. If the search is unsuccessful, the Expressway may then search the zone again using the alternative protocol, depending on where the search came from and the H.323 <-> SIP Interworking Mode setting. Note that the zone must also be configured with the relevant protocols enabled (SIP and H.323 are enabled on a zone by default).

- If the request has come from a neighboring system and Interworking Mode is set to Registered Only, the Expressway searches the Local Zone using both protocols, and all other zones using the native protocol only (because it will interwork the call only if one of the endpoints is locally registered).
- If Interworking Mode is set to On, or the request has come from a locally registered endpoint, the Expressway searches the Local Zone and all external zones using both protocols.

SIP endpoints can only make calls in the form of URIs, such as *name@domain*. If the caller does not specify a domain when placing the call, the SIP endpoint automatically appends its own domain to the number that is dialed. If you dial 123 from a SIP endpoint, the search will be placed for *123@domain*. If the H.323 endpoint being dialed is just registered as 123, the Expressway will not be able to locate the alias *123@domain* and the call will fail. The solution is to do either of the following:

- Ensure all your endpoints, both H.323 and SIP, register with an alias in the form *name@domain*.
- Create a pre-search transform on the Expressway that strips the *@domain* portion of the alias for those URIs that are in the form of *number@domain*.

You will dive into pre-search Transforms in Chapter 7, “Cisco Expressway Call Processing Order,” for more depth on how to accomplish this.

For SIP calls, the Expressway implements RFC 4733 (obsoletes RFC 2833) for **dual-tone multifrequency (DTMF)** signaling in RTP payloads. For H.323 calls, the Expressway implements H.245 **UserInputIndication** for DTMF signaling. **dtmf** is the only supported **User InputCapability**. Expressway does not support any other H.245 user input capabilities (e.g., **basicString**, **generalString**). When the Expressway is interworking a call between SIP and

H.323, it also interworks the DTMF signaling, but only between RFC 4733 DTMF and the H.245 user input indicators `dtmf` and `basicString`.



The Expressway can also act as a gateway for calls between IPv4 and IPv6 devices. To enable this feature, select Both for the IP protocol on the IP page (**System > Network Interfaces > IP**). Calls for which the Expressway is acting as an IPv4 to IPv6 gateway are traversal calls and require a Rich Media Session license.

Verifying Registration on the Cisco Expressway

For an endpoint to use the Expressway as its H.323 gatekeeper or SIP registrar, the endpoint must first register with the Expressway. The Expressway can be configured to control which devices are allowed to register with it by using the following mechanisms:

- A device authentication process based on the username and password supplied by the endpoint
- A registration restriction policy that uses either Allow Lists or Deny Lists or an external policy service to specify which aliases can and cannot register with the Expressway
- Restrictions based on IP addresses and subnet ranges through the specification of subzone membership rules and subzone registration policies

You can use these mechanisms together. For example, you can use authentication to verify an endpoint's identity from a corporate directory and use registration restriction to control which of those authenticated endpoints may register with a particular Expressway. You can also control some protocol-specific behavior, including:

- The Registration Conflict Mode and Auto Discover settings for H.323 registrations
- The SIP registration proxy mode for SIP registrations

In a Cisco Unified CM deployment, endpoint registration for SIP devices may be provided by Unified CM. In this scenario, the Expressway provides secure firewall traversal and line-side support for Unified CM registrations. When configuring a domain, you can select whether Unified CM or Expressway provides registration and provisioning services for the domain.

H.323 systems such as gateways, multipoint control units (MCUs), and content servers can also register with an Expressway. They are known as locally registered services. These systems are configured with their own prefix, which they provide to the Expressway when registering. The Expressway then knows to route all calls that begin with that prefix to the gateway, MCU, or content server as appropriate. These prefixes can also be used to control registrations. SIP devices cannot register prefixes. If your dial plan dictates that a SIP device should be reached via a particular prefix, then you should add the device as a neighbor zone with an associated Search Rule using a pattern match equal to the prefix to be used.

When registering, the H.323 endpoint presents the Expressway with one or more of the following:



- **H.323 IDs**
- E.164 aliases
- URIs

Users of other registered endpoints can then call the endpoint by dialing any of these aliases. Note the following recommendations:

- Register your H.323 endpoints using a URI. This facilitates interworking between SIP and H.323, as SIP endpoints register using a URI as standard.
- Do not use aliases that reveal sensitive information. Due to the nature of H.323, call setup information is exchanged in an unencrypted form.

When registering, the SIP endpoint presents the Expressway with its contact address (IP address) and logical address (Address of Record). The logical address is considered to be its alias and generally is in the form of a URI.

An endpoint may attempt to register with the Expressway using an alias that is already registered to the system. How this is managed depends on how the Expressway is configured and whether the endpoint is SIP or H.323:

- **H.323:** An H.323 endpoint may attempt to register with the Expressway using an alias that has already been registered on the Expressway from another IP address. You can control how the Expressway behaves in this situation by configuring the Registration Conflict Mode setting on the H.323 page (**Configuration > Protocols > H.323**).
- **SIP:** A SIP endpoint will always be allowed to register using an alias that is already in use from another IP address. When a call is received for this alias, all endpoints registered using that alias will be called simultaneously. This SIP feature is known as *forking*.

All endpoints must periodically re-register with the Expressway to keep their registration active. If you do not manually delete the registration, the registration could be removed when the endpoint attempts to re-register, but this depends on the protocol being used by the endpoint:

- H.323 endpoints may use “light” re-registrations that do not contain all the aliases presented in the initial registration, so the re-registration may not get filtered by the restriction policy. If this is the case, the registration will not expire at the end of the registration timeout period and must be removed manually.
- SIP re-registrations contain the same information as the initial registrations, so they will be filtered by the restriction policy. This means that, after the list has been activated, all SIP registrations will disappear at the end of their registration timeout period.

The frequency of re-registrations is determined by the Registration Controls setting for SIP (**Configuration > Protocols > SIP**) and the Time to Live setting for H.323 (**Configuration > Protocols > H.323**).

Check that all endpoints that are expected to be registered are actually registered to the relevant Expressway and that they are registering the expected aliases. All successfully registered endpoints are listed on **Status > Registrations > By Device**. If the expected endpoints are not registered, review the following items:

- The endpoint's registration configuration. Is it configured to register with the Expressway-E if located on the external network/Internet, and to register with the Expressway-C if located on the internal network?
- The SIP domains.
- Any registration restriction configuration applied to the Expressway.

In some cases, home endpoints may fail to register when using **Service (SRV) records**. This can happen if the endpoint uses the home router for its DNS server and the router's DNS server software doesn't support SRV records lookup. (This also applies to the DNS server being used by a PC when Jabber Video is running on it.) If registration failure occurs, do either of the following:

- Change the DNS server on the endpoint to use a publicly available DNS server that can resolve SRV record lookups; for example, Google - 8.8.8.8.
- Change the SIP server address on the endpoint to use the FQDN of a node in the Expressway cluster and not the cluster SRV record, so that the device performs an AAAA or A record lookup.

Exam Preparation Tasks

As mentioned in the section "How to Use This Book" in the Introduction, you have a couple of choices for exam preparation: the exercises here, Chapter 22, "Final Preparation," and the exam simulation questions in the Pearson Test Prep Software Online.

Review All Key Topics

Review the most important topics in this chapter, noted with the Key Topics icon in the outer margin of the page. Table 3-4 lists a reference of these key topics and the page number on which each is found.



Table 3-4 Key Topics for Chapter 3

Key Topic Element	Description	Page Number
List	Interworking modes	55
Paragraph	IPv4 to IPv6 interworking	57
List	Registration aliases	58

Complete Tables and Lists from Memory

There are no memory tables or lists for this chapter.

Define Key Terms

Define the following key terms from this chapter and check your answers in the glossary:

Cisco Unified Communications Manager (Unified CM), dual-tone multifrequency (DTMF), E.164, endpoint, Extensible Messaging and Presence Protocol (XMPP), fully qualified domain name (FQDN), gatekeeper, H.225.0, H.245, H.320, H.323, H.323 ID, Instant Messaging and Presence (IMP), Integrated Services Digital Network (ISDN), International Telecommunications Union (ITU), interworking, Registration, Admission, and Status (RAS), Request for Comments (RFC), Rich Media Session (RMS), Service record (SRV), SIP registrar, Transmission Control Protocol (TCP), Universal Measurement and Calibration Protocol (XCP), User Datagram Protocol (UDP), Voice over IP (VoIP)

Q&A

The answers to these questions appear in Appendix A. For more practice with exam format questions, use the Pearson Test Prep practice test software.

1. Define the ITU-T H.323 standard and its core protocols.
2. What are the option modes of interworking on the Cisco Expressway and what do they imply?



Index

Symbols

* (asterisk), 64, 119
\
^ (caret), 65, 119
\$ (dollar sign), 65
... (ellipses), 65
(?! (negative lookahead), 65
(?<! (negative lookbehind), 65
. (period)
 in domain names, 54, 292
 in regular expressions, 64
| (pipe symbol), 65
? (question mark), 64
[] (square brackets), 64, 119
(.*) syntax, 120
[^] syntax, 65
(.) syntax, 65
{n} syntax, 64
{n,m} syntax, 64
300–820 Implementing Cisco
 Collaboration Cloud and Edge
 Solutions (CLCEI) exam
 customizing, 456–457
 final preparation for, 454–458
 exam customization, 456–457
 exam updates, 457
 final review/study, 458
 Pearson Test Prep software,
 455–456
 test-taking tips, 454

Premium Edition, 457

updating, 457

401 Unauthorized error, 294

403 Forbidden error, 295

404 errors, 295

407 Proxy Authentication Required
error, 295

500 Internal Server Error, 295

502 error, 295

A

A option (DNS Lookup), 230

A records (DNS), 200, 251

AAAA option (DNS Lookup), 230

Accept Proxied Registrations setting
(SIP), 53

accounts

 Cisco Webex Hybrid Calendar Service

impersonation accounts,
 348–349

service accounts, 348

 emergency, 74

 Smart Accounts, 14–15

Acknowledgement messages (DHCP), 6

ACLs (access control lists), 122

ACME (Automated Certificate
Management Environment), 75

Active Directory (AD), 102

 ADCS (Active Directory Certificate
 Services), 262

- configuration and synchronization, 326–338
 - AD LDS (Active Directory Lightweight Directory Services)*, 322–323
 - avatar synchronization*, 332–333
 - Cisco Directory Connector automatic upgrades*, 329
 - enabling*, 326–327
 - full synchronization*, 335–338
 - incremental synchronization*, 335
 - LAN Settings*, 327–329
 - notifications*, 334–335, 337–338
 - Object Selection*, 329–330
 - overview of*, 318–319
 - room information synchronization*, 333–334
 - User Attribute Mapping*, 330–332
- Active Directory Certificate Services (ADCS), 262
- Active Message Service Users status (Hybrid Message Service), 398
- AD. *See* Active Directory (AD)
- ADAuthLevel setting, 327
- ADCS (Active Directory Certificate Services), 262
- Add Marker command, 288
- Additional Recording Storage privilege (Cisco Webex), 338
- Address of Record (AOR), 52, 204
- addresses
 - IP (Internet Protocol), 216
 - IPv4 (Internet Protocol version 4)*, 109–110, 182
 - IPv6 (Internet Protocol version 6)*, 182
 - LAN (local-area network), 212
 - MAC (Media Access Control), 28
- Administration command (System menu), 34, 232
- Administrative XML Web Service (AXL), 386
- administrator authentication, 80–90
 - Advanced Security, 81–84
 - changes and limitations to standard Expressway functionality*, 83–84
 - disabling*, 84
 - enabling*, 83
 - HTTP methods*, 81–83
 - FIPS140–2 cryptographic mode, 84–87
 - enabling*, 85–87
 - overview of*, 84–85
 - SSH (Secure Shell) configuration, 81
- Administrator Policy. *See* Call Policy
- Admission Confirmation (ACF), 9
- Admission Reject (ARJ), 9
- Admission Request (ARQ), 9, 116–117
- Advanced Encryption Standard (AES), 70
- Advanced Networking, 4, 39–42
- Advanced Security, 81–84
 - changes and limitations to standard Expressway functionality*, 83–84
 - disabling*, 84
 - enabling*, 83
 - HTTP methods*, 81–83
- Advanced Security command (Maintenance menu), 81, 83, 84, 85
- AEAD (Authentication Encryption with Associated Data), 70
- AES (Advanced Encryption Standard), 70
- alarms, 235. *See also* errors
 - Cisco Webex Hybrid Message Service, 397

- MRA (Mobile and Remote Access), 287
 - viewing, 235
- Alarms command (Status menu), 235, 287, 397
- ALGs (Application Layer Gateways), 198
- Alias Pattern Match, 111
- aliases
 - Alias Pattern Match, 111
 - E.164, 8, 58, 95, 200–201
 - transformation, regular expressions with, 64
- All option (DNS Lookup), 230
- All Zones setting (Search Rules), 155
- Allow lists (HTTP)
 - configuration for MRA (Mobile and Remote Access), 270–273
 - automatically added rules*, 276–277
 - manually added rules*, 277–278
 - overview of*, 274–275
 - uploaded rules*, 278
 - policies, 97
 - regular expressions with, 64
- Any setting (Search Rules), 155
- AOR (Address of Record), 52, 204
- API (application programming interface) integration, 300–301
 - Active Directory (AD), 318–319
 - administrator access, 82
 - AXL (Administrative XML Web Service), 266, 386, 410
 - Google Calendar deployment in the cloud, 362
 - IM&P (IM and Presence), 394
- API controls command (Security menu), 363
- Application Awareness, 41
- Application Layer Gateways (ALGs), 198
- application programming interfaces. *See* API (application programming interface) integration
- Application User menu commands (User Management menu), 394
- ApplicationImpersonation privileges, 349
- Applications menu commands, Hybrid Services, 355, 356, 392
- architecture
 - Cisco Jabber
 - cloud deployments*, 446–447
 - hybrid deployments*, 447–450
 - Cisco Webex Hybrid Calendar Service, 3451
 - Google Calendar deployment in the cloud, 362–363
 - Webex Video Mesh
 - geographic distribution*, 442
 - geographic distribution with SIP dialing*, 443
 - hub-and-spoke*, 442
 - Webex Video Mesh cascade, 439–440
- ARJ (Admission Reject), 9
- ARQ (Admission Request), 9, 116–117
- ASNs (Autonomous System Numbers), 419
- Assent, 153, 188–189
- asterisk (*), 64, 119
- asymmetric cryptography, 255
- asymmetric networks
 - ICE (Interactive Connectivity Establishment) in, 186
 - STUN (Session Traversal Utilities for NAT) in, 183–184
- Audio, Webex Edge, 418. *See also* Video Mesh (Webex)

- overview of, 418
 - Webex Edge Connect, 418–420
 - authentication**
 - administrator, 80–90
 - Advanced Security*, 81–84
 - FIPS140–2 cryptographic mode*, 84–87
 - SSH (Secure Shell) configuration*, 81
 - Authentication Encryption with Associated Data (AEAD), 70
 - versus authorization, 73–74
 - Call Policy, 125
 - certificate-based, 73–74
 - emergency accounts*, 74
 - enabling*, 73
 - overview of*, 73
 - username, obtaining from certificate*, 74
 - initial configuration settings, 221
 - MRA (Mobile and Remote Access), 291
 - MTLS (Mutual TLS), 241, 242
 - registration, 101–106
 - configuration*, 101–106
 - definition of*, 100
 - encryption standards*, 101
 - Registration Authentication, 101–106
 - configuration*, 101–106
 - definition of*, 100
 - encryption standards*, 101
 - Authentication Encryption with Associated Data (AEAD)**, 70
 - Authentication menu commands**
 - Devices, 102
 - Local Database, 278
 - authorization, authentication versus**, 73–74
 - Auto discover field (H.323 configuration)**, 51
 - Auto Discovery**
 - disabling, 49
 - enabling, 358
 - auto encryption policies**, 71–72
 - Automated Certificate Management Environment (ACME)**, 75
 - Automated Detection menu commands**
 - Blocked Addresses, 292
 - Configuration, 293, 295
 - automatic CRL updates**, 76–77
 - Automatic Inbound Rules command (HTTP Allow List menu)**, 275
 - Automatic Outbound Rules command (HTTP Allow List menu)**, 275
 - Automatically upgrade to the new Cisco Directory Connector Version setting**, 329
 - Autonomous System Numbers (ASNs)**, 419
 - Avatar command (Configuration menu)**, 332
 - avatar synchronization, Active Directory**, 332–333
 - AXL (Administrative XML Web Service) API**, 266, 386, 410
-
- B
- B2B (business-to-business) collaboration solutions**, 214
 - bandwidth management, 137
 - calls
 - bandwidth management*, 137
 - Expressway clusters for*, 214
 - compatibility of, 30
 - DNS Zones for, 199–204
 - DNS settings*, 201–202
 - ENUM Zones*, 200

- internal call routing*, 199–200
- A records*, 202–204
- SRV (Service) records*, 204
- Expressway clusters for, 214
- Expressway Media Traversal, 187
 - Assent and H.460.18/19*, 188–189
 - Traversal Zone configuration*, 189–196
 - Traversal Zone deployment scenarios*, 196–199
- firewall issues, 181
- ICE (Interactive Connectivity Establishment), 183, 186
- licensing for, 15
- NAT (Network Address Translation)
 - issues, 181
 - overview of, 178
- STUN (Session Traversal Utilities for NAT), 183–184
- troubleshooting
 - additional tools for*, 234–237
 - alarms*, 235–236
 - bandwidth monitoring logs*, 234
 - calling issues*, 225–229
 - certificate issues*, 232–234
 - Configuration Log*, 235
 - Diagnostic Logging tool*, 236–237
 - DNS issues*, 230–232
 - overview of*, 218–219
 - registration issues*, 220–225
- TURN (Traversal Using Relay NAT), 183, 184–186
 - configurable options for*, 185–186
 - operation within symmetric networks*, 184
- B2BUA (back-to-back user agent)**, 71–72, 197, 289
- B2C (business-to-consumer) collaboration solutions**, 15, 137
- backslash (\), 65
- back-to-back user agent (B2BUA), 71–72, 197, 289
- Backup and Restore command (Maintenance menu)**, 42, 43
- Backup and Restore page**, 42–44
 - backup process, 42–43
 - encryption, 42
 - password protection, 42
 - restore process, 43–44
- Bandwidth command (Status menu)**, 234
- bandwidth management**, 116–117
 - bandwidth monitoring logs, 234
 - Links and Pipes, 140–145
 - benefits of*, 140
 - call control using*, 145–146
 - definition of*, 140
 - one Pipe, one Link*, 141
 - one Pipe, two or more Links*, 141–142
 - Pipe configuration*, 144–145
 - troubleshooting tips*, 234
 - two Pipes, one Link*, 142–144
 - when to use*, 140–141
 - overview of, 134
 - Subzone, 136–139
 - Downspeed Mode settings*, 138–139
 - Local Zone settings*, 139–140
 - per-call restrictions*, 136–137
 - restriction modes*, 137
 - total-bandwidth restrictions*, 136–137

Bandwidth menu commands
 Configuration, 138
 Links, 144, 234
 Pipes, 144, 234

bandwidth monitoring logs, 234

Base 64 Encoded option, 264

best effort encryption policies, 71–72

BFCP (Binary Floor Control Protocol), 295

BGP (Border Gateway Protocol), 419

Binary Floor Control Protocol (BFCP), 295

Bind to a New Domain command, 328

Blocked Addresses command (Automated Detection menu), 292

Blocked Addresses list, 292

Border Gateway Protocol (BGP), 419

bring-your-own-device (BYOD), 4

business-to-business collaboration.
See B2B (business-to-business) collaboration solutions

business-to-consumer (B2C), 15, 137

By Alias command (Registration menu), 222

By Device command (Registration menu), 98, 222

BYOD (bring-your-own-device), 4

C

CAC (Call Admission Control), 7

calendar, TMS (Telepresence Management Suite), 408

Calendar Service, Cisco Webex Hybrid, 311
 Expressway-Based Calendar Connector, 345–354
architecture, 3451
Expressway-C preparation checklist, 350–354
HTTPS connection, 3450
impersonation accounts, 348–349
prerequisites, 349–350
service accounts, 348
throttling policy, 354
TMS (Telepresence Management Suite), 347

Google Calendar deployment in the cloud, 362–367
architecture, 362–363
Cisco Webex users, enabling, 364–365
Default Language setting, 364
enabling and configuring, 363–364
testing and verification, 367
User Email Notifications, 365
workspaces, adding devices to, 365–367

Hybrid Calendar Service deployment, 354–362
Cisco Conferencing Services Configuration, 359–360
Cisco Webex users, enabling, 361–362
Connector Management, 361
Connector Proxy settings, 355–356
Default Language setting, 360
Microsoft Exchange Configuration, 357–359
Trusted CA Certificate, 356–357

OBTP (One Button to Push), 347, 374–377
device registration, 374–375
workspaces, adding devices to, 375–376

Office 365, 368–374
Default Language setting, 372

- hybrid Exchange environments*, 370
 - Microsoft Graph API*, 368
 - permissions*, 368
 - requirements*, 369
 - scheduling flow*, 371
 - setup process*, 372
- operation of, 344–345
- overview of, 342
- Call Activity command (Resources menu)**, 434
- Call Admission Control (CAC)**, 7
- call control, with Pipes, 145–146
- Call Details page**, 229
- Call History page**, 289
- Call Loop Detection Mode**, 160
- Call Policy**, 122–128
 - ACLs compared to, 122
 - Call Processing Language (CPL) Script, 122–123
 - configuration, 124–128
 - definition of, 122
 - priority of, 123–124
 - rules, 124–128
- Call Policy command (Configuration menu)**, 124
- Call Policy menu commands**
 - Configuration, 124
 - Rules, 124
- Call Processing Language (CPL)**, 64, 98, 122–123
- Call Processing Order**. *See also* **bandwidth management**
 - Call Policy, 122–128
 - ACLs compared to*, 122
 - definition of*, 122
 - components of, 225–226
 - definition of, 136
 - illustrated flow of, 116–117
- Locate tool, 132
- overview of, 114
- Search History, 131
- Transforms, 116–121
 - configuration of*, 118–121
 - definition of*, 117–118
 - example of*, 118–121
 - Pre-Search*, 117
 - Search Rule*, 117
- User Policy (FindMe), 128–130
- Zone search, 116
- Call Routing command (Configuration menu)**, 164
- Call Routing menu commands**
 - Route Hunt, 174
 - SIP Route Pattern, 174
- Call Service, Cisco Webex Hybrid**, 311–312
- call setup process**
 - Call Setup Mode, 9
 - H.323 protocol, 9–10
 - SIP (Session Initiation Protocol), 7–8
- Call Signaling Optimization**, 164
- Call signaling port range start and end field (H.323 configuration)**, 50
- Call signaling TCP port field (H.323 configuration)**, 50
- call status information, 289–290
- Call Status page**, 289
- Call time to live field (H.323 configuration)**, 51
- Caller ID field (H.323 configuration)**, 51
- Calling, Webex**, 309–310
- Calling, Webex Edge for**, 417–418
- calling issues, troubleshooting for B2B collaboration solutions, 225–229

- Call Processing Order, 225–226
- Calls logs, 229
- Locate tool, 227–228
- Network Log, 229
- Search History tool, 226–227
- Calls command (Calls menu), 229, 289
- Calls logs, 229
- Calls menu commands
 - Calls, 289
 - History, 229, 289
- “Cannot communicate with the server” error, 294
- Capabilities Exchange (CapEx), 10
- capacity licenses, 210–211
- caret (^), 65, 119
- CAS (Central Authentication Service), 449
- CAs (certificate authorities), 72, 254, 345
 - Cisco Jabber deployments with, 449
 - for Cisco Webex Hybrid Message Service, 391–392
 - IdenTrust Commercial Root CA 1, 416–417
- CAS (Client Access server), 347
- cascade architecture, Webex Video Mesh, 439–440
- cascade link, Webex Video Mesh, 438–439
- CCNP and CCIE Collaboration CLCOR 350–801 Official Cert Guide (Cisco Press), 7
- CDP (Cisco Delivery Protocol), 6, 76
- CE (Collaboration Endpoint), 6, 240, 406
- CE1200 platform, Cisco Expressway license limitations for, 21
- Central Authentication Service (CAS), 449
- CER (Cisco Emergency Responder), 304
- certificate authorities. *See* CAs (certificate authorities)
- Certificate Management command (Security menu), 292
- Certificate revocation checking mode field (SIP configuration), 54
- Certificate Revocation settings, 78–80
- certificate signing requests (CSRs), 72, 262–263, 292
- Certificate Validation status (Hybrid Message Service), 398
- Certificate verification mode field (Policy Service), 99
- Certificate-based Authentication Configuration command (Security menu), 73
- Certificate-based Authentication Configuration page, 233
- certificates
 - ACME (Automated Certificate Management Environment), 75
 - CAs (certificate authorities), 72, 254, 345
 - Cisco Jabber deployments with, 449*
 - for Cisco Webex Hybrid Message Service, 391–392*
 - IdenTrust Commercial Root CA 1, 416–417*
 - certificate-based authentication, 73–74
 - authentication versus authorization, 73–74*
 - emergency accounts, 74*
 - enabling, 73*
 - overview of, 73*
 - username, obtaining from certificate, 74*

- for Cisco Webex Hybrid Message Service, 392
- for Cisco Webex Messenger, 449
- Client Certificate Testing, 74
- CRLs (certificate revocation lists), 72, 76–80
 - automatic CRL updates*, 76–77
 - Certificate Revocation settings*, 78–80
 - certificate revocation sources*, 76
 - manual CRL updates*, 77–78
 - OCSP (Online Certificate Status Protocol)*, 78
- CSRs (certificate signing requests), 72, 76, 262–263, 292
- domain, 88–90
 - for Expressway clusters, 76, 212
 - Expressway Server Certificate, 75–76
 - for Hybrid Calendar Service, 356–357
- LSC (Locally Significant Certificate), 255
- for MRA (Mobile and Remote Access) deployment, 241, 254–255
 - CAs (certificate authorities)*, 254
 - Cisco Expressway*, 254, 259
 - Cisco Unified CM*, 254, 259–261
 - classes of*, 258
 - creating*, 261–265
 - Domain Validation (DV)*, 258
 - Extended Validation (EV)*, 258
 - Organization Validation (OV)*, 258
 - overview of*, 254–255
 - root CA*, 254–255
 - table of*, 255
 - TLS Verify*, 254, 255–258, 259
 - troubleshooting*, 291–292
 - Trusted CA Certificates*, 265
- Unified CM Tomcat*, 254, 259–261
- OCSP (Online Certificate Status Protocol), 76
 - overview of, 72–73
- PKI (public key infrastructure), 251
- Subject Alternate Name list, 291
- troubleshooting for B2B collaboration solutions, 232–234
 - Client Certificate Testing tool*, 232–233
 - Secure Traversal Test tool*, 233–234
- Trusted CA Certificates, 74–75, 265, 273, 356–357, 391
- CEtcp prefix, 289
- CEtls prefix, 289
- Check Against the Following DNS Servers option, 230
- Check Credentials authentication policy, 168
- Check Pattern tool, 66–67
- CIDR notation, 110
- Cisco AXL Web Service setting (Cisco Unified Communications Manager), 244
- Cisco Cloud Onboarding, 245
- Cisco Collaboration Edge, 240.
 - See also* MRA (Mobile and Remote Access)
- Cisco Collaboration Endpoint. *See* CE (Collaboration Endpoint)
- Cisco Collaboration Flex Plan, 11, 13–14, 304
- Cisco Collaboration Meeting Rooms (CMR) Hybrid Configuration Guide*, 350
- Cisco Conferencing Services Configuration, 359–360
- Cisco Customer Success Manager (CSM), 440

- Cisco Delivery Protocol. *See* CDP (Cisco Delivery Protocol)
- Cisco Directory Connector, 323–325, 329, 385. *See also* Directory Service, Cisco Webex Hybrid
- Cisco DX70, 19
- Cisco Emergency Responder (CER), 304
- Cisco EX60, 19
- Cisco EX90, 19
- Cisco Expressway. *See also* multisite collaboration solutions
 - authentication, 221
 - bandwidth management
 - call control using Pipes*, 145–146
 - Links and Pipes*, 140–146
 - overview of*, 134
 - Subzone*, 136–139
 - Call Loop Detection Mode, 160
 - Call Processing Order
 - Call Policy*, 122–128
 - definition of*, 136
 - illustrated flow of*, 116–117
 - Locate tool*, 132
 - overview of*, 114
 - Search History*, 131
 - Transforms*, 116–121
 - User Policy (FindMe)*, 128–130
 - Zone search*, 116
 - certificates. *See* certificates
 - versus Cisco VCS licensing, 15–16
 - clustering
 - benefits of*, 210
 - Cisco Expressway Cluster Creation and Maintenance Deployment Guide*, 210
 - cluster registration and call capacity limitations*, 210
 - DNS (Domain Name System)
 - and*, 213–214
 - operation as one large local zone*, 212–213
 - overview of*, 208
 - redundancy with*, 210
 - requirements for*, 210–212
 - security certificates*, 212
 - server certificates*, 76
 - zones and*, 214–216
 - directory Expressways, 162
 - Expressway Media Traversal, 187
 - Assent and H.460.18/19*, 188–189
 - Traversal Zone configuration*, 189–196
 - Traversal Zone deployment scenarios*, 196–199
 - Expressway Series, 5
 - history and development of*, 240–241
 - launch of*, 240–241
 - versions of*, 240–241
 - Expressway Server Certificate, 75–76
 - Expressway to Cisco Unified CM Neighbor Zones, 169–176
 - compared to Expressway to Expressway Neighbor Zones*, 169
 - dialing rules*, 173–175
 - SIP route patterns*, 173–175
 - SIP trunk security profiles*, 170–171
 - SIP trunk settings*, 171–172
 - Transforms*, 175–176
 - Expressway to Expressway Neighbor Zones, 166–176
 - Authentication, Location, and Advanced Neighbor Zone menus*, 167–168

- H.323 and SIP Neighbor Zone menus*, 166
- Expressway-Based Calendar Connector, 345–354
 - architecture*, 345
 - Expressway-C preparation checklist*, 350–354
 - HTTPS connection*, 345
 - impersonation accounts*, 348–349
 - prerequisites*, 349–350
 - service accounts*, 348
 - throttling policy*, 354
 - TMS (Telepresence Management Suite)*, 347
- Expressway-based Calendar Connector, 345–354
 - architecture*, 345
 - Expressway-C preparation checklist*, 350–354
 - HTTPS connection*, 345
 - impersonation accounts*, 348–349
 - prerequisites*, 349–350
 - service accounts*, 348
 - throttling policy*, 354
 - TMS (Telepresence Management Suite)*, 347
- Expressway-C (Core) versus Expressway-E (Edge), 4
- H.323 on. *See* H.323 protocol
- initial configuration settings
 - Auto Discovery*, 49
 - H.323 settings*, 48–51
 - overview of*, 46
 - SIP (Session Initiation Protocol) settings*, 51–55
- interworking on, 51, 55–57
 - definition of*, 55
 - initial configuration of*, 55–57
 - licensing and*, 19–20
- licensing
 - Cisco Collaboration Flex Plan*, 11, 13–14
 - Cisco Expressway versus Cisco VCS*, 15–16
 - CUCL (Cisco User Connect Licensing)*, 11–13
 - CUWL (Unified Workspace Licensing)*, 11–13, 15
 - device-based versus user-based*, 5, 11
 - direct registration and*, 5
 - license consumption*, 17–21
 - license limitations*, 21
 - Option Key*, 15–16
 - overview of*, 11–15
 - PAK (Product Activation Key)*, 14
 - Release Key*, 16–17
 - Smart Licensing*, 14–15
- Mobile and Remote Access. *See* MRA (Mobile and Remote Access)
- MTLS (Mutual TLS), 241, 242, 259
- overview of, 2
- registration on. *See* registration
- RMS (Rich Media Session), 15, 56, 210, 289
- SIP (Session Initiation Protocol)
 - on. *See* SIP (Session Initiation Protocol)
- subzones, 106–112
 - creating*, 108–109
 - Default Subzone*, 107
 - Links*, 107
 - Local Zone*, 106–112
 - Membership Rules for*, 109–112
 - Traversal Subzone*, 107

- system configuration
 - Backup and Restore*, 42–44
 - Expressway deployment on VM*, 26–28
 - overview of*, 24
 - Service Setup Wizard through web interface*, 28–34
 - System Configuration settings*, 34–42
- troubleshooting. *See* troubleshooting
- Unified Communications
 - configuration on, 270–273
 - DNS settings*, 271–273
 - MRA-specific settings*, 270–271
 - overview of*, 270
 - Unified CM discovery settings*, 273
 - zones*, 273
- VCS to Expressway Migration, 4–5
- verification of registration on, 51–55
- versions of, 5
- virtualization of, 17–19
- Cisco Expressway Administrator Guide*, 32, 104, 122
- Cisco Expressway Basic Configuration Deployment Guide*, 390
- Cisco Expressway Certificate Creation and Use Deployment Guide*, 75, 90
- Cisco Expressway Cluster Creation and Maintenance Deployment Guide*, 210
- Cisco Expressway Media Traversal, 187
 - Assent and H.460.18/19, 188–189
 - Traversal Zone configuration, 189–196
 - authentication credentials*, 189–190
 - Traversal Client Zone*, 189, 193–196
 - Traversal Server Zone*, 189, 190–193
- Traversal Zone deployment scenarios, 196–199
 - dual NIC DMZ*, 197–198
 - single-subnet DMZ*, 196
 - three-port firewall DMZ*, 197
 - triple Expressway*, 198–199
- Cisco Expressway on Virtual Machine Installation Guide*, 28
- Cisco Expressway Series, 5
 - capabilities of, 5
 - history and development of, 240–241
 - launch of, 240–241
 - versions of, 240–241
- Cisco Expressway-C Connector Host, 345–354
 - architecture, 3451
 - Expressway-C preparation checklist, 350–354
 - HTTPS connection, 3450
 - impersonation accounts, 348–349
 - prerequisites, 349–350
 - service accounts, 348
 - throttling policy, 354
 - TMS (Telepresence Management Suite), 347
- Cisco Hosted Collaboration Solution (HCS), 300–302, 417
- Cisco Intercluster Lookup Service (ILS), 294
- Cisco Jabber, 4, 382
 - capabilities of, 303
 - deployment with Cisco Webex Messenger
 - certificate validation*, 449
 - Cisco Unified CM configuration*, 450–452

- Cisco Unity Connection (CUC)*, 447–449
- Cisco Webex Administration Tool*, 447
- cloud-based deployment architecture*, 446–447
- compatibility of*, 445
- CSV files, importing users from*, 447
- hybrid cloud-based deployment architecture*, 447–450
- monitoring with Cisco Webex Administration Tool*, 445
- On-Premises Deployment for Cisco Jabber*, 449
- overview of*, 444
- requirements of*, 445–450
- service discovery*, 449–450
- IM&P (IM and Presence) capabilities, 445
- MRA (Mobile and Remote Access) and, 240
- sign-in issues, troubleshooting, 292–294
- Cisco Nexus switching platforms, 302
- Cisco Options Package (COP), 386
- Cisco SAFE security reference architecture model, 301
- Cisco SD-WAN, 304
- Cisco Spark Calling, 309–310
- Cisco Technical Assistance Center (TAC), 287
- Cisco Telepresence endpoints, 6
- Cisco Telepresence Management Suite Extension for Microsoft Exchange Administrator Guide*, 350
- Cisco TelePresence Management Suite Provisioning Extension (TMSPE), 87
- Cisco TelePresence Management Suite (TMS), 6, 34, 213, 367
- Cisco Unified Border Element (CUBE), 20
- Cisco Unified Communications Manager IP Phone (CCMCIP), 449
- Cisco Unified Communications Manager (Unified CM), 52, 300, 301, 303–306, 406
- certificates, 254, 259–261
- configuration, 244–245, 266–269, 450–452
- configuration settings for, 241
 - diagnostic logs*, 288
 - overview of*, 284
 - status*, 287, 290
 - View Detailed MRA Authentication Statistics*, 291
- Expressway to Cisco Unified CM Neighbor Zones, 169–176
 - compared to Expressway to Expressway Neighbor Zones*, 169
 - dialing rules*, 173–175
 - SIP route patterns*, 173–175
 - SIP trunk security profiles*, 170–171
 - SIP trunk settings*, 171–172
 - Transforms*, 175–176
- MRA (Mobile and Remote Access) deployment, 270–273
 - DNS settings*, 271–273
 - MRA-specific settings*, 270–271
 - overview of*, 270
 - Unified CM discovery settings*, 273
 - zones*, 273
- overview of, 2
- phones, 240
- SIP registration, 52
- TLS (Transport Layer Security) with, 70

- Transforms for, 121
- Unified CM Certificate Authority
 - Proxy Function (CAPF) certificate, 255
- Unified CM Phone Security Profile
 - Names, 292
- Unified CM Tomcat certificates, 254, 259–261
- Cisco Unified Communications (UC), 300
- Cisco Unified Serviceability command, 266
- Cisco Unity Connection (CUC), 295, 447–449
- Cisco User Connect Licensing (CUCL), 11–13
- Cisco Validated Design (CVD), 301
- Cisco VCS Certificate Creation and Use Deployment Guide*, 262
- Cisco Video Communications Server. *See* VCS (Video Communications Server)
- Cisco Webex, 14, 310–313, 345, 382, 445
 - Administration Tool, 447
 - Assistant for Webex Meetings, 307
 - CAs (certificate authorities) for, 416–417
 - Cisco UCM (Unified Communications Manager) Cloud, 303–306
 - compatibility of, 29
 - components of, 306
 - Control Hub, 318, 416–417, 434
 - Control Hubs, 318, 383, 416–417
 - DLP (data loss prevention), 303
 - DX80, 15, 19
 - FedRAMP (Webex for Government), 408
 - Hybrid Calendar Service, 311
 - Expressway-Based Calendar Connector*, 345–354
 - Google Calendar deployment in the cloud*, 362–367
 - Hybrid Calendar Service deployment*, 354–362
 - OBTP (One Button to Push)*, 347, 374–377
 - Office* 365, 368–374
 - operation of*, 344–345
 - overview of*, 342
 - prerequisites for*, 349–350
- Hybrid Call Service, 311–312
- Hybrid Data Security Service, 312, 384
- Hybrid Directory Service, 311
 - Active Directory configuration and synchronization*, 318–319, 322–323, 326–338
 - deployment models*, 318–319
 - deployment requirements*, 319–321
 - infrastructure requirements*, 321–325
 - overview of*, 316
 - Webex user service assignment*, 338–340
- Hybrid Message Service, 312
 - certificates*, 392
 - deployment models*, 382–384
 - deployment requirements*, 385–388
 - Expressway connector registration to Cisco Webex cloud*, 392–394
 - Expressway requirements*, 388–391
 - IM&P (IM and Presence) configuration*, 394–396
 - management of*, 396–402

- overview of*, 380
- Message Free entitlement, 387
- Messenger, Cisco Jabber deployments with
 - certificate validation*, 449
 - Cisco Unified CM configuration*, 450–452
 - Cisco Unity Connection (CUC)*, 447–449
 - Cisco Webex Administration Tool*, 447
 - cloud-based deployment architecture*, 446–447
 - compatibility of*, 445
 - CSV files, importing users from*, 447
 - hybrid cloud-based deployment architecture*, 447–450
 - monitoring with Cisco Webex Administration Tool*, 445
 - On-Premises Deployment for Cisco Jabber*, 449
 - overview of*, 444
 - requirements of*, 445–450
 - service discovery*, 449–450
- overview of, 303
- users, enabling
 - for Google Calendar deployment in the cloud*, 364–365
 - for Hybrid Calendar Service*, 361–362
 - for Office 365*, 373–374
- Video Mesh. *See* Video Mesh (Webex)
- Webex Calling, 309–310
- Webex Edge solutions. *See* Cisco Webex Edge
- Webex Meetings, 306–308, 438
- Webex Messaging, 308–309
- Cisco Webex Device Connector, 408–411
- Cisco Webex DX80, 15, 19
- Cisco Webex Edge
 - overview of, 404
 - Video Mesh
 - capacity of*, 430–432
 - cluster deployment*, 435–440
 - integration with call control and meeting infrastructure*, 420–423
 - proxy solutions*, 429–430
 - system and platform requirements for*, 423–429
 - VMNLite call capacity benchmark*, 433–434
 - WebSocket connections*, 430
- Webex Edge Audio, 418. *See also* Video Mesh (Webex)
 - overview of*, 418
 - Webex Edge Connect*, 418–420
- Webex Edge Connect, 418–420
- Webex Edge for Calling, 417–418
- Webex Edge for Devices, 406–417
 - Cisco Webex Control Hub*, 413–416
 - Cisco Webex Device Connector*, 408–411
 - cloud onboarding and linking*, 411–412
 - features and functionality*, 406–407, 408–411
 - limitations*, 408
 - prerequisites*, 407
 - proxy server features*, 412–413
 - supported operating systems*, 407
 - URLs for on-premises device linking*, 413–416

- Webex Video Mesh. *See* Video Mesh (Webex)
- Cisco Webex Edge Audio Customer Configuration Guide*, 418
- Cisco Webex Meetings Security White Paper, 308
- CLI (command line interface), 37
- Client Access server (CAS), 347
- Client Certificate Testing, 74, 232–233
- Client Certificate Testing command (Security menu), 79, 232
- cloud collaboration
 - Cisco HCS (Hosted Collaboration Solution), 300–302
 - Cisco Hosted Collaboration Solution (HCS), 300–302, 417
 - Cisco Jabber, cloud deployments with Cisco Webex Messenger
 - architecture of*, 446–447
 - certificate validation*, 449
 - Cisco Unified CM configuration*, 450–452
 - Cisco Unity Connection (CUC)*, 447–449
 - Cisco Webex Administration Tool*, 447
 - CSV files, importing users from*, 447
 - requirements of*, 445–450
 - service discovery*, 449–450
 - Cisco Webex. *See* Cisco Webex
- CMR Cloud, 29
- Google Calendar deployment in the cloud, 362–367
 - architecture*, 362–363
 - Cisco Webex users, enabling*, 364–365
 - Default Language setting*, 364
 - enabling and configuring*, 363–364
 - testing and verification*, 367
 - User Email Notifications*, 365
 - workspaces, adding devices to*, 365–367
- overview of, 298, 300
- Clustering command (System menu), 352, 390
- clusters
 - Expressways
 - benefits of*, 210
 - Cisco Expressway Cluster Creation and Maintenance Deployment Guide*, 210
 - cluster registration and call capacity limitations*, 210
 - DNS (Domain Name System) and*, 213–214
 - licensing and*, 16
 - operation as one large local zone*, 212–213
 - overview of*, 208
 - redundancy with*, 210
 - requirements for*, 210–212
 - security certificates*, 212
 - server certificates and*, 76
 - zones and*, 214–216
 - Webex Video Mesh, 435–440
 - cascade architecture*, 439–440
 - cascade link*, 438–439
 - cluster selection for overflow*, 439–440
 - deployment task flow*, 440
 - documentation for*, 433
 - geographic distribution*, 442
 - geographic distribution with SIP dialing*, 443
 - guidelines for*, 435–436

- hub-and-spoke architecture*, 442
- node installation for*, 441–442
- on-premise and cloud calls*, 437–439
- overview of*, 435
- ports and protocols for Cisco Webex Meetings traffic*, 438
- ports and protocols for management*, 433–435
- ports for audio/video streams*, 435–437
- provisioning*, 440
- round-trip delay tests*, 436–437
- shared clusters*, 436
- supported deployment models*, 439–440
- traffic signatures for*, 435
- CMR Cloud, 29
- CN (Common Name), 256, 260, 262
- CollabEdge validator tool, 287
- Collaboration Endpoint. *See* CE (Collaboration Endpoint)
- collaboration environments. *See* B2B (business-to-business) collaboration solutions; multisite collaboration solutions
- Collaboration Solutions Analyzer (CSA), 287
- Collect Log option, 288
- command line interface (CLI), 37
- Comma-Separated Values (CSV) files, 318, 388, 447
- commObject schema, 103
- Common Name (CN), 256, 260, 262
- companion website, 486–487
- complex video network deployments
 - with flat dial plan, 158–160
 - with structured dial plan, 161
- Computer Telephony Integration (CTI), 449
- configuration, 396–402. *See also* B2B (business-to-business) collaboration solutions; deployment; multisite collaboration solutions
- Active Directory (AD), 326–338
 - AD LDS (Active Directory Lightweight Directory Services)*, 322–323
 - avatar synchronization*, 332–333
 - Cisco Directory Connector automatic upgrades*, 329
 - enabling*, 326–327
 - full synchronization*, 335–338
 - incremental synchronization*, 335
 - LAN Settings*, 327–329
 - notifications*, 334–335, 337–338
 - Object Selection*, 329–330
 - overview of*, 318–319
 - room information synchronization*, 333–334
 - User Attribute Mapping*, 330–332
- Advanced Security, 83
- authentication, 221
- Call Policy, 124–128
- Call Signaling Optimization, 164
- Certificate Revocation settings, 78–80
- certificate-based authentication, 73–74
 - authentication versus authorization*, 73–74
 - emergency accounts*, 74
 - enabling*, 73

- overview of*, 73
- username, obtaining from certificate*, 74
- certificates. *See* certificates
- Cisco Expressway initial configuration settings
 - Auto Discovery*, 49
 - H.323 settings*, 48–51
 - overview of*, 46
 - SIP (Session Initiation Protocol) settings*, 51–55
- Cisco Expressway system configuration
 - Backup and Restore*, 42–44
 - Expressway deployment on VM*, 26–28
 - overview of*, 24
 - Service Setup Wizard through web interface*, 28–34
 - System Configuration settings*, 34–42
- Cisco Unified Communications Manager (Unified CM) integration, 450–452
- Cisco Webex. *See* Cisco Webex
- DNS Lookup, 289
- Expressway clusters
 - benefits of*, 210
 - Cisco Expressway Cluster Creation and Maintenance Deployment Guide*, 210
 - cluster registration and call capacity limitations*, 210
 - DNS (Domain Name System) and*, 213–214
 - operation as one large local zone*, 212–213
 - overview of*, 208
 - redundancy with*, 210
 - requirements for*, 210–212
 - security certificates*, 212
 - zones and*, 214–216
- FIPS140–2 cryptographic mode, 84–87
 - enabling*, 85–87
 - overview of*, 84–85
- IM&P (IM and Presence), 394–396
- Links and Pipes bandwidth management, 140–145
 - benefits of*, 140
 - call control using*, 145–146
 - definition of*, 140
 - one Pipe, one Link*, 141
 - one Pipe, two or more Links*, 141–142
 - Pipe configuration*, 144–145
 - two Pipes, one Link*, 142–144
 - when to use*, 140–141
- Membership Rules, 111–112
- Mobile and Remote Access. *See* MRA (Mobile and Remote Access)
- Neighbor Zones
 - characteristics of*, 165–166
 - Expressway clusters and*, 216
 - Expressway to Cisco Unified CM*, 169–176
 - Expressway to Expressway*, 166–168
 - Unified CM*, 241
- registration. *See* registration
- Search Rules, 155–156
- SIP trunks
 - dialing rules*, 173–175
 - SIP route patterns*, 173–175
 - SIP trunk settings*, 171–172
- SSH (Secure Shell), 81
- Subzone bandwidth management, 136–139

- Downspeed Mode settings*, 138–139
- Local Zone settings*, 139–140
- per-call restrictions*, 136–137
- restriction modes*, 137
- total-bandwidth restrictions*, 136–137
- Transforms, 118–121
- TURN (Traversal Using Relay NAT), 184–186
- Unified Communications, 241
- User Policy (FindMe), 128–130
- zones. *See* zones
- Configuration and Administration of the IM and Presence Service*, 294
- Configuration command**
 - Call Policy menu, 124
 - Dial Plan menu, 152
 - Registration menu, 98–99
- Configuration Log**, 235
- Configuration menu commands**
 - Authentication, 278
 - Avatar, 332
 - Call Policy, 124
 - Call Routing, 164
 - Dial Plan, 122, 152, 273, 279
 - Domains, 36, 54, 271
 - HTTP Proxy Authorization Failure, 293
 - Local Zone, 102, 109, 111
 - Notification, 334
 - Object Selection, 329, 333
 - Protocols, 48, 53, 55, 58, 96
 - Registration, 98–99
 - SIP, 78
 - Traversal, 184
 - Unified Communications, 270, 273, 291, 295
 - User Attribute Mapping, 331
 - Zones, 166, 273
- Conflict Policy, Registration. *See* Registration Conflict Policy**
- Connections command (Internet Options menu)**, 327
- Connections menu commands, LAN Settings**, 327
- Connectivity to Cisco Webex status (Hybrid Message Service)**, 397
- Connector Management**
 - for Hybrid Calendar Service, 361
 - for Hybrid Message Service, 399
- Connector Management command (Hybrid Services menu)**, 395, 399, 400
- Connector Proxy command (Hybrid Services menu)**, 355, 392
- connectors, Expressway**
 - for Cisco Webex Hybrid Calendar Service, 345–354
 - architecture*, 3451
 - Expressway-C preparation checklist*, 350–354
 - HTTPS connection*, 3450
 - impersonation accounts*, 348–349
 - prerequisites*, 349–350
 - service accounts*, 348
 - throttling policy*, 354
 - TMS (Telepresence Management Suite)*, 347
 - for Cisco Webex Hybrid Message Service, 392–394
 - for Webex Edge for Devices, 408–411
- consumption, of licenses**, 17–21
- Contact Information privilege (Cisco Webex)**, 338
- content servers**, 57

- Control Hub, Cisco Webex, 318, 416–417, 434
 - COP (Cisco Options Package), 386
 - COVID-19 pandemic, 303
 - CPL (Call Processing Language), 64, 98, 122–123
 - CPU, oversubscription of, 27
 - Create Pipe command, 144
 - Create Recording Transcripts privilege (Cisco Webex), 338
 - CRL Distribution Point (CDP) URIs, 76
 - CRL Management command (Security menu), 77
 - CRLs (certificate revocation lists), 72, 76–80
 - automatic CRL updates, 76–77
 - Certificate Revocation settings, 78–80
 - certificate revocation sources, 76
 - manual CRL updates, 77–78
 - OCSP (Online Certificate Status Protocol), 78
 - CSA (Collaboration Solutions Analyzer), 287
 - csf-unified.log file, 288
 - CSM (Customer Success Manager), 440
 - CSRs (certificate signing requests), 72, 262–263, 292
 - CSV (Comma-Separated Values) files, 318, 388, 447
 - CTI (Computer Telephony Integration), 449
 - CUBE (Cisco Unified Border Element), 20
 - CUC (Cisco Unity Connection), 295
 - CUCL (Cisco User Connect Licensing), 11–13
 - Customer Success Manager (CSM), 440
 - customizing exam, 456–457
 - CUWL (Unified Workspace Licensing), 11–13, 15
 - CVD (Cisco Validated Design), 301
- ## D
-
- \d syntax, 64
 - data loss prevention (DLP), 303
 - Data Security Service, Cisco Webex Hybrid, 312
 - databases, local, 102
 - Debug log level, 236
 - DEBUG_MARKER tag, 288
 - Deep Packet Inspection, 41
 - Default Call Bandwidth setting, 138–139, 244
 - Default CPL field (Policy Service), 100
 - Default Language setting
 - for Google Calendar deployment in the cloud, 364
 - for Hybrid Calendar Service, 360
 - for Office 365, 372
 - default Local Zone rule, 120
 - Default Subzone, 102, 107
 - Default Zones, 152
 - delay tests, round-trip, 436–437
 - DELETE method, 82
 - demilitarized zone (DMZ)
 - overview of, 188, 259, 274, 441
 - Traversal Zone deployment scenarios, 196–199
 - dual NIC DMZ*, 197–198
 - single-subnet DMZ*, 196
 - three-port firewall DMZ*, 197
 - triple Expressway*, 198–199
 - deny lists, 64, 97
 - deployment. *See also* configuration
 - Cisco Directory Connector, 323–325
 - Cisco Jabber for Cloud

- certificate validation*, 449
- Cisco Unified CM configuration*, 450–452
- Cisco Unity Connection (CUC)*, 447–449
- Cisco Webex Administration Tool*, 447
- cloud-based deployment architecture*, 446–447
- compatibility of*, 445
- CSV files, importing users from*, 447
- hybrid cloud-based deployment architecture*, 447–450
- monitoring with Cisco Webex Administration Tool*, 445
- On-Premises Deployment for Cisco Jabber*, 449
- overview of*, 444
- requirements of*, 445–450
- service discovery*, 449–450
- Cisco Webex Hybrid Calendar Service, 354–362
 - Cisco Conferencing Services Configuration*, 359–360
 - Cisco Webex users, enabling*, 361–362
 - Connector Management*, 361
 - Connector Proxy settings*, 355–356
 - Default Language setting*, 360
 - Expressway-Based Calendar Connector*, 345–354
 - Google Calendar deployment in the cloud*, 362–367
 - Hybrid Calendar Service deployment*, 354–362
 - Microsoft Exchange Configuration*, 357–359
 - OBTP (One Button to Push)*, 347, 374–377
 - Office* 365, 368–374
 - operation of*, 344–345
 - overview of*, 342
 - Trusted CA Certificate*, 356–357
- Cisco Webex Hybrid Directory Service
 - Active Directory configuration and synchronization*, 318–319, 322–323, 326–338
 - deployment models*, 318–319
 - deployment requirements*, 319–321
 - infrastructure requirements*, 321–325
 - overview of*, 316
 - Webex user service assignment*, 338–340
- Cisco Webex Hybrid Message Service
 - certificates*, 392
 - deployment models*, 382–384
 - deployment requirements*, 385–388
 - Expressway connector registration to Cisco Webex cloud*, 392–394
 - Expressway requirements*, 388–391
 - IM&P (IM and Presence) configuration*, 394–396
 - service management*, 396–402
- Cisco Webex Video Mesh. *See* Video Mesh (Webex)
- Google Calendar in the cloud, 362–367
 - architecture*, 362–363
 - Cisco Webex users, enabling*, 364–365
 - Default Language setting*, 364

- enabling and configuring*, 363–364
- testing and verification*, 367
- User Email Notifications*, 365
- workspaces, adding devices to*, 365–367
- Mobile and Remote Access solutions. *See* MRA (Mobile and Remote Access)
- multisite collaboration solutions
 - complex video network with flat dial plan*, 158–160
 - complex video network with structured dial plan*, 161
 - hierarchical video network with structured dial plan*, 162–165
 - simple video network with flat dial plan*, 157
- Traversal Zones, 196–199
 - dual NIC DMZ deployment scenarios*, 197–198
 - single-subnet DMZ deployment scenario*, 196
 - three-port firewall DMZ deployment scenario*, 197
 - triple Expressway deployment scenarios*, 198–199
- Deployment Guide for Cisco Webex Video Mesh*, 440–441
- Description setting (Search Rules), 155
- Desktop System licenses, 15, 19, 210–211
- Desktop systems, 4
- Device menu commands
 - Local Database, 102
 - Phone, 290
 - Trunk, 171
- Device Pool command (System menu), 267
- Device Provisioning, 4
- Devices, Webex Edge for, 406–417
 - Cisco Webex Control Hub, 416–417
 - Cisco Webex Device Connector, 408–411
 - cloud onboarding and linking, 411–412
 - features and functionality, 406–407
 - limitations, 408
 - prerequisites, 407
 - proxy server features, 412–413
 - supported operating systems, 407
 - URLs for on-premises device linking, 413–416
- Devices command (Authentication menu), 102
- DHCP (Dynamic Host Configuration Protocol), 6
- Diagnostic Logging command (Diagnostics menu), 236, 288
- Diagnostic Logging tool, 236–237
- diagnostic logs, 236–237, 288–289
- Diagnostics command (Maintenance menu), 236
- Diagnostics menu commands
 - Diagnostic Logging, 236, 288
 - Support Log configuration, 288
- Dial Plan command (Configuration menu), 122, 152, 273, 279
- Dial Plan menu commands
 - Configuration, 152
 - Search Rules, 273, 279
 - Transforms, 122
- dial plans
 - deployments
 - complex video network with flat dial plan*, 158–160
 - complex video network with structured dial plan*, 161

hierarchical video network with structured dial plan, 162–165

simple video network with flat dial plan, 157

overview of, 151

zones. *See* zones

Differentiated Service Code Point (DSCP), 37–38

Diffie-Hellman key exchange, 255, 292

Digest, 101

Digital Signature Algorithm (DSA), 75

direct registration, 5

Directory Connector, 323–325, 329, 385. *See also* Directory Service, Cisco Webex Hybrid

directory Expressways, 162

Directory Numbers (DNs), 173–174

Directory Service, Cisco Webex Hybrid, 311

Active Directory configuration and synchronization, 326–338

AD LDS (Active Directory Lightweight Directory Services), 322–323

avatar synchronization, 332–333

Cisco Directory Connector automatic upgrades, 329

enabling, 326–327

full synchronization, 335–338

incremental synchronization, 335

LAN Settings, 327–329

notifications, 334–335, 337–338

Object Selection, 329–330

overview of, 318–319

room information

synchronization, 333–334

User Attribute Mapping, 330–332

Cisco Directory Connector, 323–325, 329, 385

deployment models, 318–319

deployment requirements, 319–321

infrastructure requirements, 321–325

Active Directory services, 322

AD LDS (Active Directory Lightweight Directory Services), 322–323

HTTP (Hypertext Transfer Protocol), 325

minimum hardware requirements, 322

NTLM (NT LAN Manager), 324–325

supported Windows Server versions, 321

web proxy, 323–324

overview of, 316

Webex user service assignment, 338–340

discovery, 6

DHCP (Dynamic Host Configuration Protocol), 6

Gatekeeper, 9

Discovery messages (DHCP), 6

DLP (data loss prevention), 303

DMZ (demilitarized zone), 188, 259, 274, 441

overview of, 188, 259, 274, 441

Traversal Zone deployment scenarios, 196–199

dual NIC DMZ, 197–198

single-subnet DMZ, 196

three-port firewall DMZ, 197

triple Expressway, 198–199

DNs (Directory Numbers), 173–174

DNS (Domain Name System)

- for Cisco Webex Video Mesh, 433
 - clustering and, 213–214
 - DNS Lookup, 230–231, 289
 - DNS Zones, 153, 199–204
 - DNS A records, 202–204*
 - DNS settings, 200*
 - ENUM Zones, 200*
 - for internal call routing, 199–200*
 - SRV (Service) records, 204*
 - MRA (Mobile and Remote Access)
 - configuration, 243–244
 - records, 59, 241, 251–254
 - A, 200, 202–204, 251*
 - MRA (Mobile and Remote Access), 241*
 - NAPTR (Name Authority Pointer), 154, 200, 230*
 - PTR (Pointer), 214*
 - SRV (Service), 153, 204, 214, 251–254*
 - System Configuration settings, 34–35
 - troubleshooting for B2B collaboration solutions, 230–232
 - Unified Communications
 - configuration on, 271–273
 - DNS Best Practices, Network Protections, and Attack Identification, 433*
 - DNS command (System menu), 34, 87, 289, 294
 - DNS Lookup, 230–231, 289
 - DNS Lookup command (Network Utilities menu), 230
 - documentation, for Webex Video Mesh deployment, 433
 - dollar sign (\$), 65
 - domain certificates, 88–90
 - Domain Certificates command (Security menu), 88–90
 - Domain Name System. *See* DNS (Domain Name System)
 - Domain Validation (DV) certificates, 258
 - domains
 - adding to E.164 number, 65
 - domain certificates, 88–90
 - initial configuration settings, 51–55
 - MRA (Mobile and Remote Access)
 - configuration, 243–244
 - names of, 54
 - removing, 66
 - SIP (Session Initiation Protocol), 36
 - Domains command (Configuration menu), 36, 54, 271
 - Download Log option, 288
 - Downspeed Mode settings, 138–139
 - Downspeed Per Call Mode setting, 139
 - Downspeed Total Mode setting, 139
 - DSA (Digital Signature Algorithm), 75
 - DSCP (Differentiated Service Code Point), 37–38
 - DTMF (dual-tone multifrequency), 56–57
 - dual NIC deployment, 38–39, 197–198
 - dual-tone multifrequency (DTMF), 56–57
 - DV (Domain Validation) certificates, 258
 - Dynamic Host Configuration Protocol. *See* DHCP (Dynamic Host Configuration Protocol)
 - dynamic link library (DLL), 322–323
-
- ## E
- E.164 aliases, 8, 58, 95, 200–201
 - E.164 Number Mapping, 64, 200
 - ECX (Equinix Cloud Exchange), 419, 420

- Edge Connect, 304, 418–420
- Edge solutions, Cisco Webex. *See* Cisco Webex Edge
- Edit Settings command (Services menu), 365
- Editable Inbound Rules command (HTTP Allow List menu), 277
- ellipses (...), 65
- emergency accounts, for certificate-based authentication, 74
- Enable Directory Synchronization command, 326
- Enable Facebook Live Integration privilege (Cisco Webex), 338
- Enable Mobile and Remote Access setting (Cisco Unified Communications Manager), 245
- encryption
 - asymmetric cryptography, 255
 - Backup and Restore, 42
 - Cisco Webex
 - Webex Hybrid Message Service*, 384
 - Webex Meetings*, 308
 - Webex Messaging*, 309
 - Diffie-Hellman key exchange, 255
 - FIPS140–2 cryptographic mode, 84–87
 - enabling*, 85–87
 - overview of*, 84–85
 - KMS (Key Management Service), 384
 - Phone Security Profiles, 268
 - public-key, 255
 - for Registration Authentication, 101
 - Rivest-Shamir-Adleman (RSA), 255
 - SIP Media Encryption Mode, 68–72
 - symmetric cryptography, 255
- endpoints, 240. *See also* Cisco Jabber; H.323 protocol; registration; SIP (Session Initiation Protocol)
 - Cisco Collaboration Endpoint (CE), 6
 - Cisco Telepresence, 6
 - troubleshooting, 291–292
- ENUM (Enumerated Dialing), 64, 151, 153, 200
- Equinix Cloud Exchange (ECX), 419, 420
- errors
 - 401 Unauthorized failure, 294
 - 404 errors, 295
 - 407 Proxy Authentication Required, 295
 - 500 Internal Server Error, 295
 - 502 error, 295
 - Cannot communicate with the server, 294
 - definition of, 236
 - Failed to establish SSL connection, 292
 - Failed to query auth component for SASL mechanisms, 295
 - Loopback, 159
 - MRA (Mobile and Remote Access), 294–295
 - Registration Rejected - Alias Conflicts with an Existing Registration, 224
 - Registration Rejected - Not Permitted by Policy, 224
 - Registration Rejected - Received from Unauthenticated Source, 224
 - Registration Rejected - Unknown Domain, 224
- ESXi supported versions, 26
- EV (Extended Validation) certificates, 258
- Event Log, 223–225
 - addressing, 223
 - error messages in, 224
 - levels of logging for, 225

Event Log command (Logs menu), 223

exam

customizing, 456–457

final preparation for, 454–458

exam customization, 456–457

exam updates, 457

final review/study, 458

Pearson Test Prep software,
455–456

test-taking tips, 454

Premium Edition, 457

updating, 457

expressions, regular

compatibility of, 64

definition of, 64

examples of, 65–66

overview of, 62

POSIX syntax for, 64

special characters in, 64–65

verification with Check Pattern, 66–67

Expressways. *See* Cisco Expressway

Extended Validation (EV) certificates,
258

Extensible Messaging and Presence
Protocol (XMPP), 55, 260, 275, 445

F

“Failed to establish SSL connection”
error, 292

“Failed to query auth component for
SASL mechanisms” error, 295

FedRAMP (Webex for Government),
408

Fiber Connect, 305

Fibre Channel SAN storage, 302

Find and List Access Control Groups
dialog box, 451–452

FindMe, 4, 15, 16, 128–130

FIPS140–2 cryptographic mode, 42,
84–87

enabling, 85–87

overview of, 84–85

Firewall Traversal Services, 241

firewalls

in collaboration environments, 181

configuration, 38–42

Firewall Traversal Services, 241

MRA (Mobile and Remote Access)
support for, 241

standard firewall traversal solutions,
240–241

Fixup, 41

Flash Card Mode, for exam, 456

flat dial plans

complex video network with, 158–160

simple video network with, 157

Flex Plan, 304

force encrypted policies, 71–72

force unencrypted policies, 71–72

FQDNs (fully qualified domain names),
6, 49, 355, 391

for Expressway clusters, 212, 214

registration, 393

troubleshooting, 289, 292

Front-End (FE) server, 214

full synchronization, Active Directory,
335–338

fully qualified domain names. *See*
FQDNs (fully qualified domain
names)

G

G.711, 10

Gatekeeper Confirmation (GCF), 9

Gatekeeper Discovery, 9

Gatekeeper Request (GRQ), 9, 21

gatekeepers

- definition of, 8

- H.323 registration to, 8–9

- security, 9

gateways

- ALGs (Application Layer Gateways), 198

- H.323, 168

- between IPv4 and IPv6 devices, 57

GCF (Gatekeeper Confirmation), 9**Generate CSR command, 262****geographic distribution, Webex Video Mesh, 442****geographic distribution with SIP dialing, Webex Video Mesh, 443****GET method, 82****get-ManagementRoleAssignment command, 348****good certificate status, 78****Google Calendar deployment in the cloud, 362–367**

- architecture, 362–363

- Cisco Webex users, enabling, 364–365

- Default Language setting, 364

- enabling and configuring, 363–364

- testing and verification, 367

- User Email Notifications, 365

- workspaces, adding devices to, 365–367

Google Workspace, adding devices to, 365–367**GRQ (Gatekeeper Request), 9, 21****H****H.225.0 protocol, 48****H.225 protocol, 10****H.235 protocol, 101, 103****H.245 protocol, 10, 48****H.261 protocol, 10****H.320 protocol, 48****H.323 command (Protocols menu), 48, 58, 96, 390****H.323 mode field (H.323 configuration), 49****H.323 protocol, 5, 48**

- call setup process, 9–10

- configuration, 48–51, 221, 390

- E.164 aliases, 8, 58, 95, 200–201

- endpoint, verification of, 56–59

- on Expressway clusters, 211

- gatekeepers, 48

- gateways, 168

- H.323 ALG, 41

- H.323 IDs, 8, 58

- interworking, 51, 118–121

- overview of, 8–10

- registration. *See* registration

- Routing Prefixes, 8

H323Identity schema, 103**H.350 directory, 102, 103****H.350.1 directory, 103****H.350.2 directory, 103****H.350.4 directory, 103****H.460.18 standard, 153****H.460.18/19 standard, 188–189****H.460.19 standard, 153****hair-pinning, 9, 126–128****Hash-based Message Authentication Code (HMAC), 70****HCS (Hosted Collaboration Solution), 300–302, 417****hierarchical video network deployments, 162–165****high availability, Cisco Webex Hybrid Directory Service, 320–321**

- High-quality Video privilege (Cisco Webex), 338**
- History command**
 - Calls menu, 229, 289
 - Registration menu, 222
- HMAC (Hash-based Message Authentication Code), 70**
- Hosted Collaboration Solution (HCS), 300–302, 417**
- HTTP (Hypertext Transfer Protocol), 30, 325**
 - Allow List/Deny List policies, 97, 274–278
 - automatically added rules, 276–277*
 - manually added rules, 277–278*
 - overview of, 274–275*
 - regular expressions with, 64*
 - uploaded rules, 278*
- HTTPS (HTTP Secure), 30, 100, 318–319, 391**
 - certificates with, 72*
 - for Cisco Webex Hybrid Calendar Service with, 3450*
 - HTTPS reverse proxy, 275*
 - reverse HTTPS proxy, 242, 275*
 - troubleshooting, 295*
- methods, 81–83
- HTTP Allow List command (Unified Communications menu), 275, 277, 278**
- HTTP Allow List menu commands**
 - Automatic Inbound Rules, 275
 - Automatic Outbound Rules, 275
 - Editable Inbound Rules, 277
 - Upload Rules, 278
- HTTP Proxy Authorization Failure, 293**
- HTTP Proxy Resource Access Failure, 295**
- HTTPS (Hypertext Transfer Protocol Secure), 30, 318–319, 391**
 - certificates with, 72
 - for Cisco Webex Hybrid Calendar Service with, 3450
 - reverse proxy, 242, 275
 - troubleshooting, 295
- HTTPS certificate revocation list (CRL) checking field (Policy Service), 100**
- hub-and-spoke architecture, Webex Video Mesh, 442**
- hybrid deployments, Cisco Jabber**
 - architecture of, 447–450
 - certificate validation, 449
 - Cisco Unified CM configuration, 450–452
 - Cisco Unity Connection (CUC), 447–449
 - Cisco Webex Administration Tool, 447
 - CSV files, importing users from, 447
 - requirements of, 445–450
 - service discovery, 449–450
- Hybrid Services, Cisco Webex, 310–313**
 - Hybrid Calendar Service, 311
 - Expressway-Based Calendar Connector, 345–354*
 - Google Calendar deployment in the cloud, 362–367*
 - Hybrid Calendar Service deployment, 354–362*
 - OBTP (One Button to Push), 347, 374–377*
 - Office 365, 368–374*
 - operation of, 344–345*
 - overview of, 342*
 - Hybrid Call Service, 311–312

- Hybrid Data Security Service, 312, 384
- Hybrid Directory Service, 311
 - Active Directory configuration and synchronization, 318–319, 322–323, 326–338*
 - deployment models, 318–319*
 - deployment requirements, 319–321*
 - infrastructure requirements, 321–325*
 - overview of, 316*
 - Webex user service assignment, 338–340*
- Hybrid Message Service, 312
 - certificates, 392*
 - deployment models, 382–384*
 - deployment requirements, 385–388*
 - Expressway connector registration to Cisco Webex cloud, 392–394*
 - Expressway requirements, 388–391*
 - IM&P (IM and Presence) configuration, 394–396*
 - management of, 396–402*
 - overview of, 380*
- Video Mesh. *See* Video Mesh (Webex)
- Hybrid Services command (Applications menu), 355, 356, 392**
- Hybrid Services menu commands**
 - Connector Management, 361, 395, 399, 400
 - Connector Proxy, 355, 392
 - Message Service, 395
- Hypertext Transfer Protocol. *See* HTTP (Hypertext Transfer Protocol)**
- Hypertext Transfer Protocol Secure. *See* HTTPS (Hypertext Transfer Protocol Secure)**
- ICANN (Internet Corporation for Assigned Names and Numbers), 182**
- ICE (Interactive Connectivity Establishment), 183, 186**
- ICSA (Intercluster Sync Agent), 386**
- IdenTrust Commercial Root CA 1, 416–417**
- IDs**
 - FindMe IDs, 129
 - H.323 IDs, 8, 58
 - Jabber ID (JID), 401–402
- IEEE (Institute of Electrical and Electronic Engineers), 182**
- IETF (Internet Engineering Task Force), 5–6, 51. *See also* SIP (Session Initiation Protocol)**
- ICE (Interactive Connectivity Establishment), 183, 186**
- NAT (Network Address Translation), 39, 181, 182–183, 419**
- STUN (Session Traversal Utilities for NAT), 183–184, 420, 435, 436–437, 439–440**
- TURN (Traversal Using Relay NAT), 38, 183, 184–186**
 - configurable options for, 185–186*
 - operation within symmetric networks, 184*
- ILS (Intercluster Lookup Service), 294**
- IM (Instant Messaging) clients, 445**
- IM and Presence Service Nodes command (Unified Communications menu), 273**
- IM&P (Instant Messaging and Presence), 55, 303, 445**
 - capabilities of, 445
 - configuration for Cisco Webex Hybrid Message Service, 394–396

- Intercluster Sync Agent, 294
 - MRA (Mobile and Remote Access), 245
 - overview of, 382
 - troubleshooting, 295, 400–402
 - impersonation accounts, Cisco Webex Hybrid Calendar Service, 348–349
 - incremental Active Directory synchronization, 335
 - Inspection, 41
 - installation. *See also* configuration; deployment
 - Cisco Webex Device Connector, 408–411
 - Webex Video Mesh Nodes, 441–442
 - Instant Messaging and Presence. *See* IM&P (Instant Messaging and Presence)
 - Instant Messaging (IM) clients, 445
 - Institute of Electrical and Electronic Engineers (IEEE), 182
 - Integrated Services Digital Network (ISDN)-based networks, 48
 - Interactive Connectivity Establishment. *See* ICE (Interactive Connectivity Establishment)
 - interactive voice response (IVR), 313
 - Intercluster Lookup Service (ILS), 294
 - Intercluster Sync Agent (ICSA), 386
 - International Telecommunications Union. *See* ITU (International Telecommunications Union)
 - Internet Corporation for Assigned Names and Numbers (ICANN), 182
 - Internet Engineering Task Force. *See* IETF (Internet Engineering Task Force)
 - Internet Options menu commands, Connections, 327
 - Internet Protocol. *See* IP (Internet Protocol) addresses
 - Interoperability, Microsoft, 4, 15, 16
 - interworking, 51
 - definition of, 55
 - initial configuration of, 55–57
 - licensing and, 19–20
 - Transforms for, 118–121
 - Interworking command (Protocols menu), 55
 - Interworking Log Level, 236
 - IP (Internet Protocol) addresses
 - for Expressway clusters, 216
 - IPv4 (Internet Protocol version 4), 57, 109–110, 182
 - IPv6 (Internet Protocol version 6), 57, 182
 - IP addressing setting (Cisco Unified Communications Manager), 244
 - IP command (Network Interfaces menu), 57
 - ISDN (Integrated Services Digital Network)-based networks, 48. *See also* H.323 protocol
 - item.Culture property, 360
 - ITU (International Telecommunications Union), 8, 48, 187. *See also* H.323 protocol
 - ITU-T (ITU Telecommunication Standardization Sector), 48
 - IVR (interactive voice response), 313
-
- J
- Jabber. *See* Cisco Jabber
 - Jabber Desktop Client Policy setting (Cisco Unified Communications Manager), 245
 - Jabber for Windows Diagnostic Logs file, 288

Jabber Guest Services, 29
 Jabber ID (JID), 401–402
 Jabber Mobile Client Policy setting
 (Cisco Unified Communications
 Manager), 245
 Jabber Team Messaging Mode, 445
 Jabber Webex Messenger IM, 445

K-L

KMS (Key Management Service), 312,
 384
 LAN Settings command (Connections
 menu), 327–329
 languages
 Call Processing Language (CPL), 64,
 98, 122–123
 Default Language setting
 *for Google Calendar deployment
 in the cloud, 364*
 *for Hybrid Calendar Service,
 360*
 for Office 365, 372
 LANs (local-area networks), 15
 Active Directory configuration and
 synchronization, 327–329
 addresses for, 212
 H.323 settings for, 48–51
 LCF (Location Confirm), 160, 164
 LDAP (Lightweight Directory Access
 Protocol), 72, 327
 DNS server settings for, 35
 LDAPS (Secure LDAP), 327
 over SSL, 327
 for Registration Authentication,
 102–106
 TLS Verify Mode, 359
 LDAPS (Secure LDAP), 327
 LDS (Lightweight Directory Services),
 322–323
 Leave setting (Search Rules), 156
 levels, Event Log, 225
 licensing, Cisco Expressway
 Cisco Collaboration Flex Plan, 11,
 13–14
 Cisco Expressway versus Cisco VCS,
 15–16
 CUCL (Cisco User Connect Licensing),
 11–13
 CUWL (Unified Workspace Licensing),
 11–13, 15
 device-based versus user-based, 5, 11
 direct registration and, 5
 Expressway deployment on VM, 28
 license consumption, 17–21
 license limitations, 21
 Option Key, 15–16
 overview of, 11–15
 PAK (Product Activation Key), 14,
 31–32
 Release Key, 16–17
 Smart Licensing, 14–15, 33–34
 Lightweight Directory Access Protocol.
 See LDAP (Lightweight Directory
 Access Protocol)
 Lightweight Directory Services (LDS),
 322–323
 Limited bandwidth restriction mode,
 137
 Links and Pipes bandwidth
 management, 107, 140–145
 benefits of, 140
 call control using, 145–146
 definition of, 140
 one Pipe, one Link, 141
 one Pipe, two or more Links, 141–142
 Pipe configuration, 144–145
 troubleshooting tips, 234
 two Pipes, one Link, 142–144

when to use, 140–141

Links command (Bandwidth menu), 234

Local Call Serial Number setting, 229

Local Database, 102

Local Database command (Device menu), 102

Local Zone command (Configuration menu), 102, 109, 111

Local Zone menu commands

- Default Subzone, 102
- Subzone Membership Rules, 111
- Subzones, 109

Local Zones, 107, 212–213

- configuration settings for, 139–140, 155, 234
- definition of, 151

local-area networks. *See* LANs (local-area networks)

locally registered services, 57

Locally Significant Certificate (LSC), 255

Locate command (Tools menu), 132, 227

Locate tool, 132, 227–228

Location Confirm (LCF), 160, 164

Location Request (LRQ), 158–160, 164, 200

log analysis tool, 287

Logging command (System menu), 225

logs, 229, 236

- bandwidth monitoring, 234
- Calls, 229
- Configuration, 235
- diagnostic, 236–237, 288–289
 - Diagnostic Logging tool, 236–237*
 - MRA (Mobile and Remote Access), 288–289*

Event, 223–225

- addressing, 223*
- error messages in, 224*
- levels of logging for, 225*

History, 222

registration, 222–225

- By Alias logs, 222*
- By Device logs, 222*

Search History, 131, 226–227

lookups, DNS (Domain Name System), 230–231

Loopback errors, 159

LRQ (Location Request), 158–160, 164, 200

LSC (Locally Significant Certificate), 255

M

MAC (Media Access Control) addresses, 28

Mailbox (MBX) servers, 347

Maintenance menu commands

- Advanced Security, 81, 83, 84, 85
- Backup and Restore, 42, 43
- Diagnostics, 236
- Option Keys, 16
- Restart Options, 83
- Security, 73, 74, 75, 77, 88, 232, 234, 262, 273, 353, 391
- Security Certificates, 356
- Tools, 132, 227, 230

Manage Domain Wide Delegation command, 363

Management menu commands, Users, 339

Manager-trust certificates, 292

manual CRL updates, 77–78

- mapping Active Directory attributes, 330–332
- markers, adding, 288
- Maximum Session Bit Rate for Video Calls setting, 244, 245, 295
- MBX (Mailbox) servers, 347
- MCUs (multipoint control units), 8, 57
- MD5 (Message Digest Algorithm 5), 101, 221
- MDM (Multiple Device Messaging), 386
- media encryption, enforcement of, 289
- Meetings, Webex, 306–308, 312–313, 438
- Membership Rules, 106–112, 221
 - Alias Pattern Match, 111
 - creating, 111–112
 - subnet masks, 109–110
- memory, random-access,
 - oversubscription of, 27
- Message Digest Algorithm 5 (MD5), 101, 221
- Message Free entitlement, 387
- Message Service, Cisco Webex Hybrid, 308–309, 312
 - certificates, 392
 - deployment models, 382–384
 - one Expressway connector cluster to multiple IM&P Service clusters*, 384
 - one-to-one Expressway to IM and Presence Service cluster*, 383
 - deployment requirements, 385–388
 - components*, 386–387
 - ports*, 386–388
 - protocols*, 385–386
 - user population*, 387–388
 - Expressway connector registration to Cisco Webex cloud, 392–394
 - Expressway requirements, 388–391
 - IM&P (IM and Presence)
 - configuration, 394–396
 - management of, 396–402
 - Connector Management*, 399
 - Message Service Status*, 396–402
 - troubleshooting*, 399–402
 - overview of, 380
- Message Service Configuration
 - command (Message Service menu), 395, 400
- Message Service menu commands
 - Message Service Configuration, 395, 400
 - Message Service Status, 395, 397–399, 400
- Message Service Status (IM&P Nodes) status (Hybrid Message Service), 398
- Message Service User Totals (This Expressway) status (Hybrid Message Service), 397
- Message Service Users from This Node status (Hybrid Message Service), 398
- methods, HTTP (Hypertext Transfer Protocol), 81–83
- Microsoft Active Directory. *See* Active Directory (AD)
- Microsoft Exchange Configuration, 357–359
- Microsoft Front-End (FE) server, 214
- Microsoft gateway service, 29
- Microsoft Graph API, 368
- Microsoft Interoperability, 4, 15, 16
- migration, VCS to Expressway, 4–5
- Minimum session refresh interval field (SIP configuration), 54
- Mobile and Remote Access. *See* MRA (Mobile and Remote Access)

- Mobile Remote Access Through Cisco Expressway Deployment Guide*, 242
- Mode setting (Search Rules), 155
- models, deployment. *See* deployment
- monitoring, with Cisco Webex Administration Tool, 445
- MPLS (Multiprotocol Label Switching), 305
- MRA (Mobile and Remote Access), 449
 - capabilities of, 304
 - certificates, 254–255
 - CAs (*certificate authorities*), 254
 - Cisco Expressway, 254, 259
 - Cisco Unified CM, 254, 259–261
 - classes of, 258
 - creating, 261–265
 - Domain Validation (DV), 258
 - Extended Validation (EV), 258
 - Organization Validation (OV), 258
 - overview of, 254–255
 - root CA, 254–255
 - table of, 255
 - TLS Verify, 254, 255–258, 259
 - Trusted CA Certificates, 265
 - Unified CM Tomcat, 254, 259–261
 - Cisco Unified CM settings, 266–269
 - compatibility of, 29
 - components of, 241–242
 - certificates, 241
 - DNS records, 241
 - Firewall Traversal Services, 241
 - reverse HTTPS proxy, 242
 - SIP Trunk Security Profile, 242
 - Unified Communications settings, 241
 - deployment, 242–245
 - Cisco Unified Communications Manager configuration, 244–245
 - Cisco Unity Connection service requirements, 245
 - domain configuration, 243–244
 - IM and Presence service requirements, 245
 - Mobile Remote Access Through Cisco Expressway Deployment Guide, 242
 - port configuration, 242
 - DNS records, 251–254
 - Expressway clusters for, 214
 - HTTP Allow list, 274–278
 - automatically added rules, 276–277
 - manually added rules, 277–278
 - overview of, 274–275
 - uploaded rules, 278
 - overview of, 5, 238, 248
 - purpose of, 240–241
 - registration capacity limitations, 21
 - standard firewall traversal solution compared to, 240–241
 - traversal zones, 153
 - troubleshooting
 - alarms, 287
 - authentication status and tokens, 291
 - call status information, 289–290
 - Cisco Jabber sign-in issues, 292–294
 - Collaboration Solutions Analyzer, 287
 - diagnostic logs, 288–289
 - DNS Lookup, 289
 - error codes, 294–295

- FQDN (fully qualified domain name), 289*
- general techniques, 287–291*
- IM and Presence Intercluster Sync Agent, 294*
- MRA authentication status and tokens, 291*
- overview of, 284*
- registration and certificate issues, 291–292*
- Unified Communications Status, 287, 290, 291*
- Unified Communications
 - configuration on Expressways, 270–273
 - DNS settings, 271–273*
 - MRA-specific settings, 270–271*
 - overview of, 270*
 - Traversal Zones, 278–281*
 - Unified CM discovery settings, 273*
 - zones, 273*
- MRA Access Policy setting (Cisco Unified Communications Manager), 245
- MTLS (Mutual TLS), 241, 242, 259
- Multiple CUCM clusters setting (Cisco Unified Communications Manager), 244
- Multiple Device Messaging (MDM), 386
- multipoint control units (MCUs), 8, 57
- Multiprotocol Label Switching (MPLS), 305
- multisite collaboration solutions
 - deployments
 - complex video network with flat dial plan, 158–160*
 - complex video network with structured dial plan, 161*
 - hierarchical video network with structured dial plan, 162–165*
 - simple video network with flat dial plan, 157*
 - dial plans
 - deployments, 157–165*
 - overview of, 151*
 - zones. See zones*
 - DNS Zones, 199–204
 - DNS settings, 201–202*
 - ENUM Zones, 200*
 - for internal call routing, 199–200*
 - A records, 202–204*
 - SRV (Service) records, 204*
 - Expressway Media Traversal, 187
 - Assent and H.460.18/19, 188–189*
 - Traversal Zone configuration, 189–196*
 - Traversal Zone deployment scenarios, 196–199*
 - firewall issues, 181
 - ICE (Interactive Connectivity Establishment), 183, 186
 - NAT (Network Address Translation)
 - issues, 182–183
 - Neighbor Zones
 - characteristics of, 165–166*
 - Expressway to Cisco Unified CM, 169–176*
 - Expressway to Expressway, 166–168*
 - overview of, 148, 178
 - Search Rules, 154–155
 - STUN (Session Traversal Utilities for NAT), 183–184
 - TURN (Traversal Using Relay NAT), 183, 184–186

configurable options for,
185–186

*operation within symmetric
networks*, 184

multitenancy

domain certificates, 88–90

SNI (Server Name Indication) protocol,
87–88

Mutual TLS (MTLS), 241, 242, 259

N

Name Authority Pointer (NAPTR), 154,
200, 230

Named setting (Search Rules), 155

names, system, 34

NAPTR (Name Authority Pointer), 154,
200, 230

NAPTR option (DNS Lookup), 230

NAT (Network Address Translation),
39, 419

in collaboration environments, 181

STUN (Session Traversal Utilities for
NAT), 420

round-trip delay tests, 436–437

SRT (STUN round-trip) delay,
435, 436–437, 439–440

negative lookahead syntax (?!), 65

negative lookbehind (?<!), 65

Neighbor Zones, 153

characteristics of, 165–166

Expressway clusters and, 216

Expressway to Cisco Unified CM,
169–176

*compared to Expressway to
Expressway Neighbor Zones*,
169

dialing rules, 173–175

SIP route patterns, 173–175

SIP trunk security profiles,
170–171

SIP trunk settings, 171–172

Transforms, 175–176

Expressway to Expressway, 166–168

*Authentication, Location, and
Advanced Neighbor Zone
menus*, 167–168

*H.323 and SIP Neighbor Zone
menus*, 166

Unified CM, 241

Network Address Translation. *See* NAT
(Network Address Translation)

network interface cards. *See* NICs
(network interface cards)

Network Interfaces menu commands
IP, 57

Static Routes, 40

Network Log, 229, 236

Network Time Protocol. *See* NTP
(Network Time Protocol)

Network Utilities command (Tools
menu), 230

Network Utilities menu commands,
DNS Lookup, 230, 289

NICs (network interface cards), 197

dual NIC deployment, 38–42,
197–198

oversubscription of, 27

No Bandwidth restriction mode, 137

Node Status status (Hybrid Message
Service), 398

Node Version status (Hybrid Message
Service), 398

Nodes, Video Mesh. *See* Video Mesh
(Webex)

non-traversal call, 15

Notification command (Configuration
menu), 334

notifications

- Active Directory configuration and synchronization, 334–335, 337–338
 - Cisco Unified Communications Manager, 245
 - NTLM (NT LAN Manager), 324–325
 - NTP (Network Time Protocol), 101, 104
 - configuration, 35–36
 - DNS server settings for, 35
 - for Registration Authentication, 104
- O**
-
- OAuth Refresh Logins setting (Cisco Unified Communications Manager), 245
 - OAuth setting (Cisco Unified Communications Manager), 245
 - OAuth Token Users command (Users menu), 291
 - Object Selection, Active Directory, 329–330
 - OBTP (One Button to Push)
 - Cisco Webex Hybrid Calendar Service with, 347, 374–377
 - device registration*, 374–375
 - testing and verification*, 376–377
 - workspaces, adding devices to*, 375–376
 - overview of, 311, 347
 - OCSP (Online Certificate Status Protocol), 76, 78
 - Offer messages (DHCP), 6
 - Office 365, configuration for Google Calendar deployment in the cloud, 368–374
 - Cisco Webex users, enabling, 373–374
 - Default Language setting, 372
 - hybrid Exchange environments, 370
 - Microsoft Graph API, 368
 - permissions, 368
 - requirements, 369
 - scheduling flow, 371
 - setup process, 372
 - On Successful Match setting (Search Rules), 156
 - One Button to Push. *See* OBTP (One Button to Push)
 - Online Certificate Status Protocol (OCSP), 76, 78
 - on-premises calls, Webex Video Mesh, 437–439
 - On-Premises Deployment for Cisco Jabber, 447–449
 - Open Virtualization Format (OVA), 26
 - OpenLDAP servers, 102–106
 - OpenSSL, 262
 - openssl x509 -text -nameopt RFC2253 -noout command, 80
 - optimization
 - Call Signaling Optimization, 164
 - optimal call routing, 163
 - Option Keys
 - Cisco VCS versus Cisco Expressway licensing, 15–16
 - configuration with Service Setup Wizard, 32–33
 - Option Keys command (Maintenance menu), 16
 - Option Keys page (Service Setup Wizard), 32–33
 - OPTIONS method, 82
 - OTT (over the top) services, 304
 - OV (Organization Validation) certificates, 258
 - OVA (Open Virtualization Format), 26
 - over the top (OTT) services, 304

overflow, Webex Video Mesh cluster selection for, 439–440

Overview command (Status menu), 30, 31

Overview page (Service Setup Wizard), 31

Overwrite Registration Conflict Policy, 94–96

P

PAK (Product Activation Key) licenses, 14, 16, 31–32

passwd command, 352, 390

Password field (Policy Service), 100

password protection, 42

PAT (Port Address Translation), 182

Path field (Policy Service), 100

Pattern Behavior setting (Search Rules), 156

Pattern String setting (Search Rules), 155

Pattern Type setting (Search Rules), 155

PBXs (private branch exchanges), 304, 417

Pearson Test Prep software, 455–456

- offline access, 455–456
- online access, 455

People Insights for Webex Meetings, 307

per-call bandwidth restrictions, 136–137

- In and Out restrictions, 137
- Within restrictions, 137

period (.)

- in domain names, 54
- in FQDNs (fully qualified domain names), 292
- in regular expressions, 64

permissions, Office 365, 368

Personal Room privilege (Cisco Webex), 338

Personal Room URL privilege (Cisco Webex), 338

Phone command (Device menu), 290

Phone Security Profile command (Security menu), 267

pipe symbol (|), 65

Pipes

- applying to Links, 144–145
- bandwidth management, 140–146
- benefits of, 140
- call control using, 145–146
- creating, 144–145
- definition of, 140
- one Pipe, one Link, 141
- one Pipe, two or more Links, 141–142
- two Pipes, one Link, 142–144
- when to use, 140–141

PKI (public key infrastructure), 241, 251

plain old telephone service (POTS), 8

plus sign (+), 64

PoE (Power over Ethernet), 6

Pointer (PTR) records, 214

policy

- Call Policy, 116–121
 - ACLs compared to*, 122
 - Call Processing Language (CPL) Script*, 122–123
 - configuration*, 124–128
 - definition of*, 122
 - priority of*, 123–124
 - rules*, 124–128
- Registration Conflict Policy, 94–96
- Registration Restriction Policy, 96–100

- Allow List/Deny List policies, 97–98*
- enabling, 97*
- Policy Service, 98–100*
- User Policy (FindMe), 128–130
- Policy Service, 98–100**
- Port Address Translation (PAT), 182**
- Portable Operating System Interface (POSIX), 64**
- ports, 7**
 - Assent and H.460.18/19, 188
 - Cisco Webex Hybrid Message Service, 386–388
 - HTTP Allow List, 275
 - HTTPS (Hypertext Transfer Protocol Secure), 275
 - MRA (Mobile and Remote Access) configuration, 242
 - RTP (Real-time Transport Protocol), 256
 - SIP (Session Initiation Protocol), 51
 - SRTP (Secure Real-time Transport Protocol), 256
 - UDP (User Datagram Protocol), 7
 - Webex Video Mesh
 - for audio/video streams, 435–437*
 - for Cisco Webex Meetings traffic, 438*
 - for management, 433–435*
- POSIX (Portable Operating System Interface), 64**
- POST method, 82**
- POTS (plain old telephone service), 8**
- Power over Ethernet (PoE), 6**
- Practice Exam Mode, 456**
- Preferred Architecture for Cisco Webex Hybrid Services, 433, 438*
- prefixes**
 - adding to numerical strings, 66
 - routing, 8
- Premium Edition, 457**
- preparation, for exam, 454–458**
 - exam customization, 456–457
 - exam updates, 457
 - final review/study, 458
 - Pearson Test Prep software, 455–456
 - offline access, 455–456*
 - online access, 455*
 - test-taking tips, 454
- pre-search components, 225–226**
 - Call Policy, 122–128
 - Call Processing Order
 - Call Policy, 122–128*
 - overview of, 114*
 - User Policy (FindMe), 128–130*
 - definition of, 136
 - illustrated flow of, 116–117
 - overview of, 114
 - Transforms, 116–121
 - configuration of, 118–121*
 - definition of, 117–118*
 - example of, 118–121*
 - Pre-Search, 117*
 - Search Rule, 117*
 - User Policy (FindMe), 128–130
- Pre-Search Transforms, 117, 118–121**
- Presence Servers, SIP, 53**
- priority**
 - Call Policy, 123–124
 - Search Rules, 154–155
- private branch exchanges (PBXs), 304, 417**
- private SRV (Service) records, 253**

privileges, user, for Cisco Webex, 338–340

Product Activation Key (PAK) licenses, 14, 16, 31–32

Product License Registration Portal, 32

profiles

- SIP Trunk Security Profile, 170–171, 242
- User Profiles, 268

Protocol setting

- Policy Service, 99
- Search Rules, 155

Protocols command (Configuration menu), 96

Protocols menu commands

- H.323, 48, 58, 96, 211, 390
- Interworking, 55
- SIP, 53, 58

provisioning Webex Video Mesh, 440

proxy solutions

- Cisco Webex Hybrid Calendar Service, 355–356
- SIP (Session Initiation Protocol), 53
- Webex Edge for Devices, 412–413
- Webex Video Mesh, 429–430

PSAP (Public Safety Answering Point), 304

PSTN (public switched telephone network), 126, 304, 305, 417, 418.
See also H.323 protocol

PTR (Pointer) records, 214

public key infrastructure (PKI), 241, 251

Public Safety Answering Point (PSAP), 304

public SRV (Service) records, 252

public switched telephone network (PSTN), 126, 304, 305, 417, 418.
See also H.323 protocol

public-key encryption, 255

push notifications, Cisco Unified Communications Manager, 245

PUT method, 82

Q

Q.931 messaging system, 10

QoS (quality of service), 420

- DSCP (Differentiated Service Code Point), 37–38
- Webex Edge Connect, 418–420
- Webex Video Mesh
 - disabled*, 436–437
 - enabled*, 438

Quality of Service command (System menu), 37

queries, DNS Lookup, 230–231

question mark (?), 64

R

RAM (random-access memory), oversubscription of, 27

RAS (Registration, Admission, and Status), 9, 48

rational expressions. *See* regular expressions (regex)

RCF (Registration Confirm), 9, 95–96, 106

Reactivate User command, 388, 399

Real-time Transport Control Protocol (RTCP), 10, 40, 48, 70

Real-time Transport Protocol (RTP), 7, 10, 40, 48, 70, 256

Recording and Content Management privilege (Cisco Webex), 338

records

- DNS (Domain Name System), 59, 241, 251–254
 - A*, 200, 251

- MRA (Mobile and Remote Access)*, 241
- NAPTR (Name Authority Pointer)*, 154, 200, 230
- PTR (Pointer)*, 214
- SRV (Service)*, 153, 204, 214, 251–254
- Firewall Traversal Services, 241
- redundancy, clustering and**, 210
- regex**. *See* regular expressions (regex)
- Regex to Match Against Certificate field (Client Certificate Testing tool)**, 233
- Region Information command (System menu)**, 267, 295
- REGISTER message**, 52
- Registrar, SIP**, 6, 29, 51–55
- registration**, 210
 - authentication, 101–106
 - configuration*, 101–106
 - definition of*, 100
 - encryption standards*, 101
 - direct, 5
 - Expressway connector, Cisco Webex Hybrid Message Service, 392–394
 - H.323 protocol, 8–9
 - logs for, 222–225
 - By Alias*, 222
 - By Device*, 222
 - Event*, 223–225
 - History*, 222
 - Membership Rules, 106–112
 - Alias Pattern Match*, 111
 - creating*, 111–112
 - subnet masks*, 109–110
 - MRA (Mobile and Remote Access)*, 291–292
 - overview of, 6, 92
 - Registration Authentication, 101–106
 - configuration*, 101–106
 - definition of*, 100
 - encryption standards*, 101
 - Registration Conflict Policy, 94–96
 - Registration Restriction Policy, 96–100
 - Allow List/Deny List policies*, 97–98
 - enabling*, 97
 - Policy Service*, 98–100
 - SIP (Session Initiation Protocol), 5–7
 - step-by-step process for, 220–222
 - Time to Live setting, 95
 - troubleshooting for B2B collaboration solutions, 220–225
 - verification of, 57–59
- Registration, Admission, and Status (RAS)**, 9, 48
- Registration Authentication**, 101–106
 - configuration, 101–106
 - definition of, 100
 - encryption standards, 101
- Registration command**
 - Configuration menu, 98–99
 - Status menu, 98, 222
- Registration Confirm (RCF)**, 9, 95–96, 106
- Registration conflict mode field (H.323 configuration)**, 49
- Registration Conflict Policy**, 94–96, 221
- Registration Controls setting (SIP)**, 58
- Registration menu commands**
 - By Alias, 222
 - By Device, 222
 - Configuration, 98–99
 - History, 222
- Registration Reject (RRJ)**, 9, 95, 106

- Registration Rejected - Alias Conflicts with an Existing Registration error, 224
- Registration Rejected - Not Permitted by Policy error, 224
- Registration Rejected - Received from Unauthenticated Source error, 224
- Registration Rejected - Unknown Domain error, 224
- Registration Request (RRQ), 9, 106
- Registration Restriction Policy, 96–100, 221
 - Allow List/Deny List policies, 97–98 enabling, 97
 - Policy Service, 98–100
- Registration UDP port field (H.323 configuration), 49
- Registrations command (Status menu), 59
- regular expressions (regex)
 - compatibility of, 64
 - definition of, 64
 - examples of, 65–66
 - overview of, 62
 - POSIX syntax for, 64
 - for Pre-Search Transform, 118–119
 - reading, 119
 - for Search Rule Transform, 119–120
 - special characters in, 64–65
 - verification with Check Pattern, 66–67
- Reject Registration Conflict Policy, 94–96
- Release Key, Cisco VCS versus Cisco Expressway licensing, 16–17
- remote access. *See* MRA (Mobile and Remote Access)
- Replace setting (Search Rules), 156
- Request for Comments. *See* RFC (Request for Comments)
- Request in Progress (RIP), 9, 106
- request messages
 - ARQ (Admission Request), 9, 116–117
 - CSRs (certificate signing requests), 72, 76, 262–263, 292
 - DHCP (Dynamic Host Configuration Protocol), 6
 - GRQ (Gatekeeper Request), 9
 - RIP (Request in Progress), 9, 106
 - RRQ (Registration Request), 9, 106
- Request Must Be Authenticated setting (Search Rules), 155
- Resources command (Control Hub menu), 434
- Resources menu commands, Call Activity, 434
- Restart Options command (Maintenance menu), 83
- restore process, 43–44
 - within Within restrictions, 137
- reverse HTTPS proxy, 242, 275
- revoked certificate status, 78
- RFC (Request for Comments)
 - RFC 2543, 51
 - RFC 2663, 182
 - RFC 2833, 56–57
 - RFC 3261, 51
 - RFC 3711, 70
 - RFC 4733, 56–57
 - RFC 5280, 72
- Rich Media Services. *See* RMS (Rich Media Session)
- RIP (Request in Progress), 9, 106
- Rivest-Shamir-Adleman (RSA), 255
- RMS (Rich Media Session), 15, 56, 210, 289
- room information, Active Directory, 333–334

Room System licenses, 15, 19, 210–211

root CA certificates, MRA (Mobile and Remote Access), 254–255

round-trip delay tests, 436–437

Route Hunt command (Call Routing menu), 174

Route Hunt menu commands, Route Pattern, 174

Route Pattern command (Route Hunt menu), 174

Routing Prefixes, 8

RRJ (Registration Reject), 95, 106

RRQ (Registration Request), 9, 106

RSA (Rivest-Shamir-Adleman), 255

RTCP (Real-time Transport Control Protocol), 10, 40, 48, 70

RTP (Real-time Transport Protocol), 7, 10, 40, 48, 70, 256

Rule Name setting (Search Rules), 155

rules

- Call Policy, 124–128
- dialing rules, 173–175
- HTTP Allow list, 270–273
 - automatically added rules*, 276–277
 - manually added rules*, 277–278
 - overview of*, 274–275
 - uploaded rules*, 278
- Membership Rules, 106–112
 - Alias Pattern Match*, 111
 - creating*, 111–112
 - subnet masks*, 109–110
- Search Rules
 - configuration*, 155–156
 - overview of*, 154
 - priority of*, 154–155

Rules command (Call Policy menu), 124

S

SAML single sign-on (SSO), 245

SANs (subject alternative names), 242, 256, 291, 294

SDP (Session Description Protocol), 6, 256

Search History, 131, 226–227

Search History command (Status menu), 131

Search Rule Transforms

- configuration of, 118–121
- definition of, 117

Search Rules, 57, 116

- configuration, 155–156
- overview of, 154
- priority of, 154–155
- Unified Communications
 - configuration on, 241, 273

Search Rules command (Dial Plan menu), 273

Secure Hash Algorithm (SHA), 70

Secure LDAP (LDAPS), 327

Secure Real-time Transport Protocol (SRTP), 70, 256

Secure Sockets Layer (SSL), 292

Secure Traversal Test, 233–234

security, 318–319

- administrator authentication, 80–90
 - Advanced Security*, 81–84
 - FIPS140–2 cryptographic mode*, 84–87
 - SSH (Secure Shell) configuration*, 81
- certificates. *See* certificates
- Cisco Webex
 - Hybrid Data Security*, 384
 - Webex Meetings*, 308, 309
- encryption

- asymmetric cryptography*, 255
- Backup and Restore*, 42
- Cisco Webex*, 308, 309, 384
- Diffie-Hellman key exchange*, 255
- FIPS140–2 cryptographic mode*, 84–87
- KMS (Key Management Service)*, 384
- Phone Security Profiles*, 268
- public-key*, 255
- for Registration Authentication*, 101
- Rivest-Shamir-Adleman (RSA)*, 255
- SIP Media Encryption Mode*, 68–72
- symmetric cryptography*, 255
- Webex Meetings*, 309
- FIPS140–2 cryptographic mode, 84–87
 - enabling*, 85–87
 - overview of*, 84–85
- gatekeepers, 9
- hair-pinning, 9, 126–128
- HTTPS (Hypertext Transfer Protocol Secure)
 - certificates with*, 72
 - for Cisco Webex Hybrid Calendar Service with*, 3450
 - for Cisco Webex Hybrid Message Service*, 391
- LDAPS (Secure LDAP), 327
- multitenancy
 - domain certificates*, 88–90
 - SNI (Server Name Indication) protocol*, 87–88
- overview of, 68
- password protection, 42
- SIP Media Encryption Mode, 68–72
- SSL (Secure Sockets Layer), 255
- TLS (Transport Layer Security). *See* TLS (Transport Layer Security)
- Security certificates command (Maintenance menu)**, 356
- Security certificates menu commands, Trusted CA Certificate**, 356
- Security command**
 - Maintenance menu, 73, 74, 75, 77, 88, 232, 234, 262, 273, 353, 391
 - Tools menu, 76
- Security menu commands**
 - API controls, 363
 - Certificate Management, 292
 - Certificate-based Authentication Configuration, 73
 - Client Certificate Testing, 79, 232
 - CRL Management, 77
 - Domain Certificates, 88–90
 - Phone Security Profile, 267
 - Secure Traversal Test, 234
 - Server Certificate, 75, 262
 - SSH Configuration, 81
 - Trusted CA Certificate, 74, 76, 265, 273, 352, 391
- Server address field (Policy Service)**, 100
- Server Certificate command (Security menu)**, 75, 262
- Server Discovery mode**, 52–53
- Server Name Indication (SNI) protocol**, 87–88
- servers**, 4–5
 - CAS (Client Access server), 347
 - content, 57
 - LDAP (Lightweight Directory Access Protocol), 72
 - MBX (Mailbox), 347

- Microsoft Front-End (FE), 214
- OpenLDAP, 102–106
- proxy, 53
 - for *Hybrid Calendar Service*, 355–356
 - Webex Edge for Devices*, 412–413
- SIP Presence Servers, 53
- Unified CM, 273
- VCS (Video Communications Server), 4–5, 15–17, 55, 240, 406
- Service (SRV) records, 59, 153, 204, 251–254
 - private, 253
 - public, 252
- service accounts, Cisco Webex Hybrid Calendar Service, 348
- Service Activation command (Tools menu), 266, 401
- service discovery, Cisco Jabber for Cloud, 449–450
- Service Parameters command (System menu), 269
- Service Selection page (Service Setup Wizard), 31–32
- Service Setup Wizard, 28–34
 - navigating, 31
 - Option Keys page, 32–33
 - Overview page, 31
 - prerequisites, 30
 - Service Selection page, 31–32
 - services that can be hosted together, 29–30
 - skipping, 30
 - Smart Licensing, 33–34
- Services menu commands, Edit Settings, 365
- Session Description Protocol (SDP), 6, 256
- Session Initiation Protocol. *See* SIP (Session Initiation Protocol)
- Session Management Edition (SME), 442
- Session refresh interval field (SIP configuration), 54
- Session Traversal Utilities for NAT. *See* STUN (Session Traversal Utilities for NAT)
- SHA (Secure Hash Algorithm), 70
- shared clusters, Webex Video Mesh, 436
- SIMPLE protocol, 53
- simple video network with flat dial plan, 157, 338–340
- single sign-on (SSO), 322, 388
- single-subnet DMZ deployment scenario, 196
- SIP (Session Initiation Protocol), 5, 29. *See also* registration
 - AOR (Address of Record), 52
 - call setup process, 7–8
 - domain configuration, 36
 - endpoint verification, 56–59
 - initial configuration settings, 51–55
 - authentication*, 221
 - domains*, 54–55
 - proxy mode settings*, 53
 - table of*, 54
 - interworking with H.323, 51, 118–121
 - Media Encryption Mode, 68–72
 - overview of, 5–8
 - Presence Servers, 53
 - Proxy function, 7
 - Registrar, 6, 29, 48, 51–55
 - RFC (Request for Comments), 51
 - support for, 51
 - TLS (Transport Layer Security), 70
 - trunks

- dialing rules, 173–175*
- SIP route patterns, 173–175*
- SIP trunk security profiles, 170–171*
- SIP trunk settings, 171–172*
- Transforms, 175–176*
- troubleshooting, 291*
- Trunk Security Profile, 242*
- URI (Uniform Resource Indicator), 52, 56
- Video Mesh geographic distribution with SIP dialing, 443
- SIP command**
 - Configuration menu, 78
 - Protocols menu, 53, 58
- SIP mode field (SIP configuration), 54**
- SIP protocols and ports field (SIP configuration), 54**
- SIP Route Pattern command (Call Routing menu), 174**
- SIP Station TCP Port Throttle Threshold service parameter (Cisco Unified Communications Manager), 245**
- SIP Trunk Security Profile, 242**
- SIPIdentity schema, 103**
- Small VMs, clustering, 210**
- Smart Accounts, 14–15**
- Smart Licensing, 14–15, 33–34**
- SME (Session Management Edition), 442**
- snapshots, VMware, 44**
- SNI (Server Name Indication) protocol, 87–88**
- Source setting (Search Rules), 155**
- Source Type field, 126**
- square brackets ([]), 64, 119**
- SRT (STUN round-trip) delay, 435, 436–437, 439–440**
- SRTP (Secure Real-time Transport Protocol), 70, 256**
- SRV (Service) records, 59, 153, 204, 251–254**
 - for Expressway clusters, 214
 - private, 253
 - public, 252
- SRV_collab-edge, testing, 449**
- SRV option (DNS Lookup), 230**
- SSH (Secure Shell), 81**
- SSH Configuration command (Security menu), 81**
- SSL (Secure Sockets Layer), 255, 292**
- SSO (single sign-on), 322, 388**
- Standard AXL API Access role, 266, 395**
- Standard CCM End Users group, 451**
- Standard SIP Profile for Cisco VCS, 172**
- Start New Log option, 288**
- State setting (Search Rules), 156**
- Stateful Packet Inspection, 41**
- Static Routes command (Network Interfaces menu), 40**
- static routes, creating, 40–42**
- Status menu commands**
 - Alarms, 235, 287, 397
 - Bandwidth, 234
 - Calls, 229, 289
 - Local Zone, 234
 - Logs, 223
 - Overview, 30, 31
 - Registration, 98, 222
 - Registrations, 59
 - Search History, 131
 - Unified Communications Status, 287, 290
- Status path field (Policy Service), 100**

Stop Logging option, 288**strings**

- adding prefixes to, 66
- reversing order of, 66

Strip setting (Search Rules), 156**structured dial plan**

- complex video network with, 161
- hierarchical video network with, 162–165

Study Mode, for exam, 456**STUN (Session Traversal Utilities for NAT), 183–184, 420**

- round-trip delay tests, 436–437
- SRT (STUN round-trip) delay, 435, 436–437, 439–440

subject alternative names (SANs), 242, 256, 291, 294**subnet masks, 109–110****Subzone bandwidth management, 136–139**

- Downspeed Mode settings, 138–139
- Local Zone settings, 139–140
- per-call restrictions, 136–137
 - In and Out restrictions, 137*
 - Within restrictions, 137*
- restriction modes, 137
- total-bandwidth restrictions, 136–137

Subzone membership, regular expressions with, 64**Subzone Membership Rules command (Local Zone menu), 111****subzones, 106–112**

- creating, 108–109
- Default Subzone, 107
- Links, 107
- Local Zone, 106–112
- Membership Rules for, 109–112
- Traversal Subzone, 107

Subzones command (Local Zone menu), 109**Support Log configuration command (Diagnostics menu), 288****SupportCMR attribute, 440****symmetric cryptography, 255****symmetric networks**

- ICE (Interactive Connectivity Establishment) in, 186
- TURN (Traversal Using Relay NAT) in, 184

synchronization, Active Directory (AD), 326–338

- AD LDS (Active Directory Lightweight Directory Services), 322–323
- avatar synchronization, 332–333
- Cisco Directory Connector automatic upgrades, 329
- enabling, 326–327
- full synchronization, 335–338
- incremental synchronization, 335
- LAN Settings, 327–329
- notifications, 334–335, 337–338
- Object Selection, 329–330
- overview of, 318–319
- room information synchronization, 333–334
- User Attribute Mapping, 330–332

system configuration, Cisco Expressway

- Backup and Restore, 42–44
 - backup process, 42–43*
 - encryption, 42*
 - password protection, 42*
 - restore process, 43–44*

Expressway deployment on VM, 26–28

- Cisco Expressway on Virtual Machine Installation Guide*, 28
 - ESXi supported versions*, 26–27
 - licensing*, 28
 - MAC addresses*, 28
 - requirements for*, 27–28
 - overview of, 24
 - Service Setup Wizard through web interface, 28–34
 - navigating*, 31
 - Option Keys page*, 32–33
 - Overview page*, 31
 - prerequisites*, 30
 - Service Selection page*, 31–32
 - services that can be hosted together*, 29–30
 - skipping*, 30
 - Smart Licensing*, 33–34
 - System Configuration settings, 34–42
 - Advanced Networking deployment*, 39–42
 - DNS settings*, 34–35
 - dual NIC deployment*, 38–39
 - firewalls*, 38–42
 - NTP settings*, 35–36
 - QoS/DSCP*, 37–38
 - SIP domains*, 36
 - system name*, 34
 - System menu commands**
 - Administration, 34, 232
 - Clustering, 352, 390
 - Device Pool, 267
 - DNS, 34, 87, 289, 294
 - Logging, 225
 - Network Interfaces, 57
 - Protection, 292
 - Quality of Service, 37
 - Region Information, 267, 295
 - Service Parameters, 269
 - Time, 36, 104
 - system names, 34, 212
-
- ## T
-
- Tandberg, 5, 240
 - Target setting (Search Rules), 156
 - TCP (Transmission Control Protocol), 10
 - for Cisco Webex Video Mesh, 435
 - responses for DNS Lookup, 231
 - with SIP (Session Initiation Protocol), 51, 71
 - TCP outbound port start/end field (SIP configuration), 54
 - Telephony Privilege privilege (Cisco Webex), 339
 - Telepresence endpoints, 240
 - Telepresence Management Suite. *See* TMS (Telepresence Management Suite)
 - TelePresence Management Suite Provisioning Extension (TMSPE), 87, 129
 - Telepresence Rooms, 4
 - Terminal Capabilities Set, 10
 - test. *See* exam
 - TFTP (Trivial File Transfer Protocol), 449
 - three-port firewall DMZ deployment scenario, 197
 - throttling policy, Webex Hybrid Calendar Service, 354
 - time. *See* NTP (Network Time Protocol)
 - Time command (System menu), 36, 104
 - Time to Live setting, 50, 58, 95

- TLS (Transport Layer Security), 51, 391**
 - certificates over, 241
 - enforcement of, 352
 - MTLS (Mutual TLS), 259
 - signaling and media encryption with, 70
 - system configuration, 41
 - TLS Verify, 212, 241, 254, 255–258, 259
 - asymmetric cryptography*, 255
 - Diffie-Hellman key exchange*, 255
 - handshake procedure*, 256
 - Rivest-Shamir-Adleman (RSA)*, 255
 - symmetric cryptography*, 255
- TLS handshake timeout field (SIP configuration), 54**
- TMS (Telepresence Management Suite), 6, 34, 129, 213, 367, 408**
 - with Cisco Webex Hybrid Calendar Service with, 347
 - ExternalConferenceData, 350
 - TMSPE (TelePresence Management Suite Provisioning Extension), 87, 129
- TMSPE (TelePresence Management Suite Provisioning Extension), 87**
- tokens, MRA (Mobile and Remote Access), 291**
- toll fraud, 126–128**
- tools, see *individual tools***
- Tools command (Maintenance menu), 132, 227, 230**
- Tools menu commands**
 - Locate, 132, 227
 - Network Utilities, 230
 - Security, 76
 - Service Activation, 266
- total-bandwidth restrictions, 136–137**
- traffic signatures, Webex Video Mesh, 435**
- Transforms, 116–121**
 - configuration of, 118–121
 - definition of, 117–118
 - example of, 118–121
 - for Expressway to Cisco Unified CM Neighbor Zones, 175–176
 - Pre-Search, 117
 - Search Rule, 117
- Transforms command (Dial Plan menu), 122**
- Transmission Control Protocol (TCP), 10**
 - for Cisco Webex Video Mesh, 435
 - with SIP (Session Initiation Protocol), 51, 71
- Transport Layer Security. *See* TLS (Transport Layer Security)**
- Traversal**
 - Chaining, 278
 - Expressway Media Traversal, 187
 - Assent and H.460.18/19*, 188–189
 - Traversal Zone configuration*, 189–196
 - Traversal Zone deployment scenarios*, 196–199
 - traversal call, 15
 - Traversal Zones, 153, 189, 190–193, 216, 254
 - configuration*, 189–196
 - deployment scenarios*, 196–199
 - Traversal Client Zone*, 153, 189, 193–196, 254
 - Unified Communications Traversal*, 241, 278–281
- TURN (Traversal Using Relay NAT), 38, 183, 184–186**

- configurable options for*, 185–186
 - operation within symmetric networks*, 184
- traversal call, 15. *See also* interworking
- Traversal Chaining, 278
- Traversal Client Zone, 153, 189, 193–196, 254
- Traversal command (Configuration menu), 184
- Traversal menu commands, TURN, 184
- Traversal Subzone, 107
- Traversal Using Relay NAT. *See* TURN (Traversal Using Relay NAT)
- Traversal Zones, 153, 189, 190–193, 216, 254
 - configuration, 189–196
 - authentication credentials*, 189–190
 - Traversal Client Zone*, 189, 193–196
 - deployment scenarios, 196–199
 - dual NIC DMZ*, 197–198
 - single-subnet DMZ*, 196
 - three-port firewall DMZ*, 197
 - triple Expressway*, 198–199
 - overview of, 153
 - Traversal Client Zone, 153, 189, 193–196, 254
 - Unified Communications Traversal, 241, 278–281
- Treat As Authenticated authentication policy, 168
- triple Expressway deployment scenario, 198–199
- Trivial File Transfer Protocol (TFTP), 449
- troubleshooting
 - B2B (business-to-business) collaboration solutions
 - additional tools for*, 234–237
 - alarms*, 235–236
 - bandwidth monitoring logs*, 234
 - calling issues*, 225–229
 - certificate issues*, 232–234
 - Configuration Log*, 235
 - Diagnostic Logging tool*, 236–237
 - DNS issues*, 230–232
 - overview of*, 218–219
 - registration issues*, 220–225
 - Cisco Webex Hybrid Message Service, 399–402
 - IM&P (IM and Presence), 400–402
 - Links and Pipes bandwidth management, 234
 - MRA (Mobile and Remote Access)
 - alarms*, 287
 - call status information*, 289–290
 - Cisco Jabber sign-in issues*, 292–294
 - Collaboration Solutions Analyzer*, 287
 - diagnostic logs*, 288–289
 - DNS Lookup*, 289
 - error codes*, 294–295
 - FQDN (fully qualified domain name)*, 289
 - general techniques*, 287–291
 - IM and Presence Intercluster Sync Agent*, 294
 - MRA authentication status and tokens*, 291
 - overview of*, 284
 - registration and certificate issues*, 291–292
 - Unified Communications Status*, 287, 290, 291
- trunks, SIP, 170–171

- configuration
 - dialing rules*, 173–175
 - SIP route patterns*, 173–175
 - SIP trunk settings*, 171–172
 - Transforms*, 175–176
- Trusted CA Certificate command (Security menu), 74, 76, 265, 273, 353, 356, 391
- Trusted CA Certificates, 74–75, 265, 273, 356–357, 391
- TURN (Traversal Using Relay NAT), 19, 21, 38, 183, 184–186
 - configurable options for, 185–186
 - operation within symmetric networks, 184
 - TURN Relays, 21, 210–211
- TURN command (Traversal menu), 184

U

- UCaaS (Unified Communications-as-a-Service), 300–301
- UCCapabilities, 350
- UDP (User Datagram Protocol)
 - for Cisco Webex Video Mesh, 435
 - DNS Lookup responses, 231
 - NAT (Network Address Translation) and, 183
 - ports, 7, 435–437
 - QoS (quality of service) disabled*, 436–437
 - QoS (quality of service) enabled*, 438
 - SIP (Session Initiation Protocol) supported by, 51
- UDS (User Data Service), 294
- unauthenticated callers, 125, 127–128
- Unified CM. *See* Cisco Unified Communications Manager (Unified CM)
- Unified Communications command (Configuration menu), 270, 273
- Unified Communications menu commands
 - HTTP Allow List, 277, 278
 - IM and Presence Service Nodes, 273
 - Unified CM Servers, 273
 - Unity Connection Servers, 273
- Unified Communications Status, 287, 290, 291
- Unified Communications Traversal, 153, 241, 278–281
- Unified Communications-as-a-Service (UCaaS), 300–301
- Unified Workspace Licensing (CUWL), 11–13, 15
- Uniform Resource Indicators (URIs), 6, 35, 52, 56, 58, 76
- Uniform Resource Locators (URLs), 324, 413–416
- Unity Connection Servers command (Unified Communications menu), 273
- Universal Measurement and Calibration Protocol (XCP) router, 55
- unknown certificate status, 78
- updates
 - on book’s companion website, 486–487
 - CRLs (certificate revocation lists)
 - automatic*, 76–77
 - manual*, 77–78
 - exam, 457
- Upload Rules command (HTTP Allow List menu), 278
- uploading rules, 278
- URIs (Uniform Resource Indicators), 6, 35, 52, 56, 58, 76
- URLs (Uniform Resource Locators), 324, 413–416

User Attribute Mapping, Active Directory, 330–332

User Attribute Mapping command (Configuration menu), 331

User Data Service (UDS), 294

User Datagram Protocol. *See* UDP (User Datagram Protocol)

User Email Notifications, Google Calendar, 365

user groups, Standard CCM End Users, 451

User Management menu commands
 Application User, 394
 User Settings, 268

User Policy (FindMe), 128–130

user population, Cisco Webex Hybrid Message Service, 387–388

User Privileges settings (Cisco Webex), 338–340

User Profiles, 268

user provisioning, with Cisco Webex Administration Tool, 447

User Settings command (User Management menu), 268

User Status Report, 372

UserInputCapability, 56–57

UserInputIndication, 56–57

Username field (Policy Service), 100

Username Format field (Client Certificate Testing tool), 233

usernames, obtaining from certificate, 74

userPrincipalName attribute, 385

Users command (Management menu), 339

Users Enabled for Hybrid Message Service status (Hybrid Message Service), 398

Users from All IM&P Clusters (ICSA) status (Hybrid Message Service), 397

Users from Connected IM&P Clusters status (Hybrid Message Service), 397

Users menu commands, OAuth Token Users, 291

Users Not Active for 72 Hours or More status (Hybrid Message Service), 398

V

Vacation Responder. 367

VCS (Video Communications Server), 55, 240, 406
 capabilities of, 5
 Cisco VCS versus Cisco Expressway licensing
Option Key, 15–16
Release Key, 16–17
 End-of-Life and End-of-Sale for, 5
 VCS to Expressway Migration, 4–5

vcs-interop normalization script, 172

Video Communication Server. *See* VCS (Video Communications Server)

Video Mesh (Webex), 312–313, 420–442
 benefits of, 420
 capacity of, 430–432
 cluster deployment, 435–440
cascade architecture, 439–440
cascade link, 438–439
cluster selection for overflow, 439–440
deployment task flow, 440
documentation for, 433

- geographic distribution*, 442
- geographic distribution with SIP dialing*, 443
- guidelines for*, 435–436
- hub-and-spoke architecture*, 442
- node installation for*, 441–442
- on-premise and cloud calls*, 437–439
- overview of*, 435
- ports (UDP) for audio/video streams*, 435–437
- ports and protocols for Cisco Webex Meetings traffic*, 438
- ports and protocols for management*, 433–435
- provisioning*, 440
- round-trip delay tests*, 436–437
- shared clusters*, 436
- supported deployment models*, 439–440
- traffic signatures for*, 435
- integration with call control and meeting infrastructure, 420–423
- overview of, 420
- ports, 420
- proxy solutions, 429–430
- QoS (quality of service) best practices, 420
- supported deployment models, 439–440
- system and platform requirements for, 423–429
- VMNLite call capacity benchmark, 433–434
- WebSocket, 412, 430
- Video Systems privilege (Cisco Webex), 339
- View Currently Blocked Addresses option, 293
- View Detailed MRA Authentication Statistics command, 291
- View Sessions Authorized by User Credentials command, 290
- Viptela, 304
- Virtual Desktop Infrastructure (VDI), Cisco Jabber for, 445
- virtual local-area networks. *See* VLANs (virtual local-area networks)
- Virtual Peering, 304
- virtual private networks. *See* VPNs (virtual private networks)
- Virtualization Technology (VT), 27
- VLANs (virtual local-area networks), 6
- VMNLite call capacity benchmark, 433–434
- VMs (virtual machines)
 - Cisco Expressway deployment on, 26–28
 - Cisco Expressway on Virtual Machine Installation Guide*, 28
 - ESXi supported versions*, 26–27
 - licensing*, 28
 - MAC addresses*, 27–28
 - requirements for*, 27–28
 - Cisco Expressway license limitations, 21
- VMware vSphere, 44, 302
- Voice over IP (VoIP), 51, 307. *See also* SIP (Session Initiation Protocol)
- VoIP (Voice over IP), 51, 169–176, 307. *See also* SIP (Session Initiation Protocol)
- VPNs (virtual private networks), 4, 238
- VT (Virtualization Technology), 27

W

WANs (wide-area networks), 15
 H.323 settings for, 48–51
 Links and Pipes bandwidth management, 142–143
 Video Mesh cluster deployment on, 436
WAPI (WLAN Authentication and Privacy Infrastructure), Cisco Jabber deployments with, 449
 warning alarms, 236
Web Server Configuration, 232
WebACD Preferences privilege (Cisco Webex), 339
Webex. *See* Cisco Webex
Webex Edge. *See* Cisco Webex Edge
Webex Events privilege (Cisco Webex), 339
Webex Support privilege (Cisco Webex), 339
Webex Teams Firewall Traversal, 432
Webex Training privilege (Cisco Webex), 339
Webex Zone, 154
@webex:space syntax, 344
WebSocket, 412, 430
wide-area networks. *See* WANs (wide-area networks)
wizards, Service Setup, 28–34
 navigating, 31
 Option Keys page, 32–33
 Overview page, 31
 prerequisites, 30
 Service Selection page, 31–32
 services that can be hosted together, 29–30
 skipping, 30
 Smart Licensing, 33–34

WLAN Authentication and Privacy Infrastructure (WAPI), 449
workspaces, adding devices to
 for Google Calendar deployment in the cloud, 365–367
 for OBTP (One Button to Push), 375–376
WSS (WebSocket Secure), 412, 430

X

xCommand DefaultLinksAdd command, 107
xCommand RouteAdd command, 40
xConfiguration IP QoS Mode command, 38
xConfiguration IP QoS Value command, 38
XCP (Universal Measurement and Calibration Protocol) router, 55
XMPP (Extensible Messaging and Presence Protocol), 55, 275, 445

Y-Z

Zone search, 116
zones, 139–140, 151–154
 call control using Pipes, 145–146
 clustering and, 214–216
 Default, 152
 DNS, 153, 199–204
 DNS settings, 200, 201–202
 ENUM Zones, 200
 for internal call routing, 199–200
 overview of, 153
 A records, 202–204
 SRV (Service) records, 204
 ENUM, 151, 200
 Local, 151
 Neighbor Zones, 153

- characteristics of*, 165–166
- Expressway to Cisco Unified CM*, 169–176
- Expressway to Expressway*, 166–168
- Subzone bandwidth management, 136–139
 - Downspeed Mode settings*, 138–139
 - Local Zone settings*, 139–140
 - per-call restrictions*, 136–137
 - restriction modes*, 137
 - total-bandwidth restrictions*, 136–137
- subzones, 106–112
 - creating*, 108–109
 - Default Subzone*, 107
 - Links*, 107
 - Local Zone*, 106–112
 - Membership Rules for*, 109–112
 - Traversal Subzone*, 107
- Traversal Zones, 153, 189–196, 216, 254
 - authentication credentials*, 189–190
 - configuration*, 189–196
 - deployment scenarios*, 196–199
 - Traversal Client Zone*, 153, 189, 193–196, 254
 - Traversal Server Zone*, 189, 190–193, 254
 - Unified Communications Traversal*, 241, 278–281
 - Unified Communications Traversal Zones*, 278–281
- Webex Zone, 154
- Zones command**
 - Configuration menu, 166, 273
 - Zones menu, 166