Practice tests

Video Training

Flash Cards

Review Exercises

Study Planner

Official Cert Guide

Advance your IT career with hands-on learning

CCNP and CCIE Collaboration Core

CLCOR 350-801

ciscopress.com

Jason Ball

CCNP and CCIE Collaboration Core CLCOR 350-801 Official Cert Guide

Jason Ball

Published by:
Cisco Press
Hoboken, NJ

ScoutAutomatedPrintCode

Library of Congress Control Number: 2020938427

ISBN-13: 978-0-13-641259-5

ISBN-10: 0-13-641259-9

Warning and Disclaimer

This book is designed to provide information about the CCNP and CCIE Collaboration Core 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.

Microsoft and/or its respective suppliers make no representations about the suitability of the information contained in the documents and related graphics published as part of the services for any purpose. All such documents and related graphics are provided "as is" without warranty of any kind. Microsoft and/or its respective suppliers hereby disclaim all warranties and conditions with regard to this information, including all warranties and conditions of merchantability, whether express, implied or statutory, fitness for a particular purpose, title and non-infringement. In no event shall Microsoft and/or its respective suppliers be liable for any special, indirect or consequential damages or any damages whatsoever resulting from loss of use, data or profits, whether in an action of contract, negligence or other tortious action, arising out of or in connection with the use or performance of information available from the services.

The documents and related graphics contained herein could include technical inaccuracies or typographical errors. Changes are periodically added to the information herein. Microsoft and/or its respective

suppliers may make improvements and/or changes in the product(s) and/or the program(s) described herein at any time. Partial screenshots may be viewed in full within the software version specified.

Microsoft® and Windows® are registered trademarks of the Microsoft Corporation in the U.S.A. and other countries. Screenshots and icons reprinted with permission from the Microsoft Corporation. This book is not sponsored or endorsed by or affiliated with the Microsoft Corporation.

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

Alliances Manager, Cisco Press: Arezou Gol

Director, ITP Product Management: Brett Bartow

Executive Editor: Nancy Davis

Managing Editor: Sandra Schroeder

Development Editor: Christopher A. Cleveland

Senior Project Editor: Tonya Simpson

Copy Editor: Chuck Hutchinson

Technical Editors: TJ Arneson, Jhun De Leon, and Ted Trentler

Editorial Assistant: Cindy Teeters

Cover Designer: Chuti Prasertsith

Composition: codeMantra

Indexer: Ken Johnson

Proofreader: Abigail Manheim

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.**

About the Author

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 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 he 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 old CCNA Collaboration certification. He also wrote the Video Infrastructure Implementation (VII) Advanced Services course for Cisco, and he was the coauthor of the CIVND 210-065 prep book for Cisco Press. Jason currently resides in Raleigh, North Carolina, with his wife and two children.

Dedications

I would like to dedicate this book to my wife of 23 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.

Acknowledgments

Special thanks must be awarded to the two best technical editors. TJ Arneson, your humor and wit are your greatest strengths. You never back down from a challenge, but your kind spirit makes you a great person to be around. I think of you like family. Jhun De Leon, I think I have learned more from you than I have ever taught you. You are a generous and humble person. The depth and breadth of knowledge you have about Collaboration are beyond measure, as is the extent of your friendship. To both of you, thank you, for this book could not have become what it is without your contributions.

I would also like to express my gratitude to Chris Cleveland, development editor of this book. I was so incredibly lucky to work with him again on this text. He is another truly exceptional example of excellence in the workplace. He is the top 1 percent. I'd like to thank Paul Carlstroem, Tonya Simpson, Brett Bartow, and Malobika Chakraborty. They each have worked patiently alongside me to help make this book a reality.

Finally, I would like to dedicate this book to the memory of a friend, colleague, and mentor of mine who passed away in March of 2020. When I first started with Tandberg, many years ago, James Lehto was one of the first mentors I had. He was always tough. He had a great depth of knowledge and he expected others he worked with to have the same depth of knowledge. James also exhibited fairness. If you lacked knowledge, he would help guide you to understanding. This quality made him a great instructor. After Tandberg was acquired by Cisco, James continued to work for Cisco, and as opportunity presented itself, he would use me to develop content or act as a subject matter expert. Through this peer work relationship, we also developed a friendship that I valued to the day he lay to rest. James was the one who suggested I write a book for Cisco Press and recommended me for the CIVND book years ago. If it wasn't for James, I wouldn't have written this book either. A professor I had in college once said, "what good is knowledge, if you never share it." James lived by that motto, and I live by that motto as well. So, as you read this book, remember James Lehto. For the knowledge shared in this book is not just from me, but from him and others who have shared their knowledge with me over the years.

CHAPTER 6

Cisco Solution for Converged Collaboration

This chapter covers the following topics:

Introduction to Cisco Endpoints: This topic will introduce the various Cisco voice and video endpoints available on the market today, including UC phones, soft clients, and Telepresence endpoints.

Introduction to Cisco Call Control: This topic will introduce the Cisco infrastructure that can be used for call control in a Collaboration solution, including the Cisco Unified Communications Manager, Cisco Unified Communications Manager Express, Cisco Expressways, and Webex Control Hub.

Introduction to Cisco Applications: This topic will introduce common Cisco infrastructure applications that enhance the user experience in a collaboration deployment, including Cisco Unity Connection Server, Cisco IM and Presence Service, Cisco Meeting Server, and Management software.

Designing a Cisco Collaboration Solution: This topic will overview the various aspects to designing a Cisco Collaboration solution, including licensing, sizing, bandwidth management, high availability, disaster recovery, dial plan, security, and quality of service.

Establishing a foundation for audio and video communication up to this point has been important. We will revisit key information shared through the first five chapters of this book throughout the rest of the chapters ahead. This chapter, as well as the rest of this book, will focus on specific products in the Cisco Collaboration product portfolio. This chapter will not cover an exhaustive list of all Cisco Collaboration products, and not every product mentioned in this chapter will be covered in later chapters. The purpose of this chapter is merely to provide a high-level overview of the main components available in a Cisco Collaboration solution. Topics discussed in this chapter include the following:

- Introduction to Cisco Endpoints
  - UC Phones
  - Soft Clients
  - Telepresence Endpoints
- Introduction to Cisco Call Control
  - Cisco Unified Communications Manager
  - Cisco Unified Communications Manager Express

- Cisco Expressways
- Webex Control Hub

- Introduction to Cisco Applications
  - Cisco Unity Connection Server
  - Cisco IM and Presence Service
  - Cisco Meeting Server
  - Management Software
- Designing a Cisco Collaboration Solution
  - Licensing
  - Sizing
  - Bandwidth
  - High Availability
  - Disaster Recovery
  - Dial Plan
  - Security
  - QoS

This chapter covers the following objectives from the Cisco Collaboration Core Technologies v1.0 (CLCOR 350-801) exam:

1.1 Describe the key design elements of the following, pertaining to the Cisco Collaboration architecture as described in the SRND/PA:

- 1.1.a Licensing (Smart, Flex)
- 1.1.b Sizing
- 1.1.c Bandwidth
- 1.1.d High availability
- 1.1.e Disaster recovery
- 1.1.f Dial plan
- 1.1.g Security (certificates, SRTP, TLS)
- 1.1.h QoS

1.3 Configure these network components to support Cisco Collaboration solutions:

- 1.3.a DHCP
- 1.3.b NTP
- 1.3.c CDP

- 1.3.d LLDP
- 1.3.e LDAP
- 1.3.f TFTP
- 1.3.g Certificates

"Do I Know This Already?" Quiz

The "Do I Know This Already?" quiz allows 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 6-1 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."

Table 6-1 "Do I Know This Already?" Section-to-Question Mapping

Foundation Topics Section	Questions
Introduction to Cisco Endpoints	1–2
Introduction to Call Control	3–6
Introduction to Cisco Applications	7–9
Designing a Cisco Collaboration Solution	10–14

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. What soft clients does Cisco offer in its current product portfolio? (Choose three.)
   - **a.** Jabber Client
   - **b.** Jabber Video for Telepresence
   - **c.** Webex (Meet, Team, Call)
   - **d.** CMS
   - **e.** WebRTC
   - **f.** CMA
2. Which of the following Cisco Telepresence endpoint category markings is used for personal endpoints?
   - **a.** DX
   - **b.** MX
   - **c.** SX
   - **d.** IX
   - **e.** Webex endpoint

3. What is the maximum number of DHCP addresses that can be delivered and managed by a CUCM?
   a. 10
   b. 100
   c. 1000
   d. 10,000
4. What is the maximum user capacity on the Cisco Unified Communications Manager Express?
   a. 150
   b. 250
   c. 350
   d. 450
5. What is the primary difference between a Cisco VCS and a Cisco Expressway Server?
   a. Cisco VCS has user-based licenses, but an Expressway has device-based licenses.
   b. Cisco VCS has device-based licenses, but an Expressway has user-based licenses.
   c. VCS is used autonomously, and the Expressway is used with CUCM exclusively.
   d. VCS is used exclusively with the CUCM, and the Expressway is autonomously.
6. Which Webex tool can be used to call into a Webex Meeting?
   a. Webex Meeting application
   b. Webex Teams application
   c. Webex Calling application
   d. All the above
7. Which of the following applications can offer voicemail services to UC phones? (Choose two.)
   a. CUCCE
   b. CUCCX
   c. CUC
   d. CUE
   e. IMP
   f. CUCM
   g. CMS
   h. Expressway
8. Which of the following is a service offered through CMS?
   a. Voicemail integration
   b. Manual creation of users
   c. Microsoft Skype for Business Integration
   d. Direct endpoint registration to the server

9. Which of the following management tools allows conference meetings to be scheduled?
   a. Telepresence Management Suite
   b. Prime Collaboration Provisioning
   c. Prime Collaboration Assurance
   d. Prime Collaboration Analytics
   e. Telepresence Management Suite and Prime Collaboration Provisioning
10. Which of the following options is included with a CUCL Enhanced license?
   a. Unity Connection
   b. Expressway Firewall Traversal
   c. PMP Basic
   d. Webex Conferencing
11. How many endpoints can a BE6000H server that is running CUCM support?
   a. 1000
   b. 1200
   c. 2500
   d. 5000
12. What is the maximum number of peers supported in an Expressway Cluster?
   a. 4
   b. 6
   c. 8
   d. 10
13. What protocol is used to secure SIP signaling across the CUCM?
   a. HTTPS
   b. SSL
   c. TLS
   d. AES128
14. What is Layer 2 QoS called?
   a. Cost of service
   b. Class of service
   c. DiffServ
   d. IntServ

Foundation Topics

Introduction to Cisco Endpoints

Cisco has spent the last several years restructuring its Collaboration endpoint portfolio to bring out a line of endpoints that offer cutting-edge technology in a sleek design at a reasonable price. All Cisco Collaboration endpoints can be divided into two main categories: Unified Communications (UC) endpoints and Telepresence endpoints. Some UC endpoints are voice-only, and others support high-definition (HD) video. Some of the soft clients available fall into the UC category as well. All Telepresence endpoints are HD video-capable and offer

more features for the end user. The Cisco Unified Communications Manager treats these two types of collaboration endpoints differently in regard to QoS.

UC Phones

Cisco voice over IP (VoIP) phones are user-friendly and full-featured to meet the needs of entire organizations. They range from a company lobby phone to the desks of the busiest managers and C-level employees. Cisco's VoIP phones provide all the features companies use from their office deskphones, such as speakerphone, transfer, hold, and voicemail access, as well as interactive video collaboration and the capability for a PC to use the same network connection as the phone. Some different models support Bluetooth, USB, Wi-Fi, and other advanced features. Some phones have a built-in camera with HD capabilities. Each phone connects back to the Cisco UCM using the Session Initiation Protocol (SIP) and comes equipped for Power over Ethernet (PoE), which can be supplied by many Cisco switches. Alternatively, a power supply can be used in conjunction with the phone. Cisco has narrowed its VoIP phone product portfolio to three categories of phones: the 3900 series, the 7800 series, and the 8800 series phones. DX series phones fit in this category as well if they are still running the Android software. Support for Android software on the DX endpoints was end of life as of October 1, 2018. Cisco strongly recommends migrating the software on these phones to the Cisco Telepresence CE software.

Soft Clients

Another product in the Cisco UC phone category is the Cisco Jabber client. This software phone can be installed on any Microsoft Windows or Apple Mac computer. An app version is also available on Android and Apple IOS devices, including phones and tablets. Jabber client phones can be configured in the Cisco Unified Communications Manager using the Cisco Unified Client Services Framework (CSF) for PC clients. Cisco Jabber client applications provide instant messaging (IM), presence, voice and video communication, voice messaging, desktop sharing, and other collaborative workspace capabilities that support 1080p30 high-definition video interoperability. The CPU must be Intel Core i5 or later, with a bandwidth of between 2 and 4 Mbps, and the client must be running version 12.6 or later. The Cisco Jabber client uses the Cisco Precision Video Engine and ClearPath technology to optimize video media. The Cisco Precision Video Engine uses fast video-rate adaptation to negotiate optimum video quality, based on network conditions. These clients can be used on premises or through a Hosted Collaboration Solution (HCS) in the cloud. No matter what platform you choose to operate this client from, Cisco Jabber clients provide a consistent experience across devices.

Cisco Unified Client Services Framework is a software application that combines several services into an integrated client. An underlying framework is provided for integration of Cisco UC services, including audio, video, web collaboration, visual voicemail, and more, into an IM and Presence application. As mentioned previously, Cisco Jabber is based on the Cisco Unified Client Services Framework and combines advanced collaborative media features with Cisco UC. Cisco Jabber uses SIP for call control, XMPP for IM and Presence, and Computer Telephony Integration (CTI) for desktop IP phone control. You can use CTI to take advantage of computer-processing functions while making, receiving, and managing telephone calls. CTI applications allow you to perform such tasks as retrieving customer information from a database using a caller ID, or working with the information gathered by an interactive voice response (IVR) system to route a customer's call, along with that caller's information, to the appropriate customer service representative.

Key Topic

Cisco Jabber operates in one of two modes: deskphone mode or softphone mode. In deskphone mode, the Cisco Jabber client controls the Cisco IP phone of the user. Should a call be placed from the Jabber soft client, the video phone connected will actually launch the call and use its own resources for audio and video. The same thing is true for answering incoming calls using Jabber in deskphone mode. For an IP phone without a camera, the video input and output are processed on the Cisco Jabber client platform, but the voice input and output are processed on the IP phone. A protocol known as Cisco Audio Session Tunnel (CAST) is used to split the audio and video media between the two destinations. In softphone mode, the Cisco Jabber client behaves like any other IP phone and originates and terminates all audio and video communication interactions using the computer resources upon which it is running.

The Cisco Meeting Application, or CMA, is another soft client application that can run on a computer, smartphone, or tablet. CMA is built on the WebRTC protocol and is dependent on the Cisco Meeting Server, or CMS. CMA is capable of audio-only calling, HD video calling, and instant messaging. Through proper integrations configured on the Cisco Meeting Server, CMA is completely interoperable with Microsoft Skype for Business. Cisco is no longer developing CMA, but development and support of WebRTC will continue. Cisco has been bolstering the Cisco Jabber application to replace CMA. For more information on these added capabilities to Jabber, see Chapter 26, "Users and Cisco Jabber Soft Clients."

Key Topic

Cisco Webex Teams is a cloud-based application that can be installed as an application on a computer, smartphone, or tablet. Originally, Webex Teams was called Cisco Spark, but Cisco decided to combine its two cloud-based solutions into a single and more powerful solution to bring more control and capabilities into the hands of users. Although the primary purpose of the Webex Teams application is persistent group and point-to-point messaging, it is capable of voice and video calling as well. The scope of this book does not cover Cisco cloud collaboration products and solutions, but watch for more information on this topic in other Cisco Press books or go to Cisco's website to find support documentation for more information.

Telepresence Endpoints

The categorization of Cisco Telepresence endpoints has changed many times over the years Cisco has been developing these products. Currently, Cisco Telepresence endpoints are divided into five categories. The SX endpoints are Solutions Experience endpoints intended for integrators to customize meeting rooms for businesses. The MX endpoints are Meeting Experience endpoints and are all-in-one meeting room solutions that don't require room remediation or integration. These endpoints offer a simple plug-and-play setup that anyone can accomplish. DX endpoints are Desktop Experience endpoints that offer a more personal user experience during meetings. In recent years, a new line of endpoints has been created within Cisco's Telepresence endpoint product portfolio. Webex endpoints, formerly known as Spark endpoints, are contained in a class all their own, although they have some similarities to the MX and SX endpoints. All of these endpoints share a common base code known as Cisco Telepresence Collaboration Endpoint (CE) software, which is based on the legacy Telepresence Codec (TC) software. Therefore, no matter what endpoint is used within an enterprise solution, configuration of each endpoint is the same, and the user experience is the same.

The fifth category of Telepresence endpoints is the Immersive Experience, or IX, room endpoints, which are complete room integration systems that offer 6–18 participants an "immersive experience" as close to an in-person meeting as current technology will allow. These

IX room systems are complex to install and cannot be moved after installation is complete. However, the user experience with these systems is as simple to use as any other Cisco Telepresence endpoint. This category of endpoints is the only Cisco Telepresence endpoint that does not use the Cisco Telepresence CE software. IX endpoints use a Cisco Telepresence System (CTS) software as the base code. There were once many endpoints in the Cisco product portfolio based on the CTS software, but they are all end of sale (EoS). The IX endpoints are the last and only endpoints that use this software, and they went end of sale in October 2019. Table 6-2 outlines all of the current endpoints in each of these categories.

Key Topic

Table 6-2 Cisco Telepresence Endpoint Product Portfolio

DX	MX	SX	IX	Webex Endpoints
DX70 (EoS August 16, 2018)	MX200G2	SX10	IX5000 (EoS October 2019)	Webex Room Kit Series
DX80	MX300G2	SX20	IX5200 (EoS October 2019)	Webex 55 (Single/Dual)
	MX700 (Single/Dual)	SX80		Webex 70 (Single/Dual)
	MX800 (Single/Dual)			Webex Board

Introduction to Cisco Call Control

What good are all these endpoints without a call control system to register to? The Cisco Collaboration solution is a complete end-to-end solution. Cisco is the only solution on the market today that can offer all the switching and routing needs, along with the call control and premium endpoints to connect users regardless of their location. Just as the endpoint portfolio is robust enough to meet the needs of any size company, the Collaboration infrastructure also is a robust and extensive solution with many facets to suit the needs of any customer. On-premises solutions offer call control through the Cisco Unified Communications Manager, the Cisco Expressway series, and the Cisco Unified Communications Manager Express (CME). The on-premises deployment can be extended with additional supporting infrastructure. Unity Connection provides unified messaging services to remote and on-premises endpoints through the Cisco Unified Communications Manager. Unity Express is a unified messaging service that runs on the Cisco Integrated Services Routers (ISRs). The Cisco Unified Communications Manager IM and Presence Service provide native standards-based, dual-protocol, enterprise instant messaging and network-based presence as part of Cisco Unified Communications. For small to medium-sized businesses, Cisco offers subscription-based cloud call control and services. Through partners of Cisco, customers can choose a Hosted Collaboration Solution (HCS), which offers the same on-premises products outlined previously, except hosted in the cloud. Alternatively, Cisco has a relatively new solution to offer to customers. The Cisco Webex Cloud solution (formerly Cisco Spark) allows the registration of endpoints, call control, and IP-to-PSTN connectivity, all managed from the cloud.

Cisco Unified Communications Manager

Cisco Unified Communications Manager extends enterprise telephony features and functions to packet telephony network devices. These packet telephony network devices include Cisco IP phones, media-processing devices, VoIP gateways, and multimedia applications. Additional data, voice, and video services, such as converged messaging, multimedia conferencing, collaborative contact centers, and interactive multimedia response systems, interact with the IP telephony solution through the Cisco Unified Communications Manager API. Cisco Unified Communications Manager provides call processing. Call processing refers to the complete process of routing, originating, and terminating calls, including any billing and statistical collection processes. Cisco Unified Communications Manager sets up all the signaling connections between endpoints and directs devices such as phones, gateways, and conference bridges to establish and tear down streaming connections. The dial plan is a set of configurable lists that Cisco Unified Communications Manager uses to determine call routing. Cisco Unified Communications Manager provides the ability to create scalable dial plans for users. Cisco Unified Communications Manager also extends services such as hold, transfer, forward, conference, speed dial, last-number redial, call park, and other features to IP phones and gateways. Cisco Unified Communications Manager uses its own database to store user information. You can authenticate users either locally or against an external directory. You also can provision users by directory synchronization. With directory synchronization, you can automatically add users from the directory to the local database. Cisco Unified Communications Manager allows synchronization from the following directories to the database:

- Microsoft Active Directory 2003 R1/R2(32-bit)
- Microsoft Active Directory 2008 R1(32-bit)/R2(64-bit)
- Microsoft Active Directory Application Mode 2003 R1/R2 (32-bit)
- Microsoft Active Directory 2012
- Microsoft Lightweight Directory Services 2008 R1(32-bit)/R2(64-bit)
- Microsoft Lightweight Directory Services 2012
- Sun ONE Directory Server 7.0
- OpenLDAP 2.3.39
- OpenLDAP 2.4
- Oracle Directory Server Enterprise Edition 11gR1

Cisco Unified Communications Manager provides a programming interface to external applications such as Cisco Jabber, Cisco Unified IP IVR, Cisco Personal Assistant, and Cisco Unified Communications Manager Attendant Console.

Cisco Unified Communications Manager uses different signaling protocols to communicate with Cisco IP phones for call setup and maintenance tasks, including SIP, SCCP, or even H.323 gateway services. When a calling endpoint dials the number of a called endpoint, dialed digits are sent to Cisco Unified Communications Manager, which performs its main function of call processing. Cisco Unified Communications Manager finds the IP address of the called endpoint and determines where to route the call. Using SCCP or SIP, Cisco Unified

Communications Manager checks the current status of the called party. If Cisco Unified Communications Manager is ready to accept the call, it sends the called party details and signals, via ring back, to the calling party to indicate that the destination is ringing. Cisco IP phones require no further communication with Cisco Unified Communications Manager until either the calling or called endpoint invokes a feature, such as call transfer, call conferencing, or call termination. After the call setup is finished, media exchange normally occurs directly between Cisco IP phones using RTP to carry the audio and potentially video stream.

Key Topic

Cisco Unified Communications Manager depends on some additional network elements. In particular, the Cisco Unified Communications Manager cluster uses external NTP and DNS servers plus DHCP and TFTP services that are used by the endpoints. NTP is a protocol for synchronizing computer system clocks over IP networks. NTP has a hierarchical organization that is based on clock strata. Stratum 0 is an extremely precise clock source, such as an atomic clock or radio clock. A stratum 1 server is directly connected to a stratum 0 clock and can provide time information to other (stratum 2) devices, which in turn serve stratum 3 devices. Cisco Unified Communications Manager typically uses stratum 1 NTP to obtain time information from a time server. Only the publisher sends NTP requests to the external NTP server or servers. Subscribers synchronize their time with the publisher. NTP must be enabled and configured during installation of Cisco Unified Communications Manager. At least one external NTP reference must be reachable and functioning when installing the Cisco Unified Communications Manager publisher to complete the installation. Cisco recommends using a minimum of three external NTP servers in a production environment.

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

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

To ensure that all network devices have the correct date and time, it is recommended that all network devices use NTP for time synchronization.

Key Topic

The Cisco Unified Communications Manager DHCP server is designed to serve IP phones in small deployments with a maximum of 1000 devices. It provides a subset of Windows, Linux, or Cisco IOS DHCP server functionality that is sufficient for IP phones, but it should not be used for other network devices, such as PCs. The DHCP server of Cisco Unified Communications Manager must not be used with deployments of more than 1000 registered

devices. Even if there are fewer devices, the CPU load of the services must be watched closely. If high CPU load is experienced, the DHCP service should be provided by other devices, such as a dedicated DHCP server, switch, router, or another server. Multiple DHCP services can be configured per Cisco Unified Communications Manager cluster. Each Cisco Unified Communications Manager DHCP server can be configured with multiple subnets. In nonattached subnets, DHCP relay must be enabled so that the DHCP requests that were sent out by the clients are forwarded to the DHCP server.

Cisco Unified Communications Manager can use IP addresses or names to refer to other IP devices in application settings. When names are used, they need to be resolved to IP addresses by DNS. Both methods have some advantages. The system does not depend on a DNS server, which prevents loss of service when the DNS server cannot be reached. When a device initiates a connection for the first time, the time that is required to establish the connection is shorter because a DNS lookup sent to the DNS server and a DNS reply sent back from the server are not required. By eliminating the need for DNS, there is no danger of errors caused by DNS misconfiguration. Troubleshooting is simplified because there is no need to verify proper name resolution.

When DNS is used, management is simplified because logical names are simpler to manage than 32-bit addresses. If IP addresses change, there is no need to modify the application settings because they can still use the same names; only the DNS server configuration has to be modified in this case. IP addresses of Cisco Unified Communications Manager servers can be translated toward IP phones because the IP phone configuration files include server names, not the original server IP address, which should appear differently to the IP phone. As long as these names are resolved to the correct address when IP phones send out DNS requests, the NAT is not a problem. If certificates are being used to secure the communications environment, DNS will be required because the DNS FQDN is an integral part of certificates. Although historically Cisco has recommended that DNS not be used, with the increasing need for secure connections, it is best practice to use DNS throughout a Cisco Collaboration environment.

The Cisco Unified Communications Manager is a very powerful tool with many call features to offer to companies of any size. Volumes of books have been dedicated to the many facets the Cisco Unified Communications Manager has to offer. Chapters 15 through 19 of this book will delve into these features, including initial setup considerations, LDAP integrations, registration methods, CAC, and globalized call routing through the Cisco Unified Communications Manager.

Cisco Unified Communications Manager Express

Cisco Unified Communications Manager Express (CME) provides call processing to Cisco Unified IP phones for distributed enterprise branch-office environments. Even branch offices within the same enterprise can have different needs and requirements when it comes to unified communications. Cisco Unified CME delivers on this need by providing localized call control, mobility, and conferencing alongside data applications on Cisco Integrated Services Routers (ISRs). Because the solution is Cisco IOS software-based, Cisco Unified CME is easy to configure and can be tailored to individual site needs. It is feature-rich and can be combined with Cisco Unity Express and other services on the Cisco ISR to provide an all-in-one branch-office solution that saves valuable real estate space. Cisco Unified CME is ideal if you are looking for an integrated, reliable, feature-rich unified communications system for up to 450 users.

Cisco Expressway

The Cisco Expressway Series call control components are based on the Cisco Telepresence Video Communication Server (VCS). In April 2010, Cisco closed on the acquisition of a company called Tandberg, which had a call control solution called the VCS. This call control system is different from the Cisco Unified Communications Manager in many ways; namely, the VCS provides call control only for video devices, whereas the Cisco Unified Communications Manager provides call control for both voice and video endpoints. However, the VCS solution possesses a capability that does not exist in the Cisco Unified Communications Manager. The VCS is capable of true firewall and NAT traversal between the internal network and the public Internet. In an effort to capitalize on this capability, Cisco released the Expressway series that is built on the same operating system (OS) as the VCS. The difference was that endpoints could not register directly to the Expressway series servers. The Expressway series existed to secure proxy registration requests from endpoints outside of the corporate network to the Cisco Unified Communications Manager inside the network without the use of a VPN. This function is known as Mobile and Remote Access (MRA).

Key Topic

In August 2016, Cisco announced that the Expressway series servers would support device registration directly to the Expressway with appropriate licenses. At this point, this announcement confused a lot of people as to what the distinction was between an Expressway and a VCS. The menus were already identical, and the only distinction before was the registration capabilities. This is still the distinction between these two servers. Although registration is allowed on both products, the Cisco VCS allows for device-based licensing, whereas the Expressway allows for user-based licensing. Endpoints can register directly to the Cisco VCS Control or the Cisco VCS Expressway via SIP or H.323. The Expressway Core and Expressway Edge can now also support endpoint registrations directly via SIP or H.323, but the Expressway Edge can also proxy registration requests to the Expressway Core or the Cisco Unified Communications Manager. However, it can only proxy SIP registration requests, not H.323. Table 6-3 compares the differences between the Cisco Expressway and the Cisco VCS.

Key Topic

Table 6-3 Comparison of the Cisco Expressway and the Cisco VCS

Feature	Cisco Expressway	Cisco VCS
Server Components	Expressway Core Expressway Edge	VCS Control VCS Expressway
Registration Licensing	Included with CUCL and CUWL user licenses (Registration supported on X8.9 or later)	Device Registration Licenses required (2500 max per server)
Call Licensing	Internal and mobile calling included Rich Media Session (RMS) Licenses required for B2B and B2C calling	Nontraversal Call Licenses required Traversal Call Licenses required
Microsoft Interop License	Requires RMS licenses	Requires Option Key
FindMe License	Available	Requires Option Key
Device Provisioning License	Requires Option Key (Free)	Requires Option Key (Free)
Clustering Capabilities	Up to 6 servers	Up to 6 servers

I do not know what Cisco's future plans are for these products. At the time this book was written, Cisco had not announced any plans to make either of these products end of sale, and they are both marketed as viable solutions for customers.

Webex Control Hub

Although cloud collaboration goes beyond the scope of this book, it is worth mentioning that Cisco does have a cloud-based call control solution for customers as well. Cisco Webex is a multifaceted cloud-based solution that warrants a deeper explanation on each of the Webex products Cisco has to offer. However, this section will only introduce Cisco Webex as a call control platform. The Cisco Webex solution can be divided into three categories: Meeting, Collaborating, and Calling.

Webex Meetings is the same powerful tool that has been used for years to allow multipoint conferencing in the cloud. Participants can join via a Webex Meeting client, through a browser, using Webex Teams, using Webex Calling, or using a phone or Telepresence endpoint. All the same tools that have traditionally been used with Webex Meetings are still available; plus, Cisco has added a few more enhancements. Webex Meetings allows for high-quality voice and HD video communication, content sharing, polling, annotation, and many more supported features. CMR Cloud through Webex Meetings can be extended to a CMR hybrid meeting deployment using the Video Mesh Node.

Webex Teams, formerly known as Spark, is a client that can be installed on a Windows or Apple computer, tablet, or smartphone. Webex Teams allows for point-to-point messaging or group messaging in Spaces. This highly secure messaging solution allows conversations to be escalated to a voice or video meeting where content can be shared, and a whiteboard application can be leveraged. All whiteboard notations can be saved into a Webex Teams Space so that collaboration can continue after the meeting ends. Webex Teams also supports the upload and download of documents, and many other integrations and bots can be leveraged through this application.

Webex Calling is a tool that has always been available with the Webex solution since the inception of Spark. However, since Cisco acquired BroadSoft, it has been working diligently to bring the BroadSoft calling features into Webex. Webex Calling allows certain phones to register to the Webex Control Hub, and from those phones, users can call out over IP or through the PSTN. Alternatively, a Webex Calling application can be used from any Windows or Mac computer, tablet, or smartphone. Additionally, Webex Calling powered by BroadSoft offers many more calling features than were previously available with Webex Calling.

The Webex Control Hub is the centralized, cloud-based management tool for all Cisco Webex–related products. Calling features, such as endpoint and phone registration and voicemail, are all managed through the Webex Control Hub. Users are also managed from here. Users can be imported through an LDAP integration, and single sign-on can be set up as well. User privileges can be assigned as needed, including additional administrators and security compliance officers. All Webex Meetings, Teams, and Calling features can be configured and managed on an individual basis, based on location or as an organization as a whole. Many different hybrid integrations are available between an on-premises deployment of Cisco Collaboration and the Webex cloud, which are all initiated through the Webex Control Hub. There are too many feature capabilities available through the Webex Control Hub to list here, but one last capability worth mentioning is the many analytics and

troubleshooting tools. They allow administrators to track, manage, and control the Cisco cloud collaboration solution. Cisco Webex is not just for small and medium-sized businesses; it is for any sized business that wants to extend and enhance its global collaboration efforts.

Introduction to Cisco Applications

UC applications are used to unify your voice, video, data, and mobile applications for collaboration within the Cisco Collaboration solutions. Applications include communication gateways, voicemail, and unified IM and Presence services. Other customer collaboration applications, which will not be discussed in this book beyond this chapter, are used to create the foundation for strong customer relationships. These products include contact center and voice self-service products. Media service applications are used to enable collaboration anywhere with more security and high-quality integrated voice, video, and content sharing. These applications include video conferencing products, web conferencing applications, and conferencing management tools.

Cisco Unity Connection Server

Cisco Unity Connection (CUC) is a robust unified messaging and voicemail solution that accelerates collaboration by providing users with flexible message access options and the IT department with management simplicity. You can access and manage messages from your email inbox, web browser, Cisco Jabber, Cisco IP phone, smartphone, or tablet with Cisco Unity Connection. You also can easily prioritize messages and respond quickly to colleagues, partners, and customers. Mobile users, or anyone who simply prefers to do so, can use the speech-activated tools for hands-free message retrieval.

For IT, CUC is an "integrated by design" extension of Cisco Unified Communications Manager. It is easy to manage using Cisco Prime Collaboration, Cisco's single application for unified management of the entire voice and video deployment. Cisco Prime Collaboration simplifies deployment, provisioning, monitoring, and system management. Chapter 23, "Understanding Cisco Unity Connection," and Chapter 24, "Cisco Unity Connection End-User and Voice Mailbox," will delve much deeper into CUC.

Cisco Unity Express (CUE) offers industry-leading integrated messaging, voicemail, fax, automated attendant, interactive voice response (IVR), time-card management, and a rich set of other messaging features on the Cisco Integrated Services Router (ISR) platform. It provides these integrated services specifically designed for small and medium-sized office environments or enterprise branch offices. With Cisco Unity Express, you can easily and conveniently manage your voice messages and greetings right through your web browser using Web Inbox, traditional intuitive telephone prompts, an easy-to-use visual voicemail interface (which is called the Cisco Unity Express VoiceView Express application), email access to messages, and a straightforward GUI that allows simple administration and management.

Cisco Unity Express is an essential component of either a Cisco Unified Communications Manager or Cisco Unified CME Solution. In a Cisco Unified Communications Manager environment, Cisco Unity Express provides local storage and processing of integrated messaging, voicemail, fax, automated attendant, and IVR for branch offices with limited WAN connectivity, thereby alleviating concerns about WAN bandwidth and quality of service (QoS). Additionally, Cisco Unified Communications Manager customers with Cisco Unity Connection unified messaging solutions at their larger locations can use Cisco Unity

Express at their branch-office locations and network the solutions so that employees can easily send messages between locations. In a Cisco Unified CME environment, customers deploy a single Cisco ISR platform with Cisco Unity Express installed to meet their office telephony and messaging needs, as well as their other business communications needs.

Cisco IM and Presence Service

Cisco Unified Communications Manager IM and Presence Service, or IMP, provides native standards-based, dual-protocol, enterprise instant messaging and network-based presence as part of Cisco Unified Communications. This secure, scalable, and easy-to-manage service within Cisco Unified Communications Manager offers feature-rich communications capabilities both within and external to the enterprise.

IM and Presence Service is tightly integrated with Cisco and third-party-compatible desktop and mobile presence and IM clients, including the Cisco Jabber platform, Cisco Webex Social, and Cisco Jabber SDK. It enables these clients to perform numerous functions such as instant messaging, presence, click-to-call, phone control, voice, video, visual voicemail, and web collaboration. IM and Presence Service offers customers and partners the flexibility of rich, open interfaces that enable IM and Cisco's rich network-based presence, as well as IM and presence federation for a wide variety of business applications. Chapter 25, "CUCM IM and Presence Service," will delve much deeper into the Cisco IM and Presence Service.

Cisco Meeting Server

Conferencing is an essential component of any collaboration solution, especially when serving remote users or a large user base. Cisco Rich Media Conferencing offers features such as instant, permanent, and scheduled audio and video conferencing, as well as content sharing. Conference bridges provide the conferencing function. A conference bridge is a resource that joins multiple participants into a single call. It can accept any number of connections for a given conference, up to the maximum capacity allowed for a single conference on that device. The output display for a given party shows all connected parties minus the viewer's own input. Cisco Rich Media Conferencing solutions utilize various infrastructures to provide audio and video conferencing capabilities and content sharing. The conferencing infrastructure can be Cisco Unified Communications Manager using software or DSP resources, Cisco Meeting Server, or Cisco Webex Collaboration Cloud. Cisco Rich Media Conferencing solutions are available as on-premises, cloud, or hybrid deployments. This allows organizations to integrate with the Collaboration solution in which they have already invested or, alternatively, to implement a service that is hosted in the cloud. This is one of the more important distinctions between the various solutions, and it is the first decision point when determining which solution is the best fit for an organization. Cisco Webex Software as a Service (SaaS) offers a completely off-premises solution, while Cisco Collaboration Meeting Rooms (CMR) Hybrid is a solution with a mix of on-premises and off-premises equipment. Organizations that have deployed Cisco Collaboration Systems Releases (CSRs) will benefit most from leveraging an on-premises solution. This section focuses specifically on introducing the CMS product.

Cisco Meeting Server (CMS) is a Rich Media Conferencing product for on-premises deployments only. It cannot be part of a CRM-Hybrid deployment. This robust CMR solution can be deployed as an appliance server or as a virtual machine. Virtual deployments use VMware ESXi hypervisors for deployment. The Cisco Meeting Server appliance server has several options available. Customers who purchased the Acano solution before the Cisco acquisition

can still use the Acano-X appliance server. Newer customers who wish to deploy the Cisco Meeting Server as an appliance can use the Cisco UCS platforms CMS1000 or CMS2000.

CMS offers a consistent one-meeting experience with many features available. However, exactly what features are available may depend on the device that is used to connect to the meeting. Calls can be made using the Cisco Meeting app, a physical endpoint, or through a third-party application. CMS supports both Telepresence Interoperability Protocol (TIP) and non-TIP supported devices. Once connected to a Space, which is what a virtual meeting room is called on CMS, users can set camera and microphone settings, mute or activate a personal microphone, share a screen or an application, chat, change devices, change screen layout, and see caller information to name a few. Bring your own device (BYOD) allows users to use their own devices to see presentations, chat with other participants, or even transfer a call from an endpoint to a smartphone or tablet using CMA.

Additional features of CMS include a seamless integration with Microsoft Skype for Business (S4B), support for WebRTC, and clustering the Database and Call Bridge services for a scalable and resilient deployment. CMS is a rich and robust CMR solution for on-premises deployments. Cisco Meeting Server is a topic that goes outside the scope of this book, so I will not go any deeper into this topic.

Management Software

Management software is a suite of tools that are used to unburden the IT administrator from some of the overwhelming day-to-day maintenance tasks of managing a collaboration network. Management tools are not essential for collaboration solutions to function, but as a network grows, these management tools do ease the stress among the people responsible for keeping all the components of the network functional. Think of what kind of car you need to take a long road trip. You don't need the comforts of leather seats, air conditioning, XM radio, or fine-tuned suspension. All you "need" is something that can get you from point A to point B. However, all those extra amenities sure do make that journey a lot more comfortable. You may even find yourself quite refreshed upon reaching your destination. Management software simply adds extra comforts to the management side of collaboration. There are two management products available in the Cisco Collaboration product portfolio: Telepresence Management Suite (TMS) and Prime Collaboration.

Cisco TMS offers everything from complete control and management of multiparty conferencing, infrastructure, and endpoints, to centralized management of the telepresence network. Flexible scheduling tools are designed to meet the needs of basic users for quick conference creation, including integration with Microsoft Exchange for scheduling through Outlook clients, and to provide advanced conference booking options for IT administrators. This includes One-Button-to-Push meeting access, which is supported in Cisco TMS Version 13.1 and later. Phonebooks can be created and pushed out to all Cisco Collaboration endpoints, and each phonebook can contain a multitiered layer of directories within it. Additional services provided by TMS include backup and restore features, scheduled system upgrades, configuration templates, dial-plan management, and many troubleshooting tools and reports.

Cisco TMS is provided as a software-based application for installation on a customer-provided Microsoft Windows Server with a SQL back end. Any physical server running an appropriate version of Microsoft Windows Server can run TMS, but Cisco recommends using the Cisco UCS server. The Cisco TMS user interface is a web browser-based

application that uses Microsoft Internet Information Services running on the .NET framework. The caveat to using TMS is that it only supports Telepresence products. UC phones and services are not supported through TMS. However, third-party Telepresence endpoints can be managed by TMS. Cisco Prime Collaboration is the management software to use for support of UC services and phones.

Cisco Prime Collaboration helps enterprises address the continuous transformation of their networks as they invest in next-generation collaboration technologies with integrated video and voice deployments. It empowers IT departments to effectively manage this transformation and the video network lifecycle as they meet demands from end users for high-quality solutions everywhere and at all times. At the same time, it addresses the need to reduce operating expenses and optimize limited resources. Prime Collaboration provides simplified, unified management for video and voice networks. This management solution helps ensure superior quality experiences for end users and lower operating expenses for supporting video and voice communication. Prime Collaboration removes management complexity and provides automated, accelerated provisioning, real-time monitoring, proactive troubleshooting, and long-term trending and analytics in one integrated product. This solution delivers a premier operations experience through an intuitive user interface and automated workflows that ease implementation and ongoing administration. Self-Provisioning and Self-Care features allow users to provision their own phones, like the 7800 and 8800 series phones, and change phone settings such as names, directories, and speed-dials. The three modules to contribute to an enhanced management experience from Prime Collaboration include

- Prime Collaboration Provisioning
- Prime Collaboration Assurance
- Prime Collaboration Analytics

As mentioned earlier, Cisco Prime Collaboration Provisioning unifies administration of your UC environment to one interface, including Cisco Unified Communications Manager, Cisco Unified Communications Manager Express, Cisco Unified Communications Manager IM and Presence service, Unity Connection, and Unity Express. It provides one interface for provisioning video, call control, messaging, and presence for a single cluster implementation. It has an intuitive interface that provides a single view of a user and the user's services, as well as a consolidated view of users across the organization. With these capabilities, Cisco Prime Collaboration significantly accelerates site rollouts and dramatically reduces the time required for ongoing moves, adds, and changes by facilitating the delegation of these tasks. This allows organizations to optimize IT resources, resulting in exceptional productivity gains and lowered operating expenses. Prime Collaboration Provisioning comes in Standard and Advanced versions. The Advanced version comes with everything in the Standard version and also includes multicluster and multiversion support for Cisco Unified Communications Manager and Unity Connection, advanced RBAC, ordering workflow, templates, and API support.

Prime Collaboration Assurance provides additional monitoring tools for the Cisco Unified Communications environment, including Cisco Unified Communications Manager, Unity Connection, and Video. It can continuously monitor in real time and do advanced troubleshooting of the environment, sending a notification when a problem arises so that issues can be proactively resolved. For video, it allows viewing of the end-to-end session paths

including jitter and packet loss, with a web-enabled interface for fault monitoring of video components, including a dashboard view. Prime Collaboration Assurance provides efficient, integrated service assurance management through a single, consolidated view of the Cisco video and voice collaboration environment and is offered in Standard and Advanced versions. The Advanced version includes all the components of the Standard version, plus diagnostics, reporting features, multiple cluster management, five access levels, and higher levels of discovery, inventory, fault management, and dashboards.

Cisco Prime Analytics enables network managers to maximize the value of the massive amounts of information available about their network traffic by

- Continuously monitoring live data
- Instantaneously processing queries
- Providing real-time analysis and action
- Efficiently using compute resources

The Analytics module provides historical reporting of key performance indicators and helps enable IT network managers to analyze trends for capacity planning, resource optimization, and quality of service. The solution helps track collaboration technology adoption rates in the network and provides metrics to help analyze how users are actually using the collaboration endpoints on a daily basis. It also provides insights into key collaboration network resource usage trends. With historical data and many reporting options with easy customization, IT managers have access to actionable information, simplifying the long-term planning process contributing to ongoing technology investment decisions, and helping to optimize the network configuration for an improved experience quality for end users. Cisco Prime Collaboration Analytics provides real-time monitoring and support capabilities for real-time communication.

Designing a Cisco Collaboration Solution

There are many factors to consider when designing a Cisco Collaboration solution for a customer. The Collaboration solution could be an on-premises solution, a cloud-based solution, or a hybrid of the two. The type of Collaboration solution being designed will directly impact the licensing used for that solution. The types of services offered to the customer will also impact the licensing model. Then there are sizing considerations that have to be taken into account. When sizing a solution, you should not forget to leave room for expected growth within the customer organization. Bandwidth allocations and CAC need to be planned so that call loads during peak hours do not overtax the network. Sometimes systems break. Therefore, high availability needs to be designed into the Collaboration solution so that appropriate redundancies are in place in the event of key system failures. When systems fail, data can be lost. Disaster recovery components will help ensure data retention during these outages. Then there's the dial plan, which may be one of the most important aspects to designing a Collaboration solution. The dial plan is used during every call, and the complexity of the dial plan will impact many aspects of the overall implementation and usability of the solution. Security is a growing concern in any networked solution. Designing appropriate security measures into the Collaboration solution is equally important. Finally, there is the quality of service design that will coincide with the Collaboration solution. QoS controls how data traffic is routed through the network during high congestion times. As you can

see, there are many aspects to designing a Collaboration solution that must be taken into consideration. Although each one of these topics could fill a chapter or more on its own, the following sections will dip into each one of them to provide a roadmap of the various aspects to consider when designing a Cisco Collaboration solution.

Licensing

Businesses today are as diverse as two snowflakes. These differences bring with them different needs in a workplace that is constantly changing. Layer this complication with a multitude of products ranging from call control devices such as the Cisco Unified Communications Manager, to conferencing applications, such as the Cisco Meeting Server, to cloud solutions, such as Cisco Webex, and contriving a singular license plan that covers the many needs of a business becomes a colossal task. Cisco rose to this charge and devised a licensing solution that can be tailored to any company's needs, regardless of the size of the organization, the solution it's using, or the components needed to meet its needs. As with any Cisco product, understanding the requirements for licensing your product at the time of installation is important.

A great example of the licensing obstacles Cisco has had to overcome, due in part to acquisitions, is the licensing differences between the Cisco VCS and the Cisco Unified Communications Manager. Historically, the Cisco VCS used "device-based" licenses, where licenses were purchased based on the number of devices that were allowed to register. Then additional call licenses were required based on the number of concurrent calls the VCS would allow, complicated even more by the type of call, and traversal or nontraversal call licenses. Cisco devised the Cisco Expressway series that could perform all the functions of the VCS because it is essentially a VCS and uses the same user-based licenses as the Cisco Unified Communications Manager. These licenses are the Cisco Unified Workspace Licensing, or CUWL.

CUWL licenses are broken down into two varieties, with a third possibility being the Cisco User Connect Licensing, or CUCL, which are designed for voice-only solutions in the Cisco Collaboration suite of devices. This program is based on users rather than devices and allows customers to simply purchase licenses based on the number of users they wish to service, with each user having access to multiple devices or services as part of the program. Table 6-4 identifies the CUWL and CUCL licenses and the capabilities included with each license as well as the purchasable options available for each license.

Key Topic

Table 6-4 CUWL and CUCL Licensing Model

	CUCL Essentials	CUCL Basic	CUCL Enhanced	CUWL Standard	CUWL Professional
Number of Devices Supported	One	One	One or Two	Multiple	Multiple
Cisco Prime Collaboration	Included	Included	Included	Included	Included
Jabber/IMP	Included	Included	Included	Included	Included
Jabber UC	N/A	N/A	Included	Included	Included

	CUCL Essentials	CUCL Basic	CUCL Enhanced	CUWL Standard	CUWL Professional
Expressway Firewall Traversal	N/A	N/A	Included	Included	Included
Unity Connection	Optional	Optional	Optional	Included	Included
Webex Conferencing	Optional	Optional	Optional	Optional	Included
PMP Basic	N/A	N/A	Optional	Optional	Included
PMP Advanced	N/A	N/A	Optional	Optional	Optional

Table 6-4 displays nine different components that can come with different licensing levels. Cisco Prime Collaboration is a Prime Collaboration Provisioning standard license that is included with the Cisco Unified Communications Manager. The difference between Jabber/IMP and Jabber UC is that Jabber/IMP refers to the desktop client on Microsoft Windows or Apple Mac computers, and Jabber UC refers to the Jabber application on smartphones and tablets. Expressway Firewall Traversal allows for firewall traversal licenses through the Expressway Core and Expressway Edge servers. This includes MRA capabilities and one RMS license per user. Unity Connection allows voicemail and other services that come with Unity Connection. Webex Conferencing includes one named user license for both Webex Meeting Center and Webex Meeting Server. Webex can be used for cloud-based meeting or Hybrid meetings using the Video Mesh server installed on premises.

To use the on-premises Cisco Meeting Server for multipoint conferences, multiparty licenses are required. Two types of multiparty licenses are available: Shared Multiparty Plus (SMP) and Personal Multiparty Plus (PMP). With the Cisco licensing model outlines in Table 6-4, PMP licenses can be purchased as Basic or Advanced. PMP Basic provides one PMP license per user that will support host meetings on the Cisco Meeting Server for up to four participants in each meeting. PMP Advanced provides one PMP license per user that will support host meetings on the Cisco Meeting Server for an undefined number of participants in each meeting. The number of participants for PMP Advanced licenses is limited only by the infrastructure that has been installed. A huge advantage to PMP licenses is the amount of security and control they offer to the meeting. Other users cannot join personal meeting spaces that have been assigned to each user on the Cisco Meeting Server unless the host to whom the space belongs has joined the meeting. Once the host drops out of a meeting hosted in that space, all other participants will be dropped as well. This feature prevents the meeting resources from being abused by other people. SMP licenses are not part of the licensing model outlined in the table because they are not assigned to any one user. When SMP licenses are added to the Cisco Meeting Server, any user can create and join a meeting using this license. Because SMP does not share the same level of control that PMP licenses do, they should be purchased and used sparingly.

There are some other differences between CUWL and CUCL licenses that should be noted. CUWL standard and professional licenses support multiple endpoints. For example, this license allows for two desktop endpoints for a single user license, allowing for a single user to have an endpoint both at the office and at home. CUCL packages are designed for voice-only solutions, whereas the Expressway series is only used to provide VPN-less traversal services for voice endpoints. Video can be used over CUCL using Jabber or video UC phones, such as 8845 or 8865, but this is not the designed purpose of these licenses. Telepresence endpoints cannot register under the CUCL model. Notice that CUCL supports only one or two devices per user. The idea here is that a user may need to register a VoIP phone and Jabber, or that user may just use a VoIP phone.

Cisco has been using CUWL and CUCL licenses for many years because it has led the market in on-premises infrastructure. In more recent years, a new market has opened up in cloud-based offerings, and Cisco has been working diligently to dominate this market as well. With the need to be able to deliver collaboration services cost-effectively, using on-premises infrastructure or cloud-based services, depending on the needs of employees, Cisco has devised a new layer to its licensing model known as Flex.

The Cisco Collaboration Flex Plan entitles people to use Cisco's industry-leading collaboration tools with one simple subscription-based offer. It helps with transitions to the cloud, and investment protection, by including cloud, premises, hosted, and hybrid deployments, with the flexibility to use them all. Companies can choose to equip employees with meetings, calling, or both, and add more licenses at the time they're needed. Companies can also easily add Contact Center capabilities, which are also included in the Collaboration Flex Plan. One agreement covers software, entitlements, and technical support for cloud-based and on-premises services. Companies simply choose the services they need today and grow at their own pace. There is no need to manage complex agreements. And you can mix and match meetings and calling subscriptions for flexibility and value. With the Flex Plan, you can choose the right subscription based on your business size and needs. Each option includes technical support. Choose from the following purchasing models:

- For enterprisewide deployment, Cisco Enterprise Agreement customers can purchase via the Cisco Collaboration Flex Plan. You can gain maximum value by enabling services for everyone in your organization for meetings or calling or both.
- To purchase meetings according to usage: Cisco Collaboration Flex Plan—Active User Meetings: Anyone can host a meeting, and you pay only for those who use the entitlement.
- To provide meetings and/or calling services to individuals, teams, or departments: Cisco Collaboration Flex Plan–Named User: Your purchase is based on the number of people who need services. You can grow at your own pace.
- To provide contact center services to your service agents: Cisco Collaboration Flex Plan—Concurrent Agent: Your purchase is based on the number of agents simultaneously using services at your peak busy hour. Again, you can grow at your own pace.

At the same time, you can seamlessly drive enhanced team collaboration with Cisco Webex Teams, which is included at no additional charge. Cisco Webex Teams is a great tool to collaborate with other coworkers for ongoing work. Teams can be used on every device, in

every place, to move work forward. You can enable services for selected individuals, teams, or departments, or for your entire organization. And you have the flexibility to add services as adoption grows. To learn more about the Cisco Collaboration Flex Plan, visit

https://cisco.com/go/collaborationflexplan

Cisco introduced a new way to add licenses to on-premises collaboration products called Smart Licensing. Smart Licensing was introduced as an option with Cisco Unified Communication product version 11.5, but it is required for licensing products from version 12.0 onward. Cisco is transforming the end-to-end software lifecycle to make the customers' experience better and easier. A major part of this change is a move away from Product Activation Key (PAK) licenses to Smart Licensing to make the license registration process faster and more flexible. At the heart of the transformation is Smart Licensing and Smart Accounts, which offer streamlined purchasing and software administration. Smart Licensing is a flexible software licensing model that simplifies the way you activate and manage licenses across your organization. The Smart Licensing model makes it easier for you to procure, deploy, and manage your Cisco software licenses. To use Smart Licensing, you must first set up a Smart Account.

A Smart Account is a central repository where you can view, store, and manage licenses across the entire organization. Comprehensively, you can get access to your software licenses, hardware, and subscriptions through your Smart Account. Smart Accounts are required to access and manage Smart License–enabled products. Creating a Smart Account is easy and takes less than five minutes. You can create a Smart Account on cisco.com. Smart Accounts offer a simple-to-use, centralized, and organized solution to license management. With a Smart Account, you get full visibility and insight into all of your Cisco software assets deposited into the Smart Account, including PAK licenses and Enterprise Agreements. When Smart Accounts are used with Smart Licenses, the benefits include

Key Topic

- **Real-Time Visibility:** You can view all of your software licenses, entitlements, and users across the organization.
- **Centralized Management:** A single location enables authorized users to see all license entitlements and move licenses freely through the network as needed.
- **Cost-Effectiveness:** You can drive down the cost of license management with reduced overhead, better utilization management, and more efficient planning.
- **Organization:** Virtual Accounts provide the flexibility to organize licenses by department, product, geography, or other designation, whatever makes the most sense for your company.

Sizing

Capacity planning involves sizing a solution to meet all of the current needs of an organization and have room to scale based on projected growth. This will determine the type of server that should be used for the installation. To illustrate how a server can be selected based on the capacity needed, this chapter will go into some of the Cisco UCS servers to a limited degree. The two primary questions that should be asked when sizing a solution are, "What is the maximum number of users who will utilize these services?" and "What is the maximum number of endpoints that will be used?"

For small and medium-sized businesses (SMB) that need only voice services, Cisco offers a great product to meet these needs. The Cisco Business Edition 4000 (BE4K) is a cloud-managed system that can support up to 200 VoIP phones. It can be preconfigured for the customer by the Cisco partner reseller through the cloud management portal and can be managed by the partner or customer after it has been installed and provisioned. This system will support the 7800 and 88X1 series phones and comes equipped with support for 120 hours of voicemail messages. You can add a 1-, 2-, or 4-port T1/E1 PRI card, or a 2- or 4-port BRI card for digital PSTN connections. You can add a 2- or 4-port FXO card, a 2- or 4-port FXS card, or a 2-port FXS with 4-port FXO combination card for analog PSTN connections. Alternatively, you can build a SIP trunk to your service provider for SIP-to-PSTN connections using the built-in CUBE gateway services.

Another UCS server Cisco offers is the Business Edition 6000 (BE6K), which comes in a Medium density (BE6000M) or High density (BE6000H) platform. The BE6K servers come preloaded with VMware ESXi and all the OVAs and ISOs needed to complete an installation of the VMs once the server has been installed and powered on. The BE6000M has a max capacity of 1000 users per cluster and 1200 endpoints per cluster. The BE6000H has a max capacity of 1000 users per cluster and 2500 endpoints per cluster. Extra nodes can be added for redundancy, but the capacity limits do not change. One of the great benefits to using a BE6K server is that the sizing tool is not needed because capacity limits are preset.

If higher capacity is needed than what the BE4K or BE6K can offer, Cisco has made available a third option called the Business Edition 7000 (BE7K). Like the BE6K, the BE7K comes preloaded with VMware ESXi and all the OVAs and ISOs needed to complete an installation of the VMs after the server has been installed and powered on. The BE7K can be purchased in a Medium density (BE7000M) or High density (BE7000H) platform. It is sized using the sizing tool, and capacity limits increase when extra nodes are added to this server. The BE7K can support up to 10,000 users per node and up to 40,000 users per cluster. It can also support up to 10,000 endpoints per node and up to 40,000 endpoints per cluster.

It should be plain to see that as the complexity of installing the server increases, the capabilities of the server increase as well. Installing the BE4K server is very easy, but it has a limited calling capability, whereas installing the BE7K is much more complex, but it has a significantly higher calling capability. What has not been mentioned before is that in the progression of each server, an increase in features is also supported. The link for the sizing tool is https://tools.cisco.com/cucst. You will have to log in with a CCO account and be associated with a Cisco partner company to access the sizing tool.

Bandwidth

Three main aspects to bandwidth must be considered when designing a Collaboration solution. First, you must consider the audio and video components being used. This includes everything discussed in Chapters 3–5 and much more. Codecs used, scan rate, compression algorithms, environmental conditions, and many other aspects can positively or negatively impact bandwidth. Second, QoS can affect bandwidth utilization. This topic will be discussed later in this chapter and in more depth in Chapter 12, “Cisco Core Network Components.” Third, provisioning and admission control allow you to set up parameters within the collaboration environment so that you can more closely observe and manage bandwidth.

Provisioning bandwidth and ensuring that the correct bit rate is negotiated between various groups of endpoints are important aspects of bandwidth management. In a Cisco Unified Communications Manager environment, bit rate is negotiated via Cisco Unified Communications Manager, which uses a concept of regions to set the maximum audio and maximum video bit rates for any given call flow. Cisco Unified Communications Manager locations work in conjunction with regions to define the characteristics of a call flow. Regions define the type of compression or bit rate that is used between any two devices. Location links define the amount of available bandwidth for the path between devices. Each device and trunk in the system is assigned to a region, by means of a device pool, and a location, by means of a device pool or by direct configuration on the device itself.

- Regions allow you to set the per-call bandwidth of voice and video calls. The audio limit on the region can result in filtering out codecs with higher bit rates. However, for video calls, the video limit constrains the quality (resolution and transmission rate) of the video.
- Locations define the amount of total bandwidth available for all calls to another location. When a call is made on a link, the regional value for that call must be subtracted from the total bandwidth allowed for that link.

Building a region matrix to manage maximum voice and video bit rate (video resolution) for groups of devices can assist in ensuring that certain groups of devices do not oversaturate the network bandwidth. When creating a region matrix, you should group devices into maximum video bit rate categories. The smaller the number of groups, the easier it is to calculate bandwidth requirements. Also, you should consider the default region settings to simplify the matrix and provide intra-region and inter-region defaults. There are other region considerations for bandwidth provisioning. The first consideration is whether to have different intra-region settings versus inter-region settings. This will determine whether per-site regions are required or not. The concept here is that if intra- and inter-regional audio or video bit rates are to be different, per-site regions will be required. This augments the configuration of regions to the number of sites (N) multiplied by the number of video groups (X): N*X = number of regions required on average. If intra- and inter-regional audio and video bit rates will be the same, only the regions for the video groups are required (X).

Another consideration is to reuse regions configured for audio-only IP phones when possible. Audio codec configuration is shared, so if video calls need to use different audio codecs, you need to configure new regions. For example, if voice-only devices use the G.729 audio codec over the WAN and G.711 or G.722 on the LAN while video devices always use G.711 or G.722, the voice-only and video endpoints cannot share a region. Thus, each site would require a region per group of devices. Sites = N, and video region groups = 4 + voice-only region group; then N*4 is the number of regions required. You can use the Prime Collaboration Provisioning tool or the Bulk Administration Tool as configuration aids. Per-site regions might not be needed if a single audio codec is used for both intra-region and inter-region calls as well as voice-only calls. If both audio and video endpoints use G.711 or G.722 over the WAN and LAN for voice-only or video calls, voice-only IP phones and video endpoints could use the same region. You should consider the default region settings to simplify the matrix.

The Call Admission Control (CAC) function can be an important component of a Collaboration system, especially when multiple sites are connected through an IP WAN and limited

bandwidth resources are available for audio and video calls. Consider for a moment that traditional TDM-based PBXs operate within circuit-switched networks, where a circuit is established each time a call is set up. As a consequence, when a legacy PBX is connected to the PSTN or to another PBX, a certain number of physical trunks must be provisioned. When calls have to be set up to the PSTN or to another PBX, the PBX selects a trunk from those that are available. If no trunks are available, the call is rejected by the PBX and the caller hears a network-busy signal.

Now consider an IP-connected Unified Communications system. Because it is based on a packet-switched IP network, no circuits are established to set up an IP telephony call. Instead, the IP packets containing the voice samples are simply routed across the IP network together with other types of data packets. Quality of service (QoS) is used to differentiate the voice packets from the data packets, but bandwidth resources, especially on IP WAN links, are not infinite. Therefore, network administrators dedicate a certain amount of "priority" bandwidth to voice traffic on each IP WAN link. However, after the provisioned bandwidth has been fully utilized, the IP telephony system must reject subsequent calls to avoid oversubscription of the priority queue on the IP WAN link, which would cause quality degradation for all voice or video calls. This function is known as Call Admission Control, and it is essential to guarantee good voice and video quality in a multisite deployment involving an IP WAN. To preserve a satisfactory end-user experience, the CAC function should always be performed during the call setup phase so that, if network resources are not available, a message can be presented to the end user, or the call can be rerouted across a different network (such as the PSTN).

High Availability

The next consideration when planning a call processing deployment should be high availability and redundancy within the solution. This involves planning clusters of the call agents being used and configuring proper redundancy. This also involves planning redundancy in power being supplied to the hosting servers along with uninterruptible power supply (UPS) sources. Finally, this involves planning high availability in the network connectivity.

As it pertains to call processing, clustering is a grouping of call agents that work together as a single call processing entity with higher capacity. Multiple Cisco Unified Communications Managers can be clustered together, multiple VCSs can be clustered together, and multiple Cisco Expressways can be clustered together. However, there is no cross-cluster between different call agents, such as the VCS and Cisco Expressway, the VCS and Cisco Unified Communications Manager, or the Expressway and the Cisco Unified Communications Manager. However, different call agent clusters can be trunked together in order to unify communications. The Cisco Unified Communications Manager cluster can be trunked to a VCS cluster, Cisco Expressway cluster, and another Cisco Unified Communications Manager cluster.

The Cisco Expressways and VCSs can support up to six peers in a cluster. One of the peers in the cluster is designated as the master, and all settings under the Configuration menu on the master are replicated to each of the other peers in the cluster. If any of these configuration settings are changed from any peer in the cluster that is not the master, those changes will immediately be overwritten by the master of the cluster. Settings under the Applications menu can be configured from any peer in the cluster, and these settings will be replicated to

all other peers in the cluster. Therefore, a round-trip delay time between any peer in the cluster should not exceed 30 ms, or 15 ms each one-way direction. In the event the master goes down, the next subsequent peer listed will assume the role of the master. When configuring a cluster of Cisco Expressways or VCSs, you need to configure each peer with a unique IP address, URL, and system name, but they should share the same cluster name, which should be in the form of a URL. The system URL should resolve to a DNS A-record for that particular call agent. The cluster URL should resolve to all call agents in the cluster using round-robin for distribution and load balancing.

Key Topic

Clusters in the Cisco Unified Communications Manager behave differently than that of the VCSs or Cisco Expressways. A Cisco Unified Communications Manager cluster is made up of two different service node types: the publisher and the subscriber. The publisher is essentially the master of the cluster, and each cluster can have only one publisher. Each subsequent node in a cluster is referred to as a subscriber. If you are installing a Cisco Unified Communications Manager for the first time, and you do not plan to establish a cluster, the one node is still designated as the publisher. You can then establish a cluster at a later time by setting up the required number of subscriber nodes. The publisher node is the only node in a cluster with full read-write access to the configuration database. Should the publisher go down, all services will continue to operate normally, and user-facing configuration changes to the database can be made during a publisher outage. Information is then synced to the publisher when connectivity is re-established. No other services can be written to the database when the publisher is down. Peers in a Cisco Unified Communications Manager cluster are referred to as *service nodes* because they can be grouped based on services they offer. Common service groupings include Call Processing, TFTP, Media Resources, Computer Telephony Integration (CTI) Manager, and Unified CM Applications. Figure 6-1 illustrates a Cisco Unified Communications Manager cluster with various service nodes grouped together.

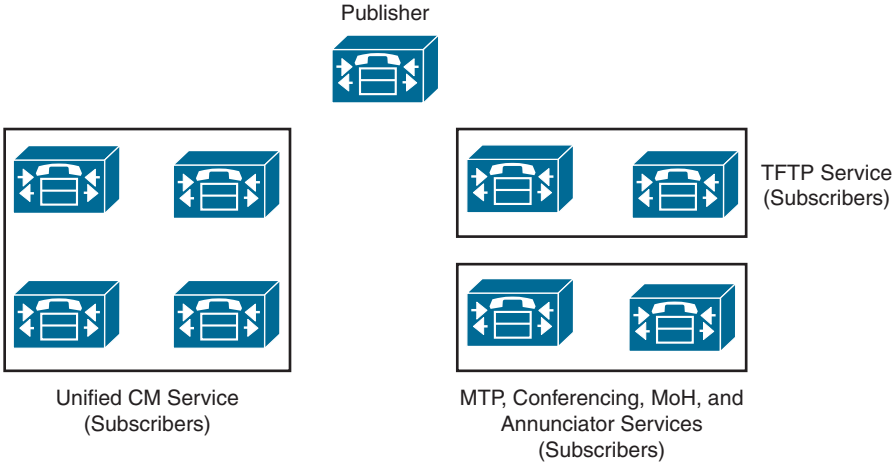

Figure 6-1 *CUCM Cluster with Service Nodes*

Key Topic

In addition to establishing service groups within a Cisco Unified Communications Manager cluster, you can also configure redundancy groups for call processing failover in the event a Cisco Unified Communications Manager within the cluster crashes. There are two options for configuring redundancy groups: a two-to-one (2:1) option and a one-to-one (1:1) option.

With the 2:1 option, there is one shared backup call processing subscriber for every two primary call processing subscribers. In the event one of the primary call processing subscribers crashes, the backup will immediately assume the role until such time the failed subscriber can be restored. However, should both primary call processing subscribers fail, the backup will be able to assume the role of only one of the primary call processing subscribers; therefore, a loss in call processing capabilities will be encountered. When the cluster is being upgraded, these redundancy groups can help maintain call processing while each primary subscriber is being rebooted. The upgrade order of sequence is to fully upgrade and reboot one of the primary subscribers first, then do the same for the second primary subscriber, and last should be the backup subscriber. Figure 6-2 illustrates how a 2:1 group of call processing subscribers can be used within the Cisco Unified Communications Manager dependent on the size of the deployment. Only two examples are provided, but many combinations exist based on the capacity of the cluster being deployed.

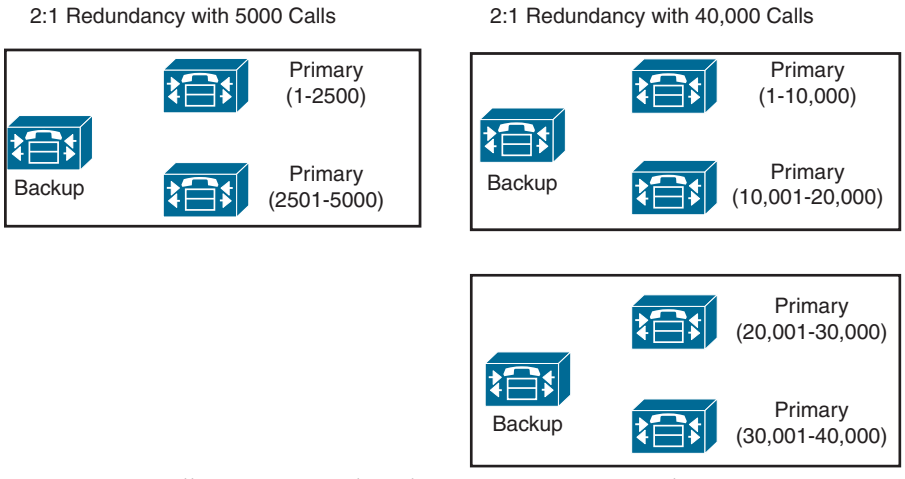

Figure 6-2 *Call Processing Subscriber Groups in a 2:1 Deployment*

Key Topic

With the 1:1 option, there is a single backup call processing subscriber for each primary call processing subscriber. This does require more server space and processing because more Cisco Unified Communications Manager deployments are needed. However, in the event any of the primary call processing subscribers crashes, the backup will immediately assume the role until such time the failed subscriber can be restored. This is a more robust solution that helps mitigate the prospect of downtime in your call center. In a 2:1 group, device registration and call processing services are available only on the primary subscribers unless a subscriber crashes; then the backup will kick in. However, in a 1:1 group, registration and call processing can be load-balanced between the primary and backup subscriber. Figure 6-3 illustrates how a 1:1 group of call processing subscribers can be used within the Cisco Unified Communications Manager dependent on the size of the deployment. Only two examples are provided, but many combinations exist based on the capacity of the cluster being deployed.

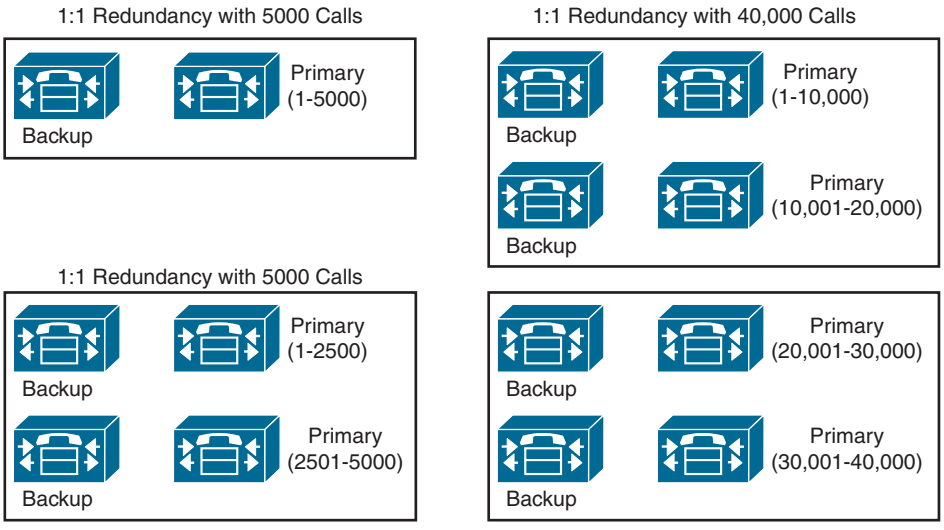

Figure 6-3 *Call Processing Subscriber Groups in a 1:1 Deployment*

When you are choosing the server(s) that will host the call agent VMs, it is best practice to choose a platform that supports dual power supplies. You should plug each power supply into different power sources so that in the event one of the power circuits fails, there is still constant power being supplied to the hosting server. Extra measures can be taken when combining dual power supplies with an UPS source. Should a power outage occur at the facility where the server is located, constant power will continue to be provided to the server, whereby phone services will also continue.

Several measures can be taken to provide high availability in the network connectivity. The speed and duplex used for network connectivity are essential to ensuring high availability. Many devices will be communicating with the call agent and will require a lot of bandwidth. Cisco recommends using a 1 Gbps or 10 Gbps throughput rate on the NIC the server is connected to. Voice and video communications should always use full duplex. If 1 Gbps or 10 Gbps throughput is used, full duplex is automatic. If a lower throughput is used, you should check the duplex configuration to ensure that it is set to full duplex, and not automatic or half duplex. Auto duplex on a Cisco switch will default to half duplex. Network redundancy can be achieved by using two Ethernet connections at the server. Each connection should be connected to a different switch so that in the event one of the switches fails, network connectivity will be maintained. This same redundancy can be implemented between switches within the network by physically distributing the network connections between different physical network switches within the same location. On the server, within the hypervisor there is a virtual switch with multiple uplinks. Therefore, a single virtual NIC defined in the call agent OVA settings is sufficient. In the VMware vSphere virtual switch, you can configure NIC teaming for the switch uplink.

Disaster Recovery

The Cisco Webex Global Site Backup architecture handles power outages, natural disaster outages, service capacity overload, network capacity overload, and other types of service interruptions. Global Site Backup supports both manual and automatic failover. The manual

failover mode is typically used during maintenance windows. The automatic failover mode is used in case of real-time failover due to a service interruption.

Global Site Backup is automatic and transparent to the end users, it is available for all users, and it imposes no limits on the number of users who can fail over. Global Site Backup consists of the following main components:

- **Global Site Service:** Is responsible for monitoring and switching traffic at the network level
- **Database Replication:** Ensures that the data transactions occurring on the primary site are transferred to the backup site
- **File Replication:** Ensures that any file changes are maintained in synchronization between the primary and the backup site

For disaster recovery, you can configure a cold-standby system in a second data center. If the primary system is configured for high availability, you can optionally choose to configure high availability for the disaster recovery system. Cisco Prime Collaboration Deployment does a direct migration, whereas previous migration methods involved more steps with a "server recovery" Disaster Recovery System relying on an initial upgrade followed by a restore from backup.

Dial Plan

The dial plan is one of the key elements of a Unified Communications and Collaboration system, and it is an integral part of all call processing agents. Generally, the dial plan is responsible for instructing the call processing agent on how to route calls. The dial plan performs many functions.

Endpoint addressing is one of the main functions of a dial plan. For destinations registered with the call processing agent, addresses are assigned to provide reachability. These internal destinations include all endpoints, such as IP phones, video endpoints, soft clients, and analog endpoints, as well as applications, such as voicemail systems, auto attendants, and conferencing systems. Path selection is another function of a dial plan. Depending on the calling device and the destination dialed, a path to the dialed destination is selected. If a secondary path is available, this path will also be considered if the primary path fails. Calling privileges is a third function of the dial plan. Different groups of devices can be assigned to different classes of service, by granting or denying access to certain destinations. For example, lobby phones might be allowed to reach only internal and local PSTN destinations, whereas executive phones could have unrestricted PSTN access. Dial plans can affect the manipulation of dialed destinations. On the path from the dialing device to the dialed destination, the dial plan can apply manipulations to the dialed destination. For example, users in the United States might dial 9011496901234 to reach a destination in the PSTN in Germany, while a user in France might be able to reach the same destination by dialing 000496901234. This dialed destination would need to be presented as 011496901234 to a PSTN trunk on a gateway in the U.S. and as 00496901234 to a PSTN trunk on a gateway in France. The dial plan can also affect calling numbers; for example, calls across the WAN may display a caller ID as 4111, but when the call is routed across the PSTN, it may appear as 3055554111. Presentation of information about identities involved in the call is also part of a dial plan. During session establishment and also while in the call, on both the calling and the called device,

information about the other device is displayed. Depending on call state and direction, this includes calling, diverting, alerting, and connected party information. The dial plan can define mappings that influence the format and content of information displayed.

Dial plan and number normalization considerations must be taken into account when deploying software-based endpoints. Jabber desktop clients typically use the directory for searching, resolving, and adding contacts. The number that is associated with those contacts must be in a form that the client can recognize, resolve, and dial.

Deployments may vary, depending on the configuration of the directory and Cisco Unified Communications Manager. In cases where the directory contains E.164 numbering, such as +18005551212, for business, mobile, and home telephone numbers, and Cisco Unified Communications Manager also contains an E.164 dial plan, the need for additional dial rules is minimized because every lookup, resolution, and dialed event results in an E.164-formatted dial string. If a Cisco Unified Communications Manager deployment has implemented a private dial plan, such as 5551212, then translation of the E.164 number to a private directory number needs to occur on Cisco Unified Communications Manager and possibly on the IOS gateways as well. Outbound calls can be translated by Cisco Unified Communications Manager translation patterns that allow the number being dialed, such as +18005551212, to be presented to the endpoint as the private number 5551212. Inbound calls can be translated by means of directory lookup rules. This allows an incoming number of 5551212 to be presented for reverse number lookup caller identification as 18005551212.

Private numbering plan deployments may arise, where the dial plan used for the company and the telephone number information stored in the LDAP directory may require the configuration of translation patterns and directory lookup rules in Cisco Unified Communications Manager to manage number format differences. Directory lookup rules define how to reformat the inbound call ID to be used as a directory lookup key. Translation patterns define how to transform a phone number retrieved from the LDAP directory for outbound dialing.

Cisco Unified Communications Manager uses translation patterns to manipulate both the calling and called numbers before a call is routed, and they are handled strictly by Cisco Unified Communications Manager. Application dialing rules can be used as an alternative to translation patterns to manipulate numbers that are dialed. Application dialing rules can automatically strip numbers from or add numbers to phone numbers that the user dials. Application dial rules are configured in Cisco Unified Communications Manager and are downloaded to the client from Cisco Unified Communications Manager. Translation patterns are the recommended method for manipulating dialed numbers.

Directory lookup rules transform caller identification numbers into numbers that can be looked up in the directory. A directory lookup rule specifies which numbers to transform based on the initial digits and the length of the number. Directory lookup rules are configured in Cisco Unified Communications Manager and are downloaded to the client from Cisco Unified Communications Manager. Before a call is placed through contact information, the client application removes everything from the phone number to be dialed, except for letters and digits. The application transforms the letters to digits and applies the dialing rules. The letter-to-digit mapping is locale-specific and corresponds to the letters found on a standard telephone keypad for that locale. Users cannot view or modify the client transformed numbers before the application places the call.

Security

Key Topic

Firewalls and ACLs are security capabilities that exist on the router to help secure your network by providing a first line of defense from attacks outside your network trying to access data inside. Unfortunately, that is not always enough to protect information inside the network from malicious attacks. If a user were to log in to his bank account across the public Internet, what is to stop a hacker from obtaining that user's login credentials and emptying the bank account? If that communication were sent over a nonsecure connection, the login information is in plain text. All the hacker would need is a packet sniffer to capture and view that information, and then would have access. To hide important information, the data needs to be encrypted. Think "Da Vinci Code" with text ciphers, only for a digital world. As long as your computer and your bank's server are the only two devices with the text ciphers, no other device will be able to read your information. Two security mechanisms can provide this level of encryption. Transport Layer Security (TLS) and its predecessor, Secure Sockets Layer (SSL), are cryptographic protocols that provide communications security over a computer network for TCP and UDP traffic. Although SSL is rarely used anymore, the TLS protocol aims primarily to provide privacy and data integrity between two communicating hosts or applications.

Client/server applications such as web browsers, email, and VoIP commonly use the TLS protocol to prevent eavesdropping and tampering of information. The easiest way to segregate the information is to use different port numbers for unencrypted traffic and encrypted traffic, such as port 80 for HTTP or port 443 for HTTPS. The connection is secure because symmetric cryptography is used to encrypt the transmitted data. The keys for this symmetric encryption are generated uniquely for each connection and are based on a shared secret negotiation at the start of the session. The server and client negotiate the details of which encryption algorithm and cryptographic keys to use before the first byte of data is transmitted. Identification is usually in the form of digital "certificates" that contain the server name, the trusted certificate authority (CA), and the server's public encryption key. The identity of the communicating parties can be authenticated using this public-key cryptography (asymmetric cryptography) to ensure only the intended recipient can decrypt the traffic. The negotiation of a shared secret is both secure and reliable against eavesdroppers and attacks, including man-in-the-middle attacks. The connection ensures integrity because each message transmitted includes a message integrity check using a message authentication code to prevent undetected loss or alteration of the data during transmission.

After the client and server have agreed to use TLS, they negotiate a stateful connection by using a handshake procedure. Figure 6-4 shows a general overview of how a TLS handshake takes place.

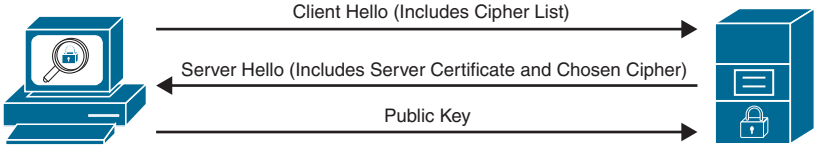

Figure 6-4 *TLS Handshake Overview*

The handshake begins when a client connects to a TLS-enabled server requesting a secure connection and presents a list of supported ciphers and hash functions. From this list, the server picks a cipher and hash function that it also supports and informs the client of the decision. The server then identifies itself with its digital certificate, which can contain the server name, the trusted certificate authority, and the server's public encryption key. The client then

validates the certificate before proceeding. Public-key encryption is used to share the pre-master secret via the use of RSA or Diffie-Hellman key exchange. This process generates a random and unique session key for encryption and decryption that has the additional property of forward secrecy, which protects past sessions against future compromises of secret keys or passwords.

Remember that the server is validated because the client initiates the secure connection. The client side confirms that the server is who it claims to be and whether it can be trusted with the use of certificates. Figure 6-5 illustrates the elements contained within a certificate that can be used to verify the certificate holder is authentic.

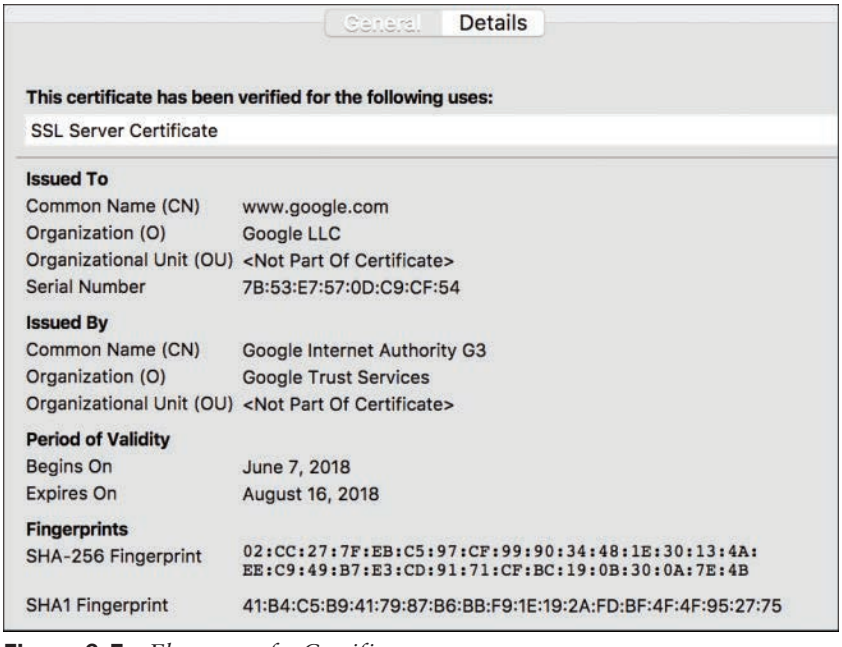

Figure 6-5 *Elements of a Certificate*

Key Topic

The client receives the digital certificate from the server side of the TLS negotiation, but the identity must be verified before proceeding. As seen in Figure 6-5, when Google's server sends its certificate, it contains the name of the certificate holder. This name is checked against the Common Name (CN) or the Subject Alternative Name (SAN), which is www.google.com in this instance. Also, it contains additional information like a serial number, expiration dates or Period of Validity, revocation status (not applicable in this figure), a copy of the certificate holder's public key (SHA-256 Fingerprint used for encrypting messages and digital signatures), and the digital signature of the certificate-issuing authority (SHA1 Fingerprint). If you trust this certificate authority, you can verify (using the CA's public key) that it really did sign the server's certificate. To sign a certificate yourself, you need the private key, which is known only to the CA of your choice. This way, an attacker cannot falsely sign a certificate and claim to be Google.com. When the certificate has been modified, the signature will be incorrect, and the client will reject it.

Although this form of TLS encryption is very secure, you can still take additional measures to ensure an even higher level of security. This is known as Mutual TLS, which is

synonymous with TLS Verify. In Mutual TLS authentication, both parties authenticate each other through verifying the provided digital certificate so that both parties are assured of the others' identity. Mutual TLS is similar to the normal process of the client handling the verification of the server's certification but includes the additional step of the client providing a certificate to the server for verification. This process allows the server side to authenticate the client, allowing both parties to trust each other. Figure 6-6 illustrates how a Mutual TLS negotiation would take place.

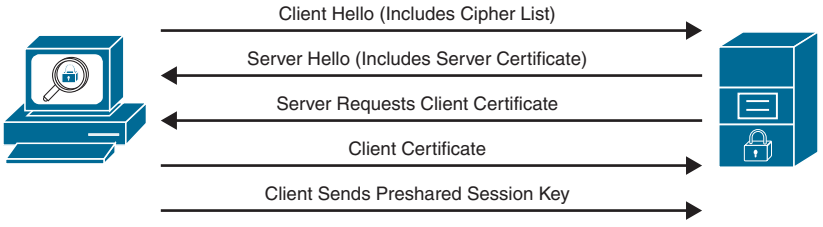

Figure 6-6 *Mutual TLS Negotiation*

Server-to-server connections rely on Mutual TLS for mutual authentication. In the Cisco Collaboration infrastructure, some examples would be a secure connection between endpoints and the Cisco Unified Communications Manager, referred to as TLS Verify, Cisco Unified Communications Manager intercluster trunks to other clusters, and even Cisco Unified Communications Manager SIP trunks to a Cisco Expressway or a Video Communication Server (VCS).

QoS

Key Topic

QoS is a marking system for network traffic that allows packets to be prioritized during high congestion times, so that drop-sensitive packets can be sent first and drop-insensitive packets are sent last. For example, an email is sent using TCP, which will resend the packets in the event they are not received at the destination. Voice and video packets are sent over UDP and will not be resent if they are dropped, which could cause media issues at the receiving end of the call. Therefore, voice and video traffic should be provided with a higher priority than email traffic. When it comes to QoS, it is best practice to mark packets as close to the source as possible. Most devices, such as computers and servers, cannot mark their own packets and should not be trusted even if they can. Cisco phones, however, can mark their own packets and can be trusted with the QoS markings they provide. Therefore, QoS trust boundaries should be set up so that the switch will trust the QoS markings that phones place on their own packets. Layer 2 QoS uses a mechanism called class of service (CoS), which operates on the 802.1q VLAN. Unlike Layer 3 QoS mechanisms, CoS does not ensure network performance or guarantee priority in packets being delivered. Therefore, after packets are marked with CoS, they will need to be converted to DSCP using the cos-to-dscp map, which is built into all Cisco switches. By default, QoS on a Cisco access switch is disabled. Once QoS is enabled, the switch does not trust QoS settings from a phone. Two simple commands can be entered under the global menu on a switch to enable QoS and change the trust boundary. Once QoS is enabled, you can use a **show** command to verify these settings. Example 6-1 illustrates the QoS Enable and Trust Boundary Commands and the **show** verification command.

Example 6-1 *QoS Enable and Trust Boundary Commands*

```
Switch(config)# mls qos
Switch(config)# interface fastethernet 0/1
Switch(config-if)# mls qos trust cos
Switch(config-if)# end
Switch# show mls qos interface fastethernet 0/1
FastEthernet0/1
trust state: trust cos
trust mode: trust cos
cos override: dis
default COS: 0
DSCP Mutation Map: Default DSCP Mutation Map
Trust device: none
```

Obviously, this is the simplest design, and there are many other concerns to consider, along with many other settings that can be configured. This example is intended to provide a basic understanding of QoS at the Layer 2 level. For more information on QoS, refer to the *Enterprise QoS Solution Reference Network Design Guide*.

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 32, "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 6-5 lists a reference of these key topics and the page numbers on which each is found.

Key Topic

Table 6-5 Key Topics for Chapter 6

Key Topic Element	Description	Page Number
Paragraph	Framework for Cisco Jabber	117
Paragraph	Deskphone Mode and Softphone Mode for Jabber	118
Paragraph	Webex Teams	118
Table 6-2	Cisco Telepresence Endpoint Product Portfolio	119
List	Databases Supported for Directory Synchronization	120
Paragraph	Signaling Protocols Supported Through the CUCM	120
Paragraph	NTP Used by CUCM	121
Paragraph	DHCP from CUCM	121

Key Topic Element	Description	Page Number
Paragraph	Licensing Differences Between the VCS and Expressway Products	123
Table 6-3	Comparison of the Cisco Expressway and the Cisco VCS	123
Paragraph	CUC	125
Paragraph	CUE	125
Paragraph	IM and Presence service	126
Paragraph	CMS	126
Paragraph	Additional Features Supported on CMS	127
Paragraph	TMS Features	127
List	Three Models of Prime Collaboration	128
Paragraph	Prime Collaboration Provisioning	128
Paragraph	Prime Collaboration Assurance	128
List	Prime Collaboration Analytics	129
Table 6-4	CUWL and CUCL Licensing Model	130
Paragraph	PMP and SMP Licenses	131
List	Purchasing Models for Flex Licensing	132
List	Benefits of Smart Accounts	133
Paragraph	Business Edition Series UCS Servers	134
List	Regions and Locations	135
Paragraph	Expressway Cluster Requirements	136
Paragraph	CUCM Cluster Behavior	137
Paragraph	2:1 Redundancy Group in CUCM	137
Paragraph	1:1 Redundancy Group in CUCM	138
Paragraph	Functions of a Dial Plan	140
Paragraph	TLS and SSL Comparison	142
Paragraph	Certificate Checking Process	143
Paragraph	QoS Best Practice for L2 Marking	144

Define Key Terms

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

CAST, CE, CMA, CME, CMS, CTI, CUBE, CUC, CUCL, CUCM, CUCSF, CUE, CUWL, DNS, DX, Flex, FXO, FXS, HCS, IM, IMP, IX, Locations, MRA, MTLS, MX, NTP, PMP, PoE, Regions, RMS, SMP, SSL, SX, TC, TIP, TLS, UC, URI, URL, VCS, VoIP, VPN, Webex Endpoints, WebRTC, XMPP

Command Reference to Check Your Memory

This section includes the most important configuration and EXEC commands covered in this chapter. It might not be necessary to memorize the complete syntax of every command, but you should be able to remember the basic keywords that are needed.

To test your memory of the commands, cover the right side of Tables 6-6 with a piece of paper, read the description on the left side, and then see how much of the command you can remember.

The CLCOR (350-801) exam focuses on practical, hands-on skills that are used by a networking professional. Therefore, you should be able to identify the commands needed to configure and test QoS settings on a switch.

Table 6-6 Cisco Meeting Server MMP Commands

Task	Command Syntax
Enables the multilayer switching quality of service	Switch(config)# **mls qos**
Enters the configuration field if fast Ethernet switch port 1	Switch(config)# **interface fastethernet 0/1**
Configures the switch to trust all ingress traffic	Switch(config-if)# **mls qos trust cos**
Takes the admin out of global configuration mode in the switch	Switch(config-if)# **end**
Displays the QoS settings configured on the switch from above	Switch# **show mls qos interface fastethernet 0/1**
Displays output from the previous **show** command	FastEthernet0/1 Trust state: **trust cos** Trust mode: **trust cos** CoS override: **dis** Default COS: **0** DSCP Mutation Map: Default DSCP Mutation Map Trust device: **none**

Q&A

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

1. List the four main categories of Webex endpoints in the Telepresence product portfolio.
2. List the licensing differences between an Expressway and a VCS.
3. List the three models of Prime Collaboration.
4. List the switch commands to enable QoS at Layer 2.