Official Cert Guide

Advance your IT career with hands-on learning

Study Planner

CCNP Enterprise Wireless Design and Implementation

ENWLSD 300-425 and ENWLSI 300-430

Jerome Henry, CCIE® No. 24750
Robert Barton, CCIE® No. 6660
David Hucaby, CCIE® No. 4594

ciscopress.com

FREE SAMPLE CHAPTER

SHARE WITH OTHERS

CCNP Enterprise Wireless Design

ENWLSD 300-425

and **Implementation**

ENWLSI 300-430

Official Cert Guide: Designing & Implementing Cisco Enterprise Wireless Networks

JEROME HENRY, CCIE No. 24750

ROBERT BARTON, CCIE No. 6660

DAVID HUCABY, CCIE No. 4594

Cisco Press

CCNP Enterprise Wireless Design ENWLSD 300-425 and Implementation ENWLSI 300-430 Official Cert Guide: Designing & Implementing Cisco Enterprise Wireless Networks

Jerome Henry
Robert Barton
David Hucaby

Copyright© 2021 Cisco Systems, Inc.

Published by:
Cisco Press
Hoboken, New Jersey

All rights reserved. This publication is protected by copyright, and permission must be obtained from the publisher prior to any prohibited reproduction, storage in a retrieval system, or transmission in any form or by any means, electronic, mechanical, photocopying, recording, or likewise. For information regarding permissions, request forms, and the appropriate contacts within the Pearson Education Global Rights & Permissions Department, please visit www.pearson.com/permissions.

No patent liability is assumed with respect to the use of the information contained herein. Although every precaution has been taken in the preparation of this book, the publisher and author assume no responsibility for errors or omissions. Nor is any liability assumed for damages resulting from the use of the information contained herein.

ScoutAutomatedPrintCode

Library of Congress Control Number: 2020909660

ISBN-13: 978-0-13-660095-4

ISBN-10: 0-13-660095-6

Warning and Disclaimer

This book is designed to provide information about the CCNP Enterprise Wireless Design ENWLSD 300-425 and Enterprise Wireless Implementation ENWLSI 300-430 exams. Every effort has been made to make this book as complete and as accurate as possible, but no warranty or fitness is implied.

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

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

Trademark Acknowledgments

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

Special Sales

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

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

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

Feedback Information

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

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

We greatly appreciate your assistance.

Editor-in-Chief: Mark Taub

Alliances Manager, Cisco Press: Arezou Gol

Director, ITP Product Management: Brett Bartow

Executive Editor: Nancy Davis

Managing Editor: Sandra Schroeder

Development Editor: Ellie Bru

Project Editor: Mandie Frank

Copy Editor: Bart Reed

Technical Editor: Samuel Clements

Editorial Assistant: Cindy Teeters

Designer: Chuti Prasertsith

Composition: codeMantra

Indexer: Timothy Wright

Proofreader: Donna Mulder

Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

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

Europe Headquarters
Cisco Systems International BV Amsterdam,
The Netherlands

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

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: www.cisco.com/go/trademarks. Third party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R)

Credits

Figure 3-1	Screenshot of a view of a wireless (non-802.11) camera in Metageek Chanalyzer © MetaGeek, LLC
Figure 3-2	Screenshot of well-known signal types in Metageek Chanalyzer © MetaGeek, LLC
Figure 3-5	Screenshot of Ekahau Site Survey Pro © 2020 Ekahau
Figure 7-1	Tatiana Grozetskaya/123RF

About the Authors

Jerome Henry, CCIE No. 24750, is a Principal Engineer in the Office of the Wireless CTO at Cisco Systems. Jerome has more than 15 years' experience teaching technical Cisco courses, in more than 15 countries and four languages, to audiences ranging from bachelor's degree students to networking professionals and Cisco internal system engineers. Focusing on his wireless and networking experience, Jerome joined Cisco in 2012. Before that time, he was consulting and teaching about heterogeneous networks and wireless integration with the European Airespace team, which was later acquired by Cisco to become its main wireless solution. He then spent several years with a Cisco Learning Partner, developing networking courses and working on training materials for emerging technologies.

Jerome is a certified wireless networking expert (CWNE No. 45), has developed multiple Cisco courses, and authored several wireless books and video courses. Jerome holds more than 150 patents, is a member of the IEEE, where he was elevated to Senior Member in 2013, and also represents Cisco in multiple Wi-Fi Alliance working groups. With more than 10,000 hours in the classroom, Jerome was awarded the IT Training Award Best Instructor silver medal. He is based in Research Triangle Park, North Carolina.

Robert Barton, CCIE No. 6660, is a Distinguished Architect with Cisco and has worked in the wireless field for over 20 years, assisting with some of the largest Wi-Fi deployments globally. He graduated from the University of British Columbia with a degree in engineering physics and is a registered professional engineer. Rob holds dual CCIEs, in Routing and Switching and Security, and is a CCDE. Rob also holds patents in the areas of wireless communications, IoT, segment routing, and AI/machine learning. Rob is also a regular presenter at Cisco Live and has been inducted into Cisco's Distinguished Speaker Hall of Fame. Rob is located in Vancouver, Canada, where he lives with his wife and two teenage children.

David Hucaby, CCIE No. 4594, CWNE No. 292, is a lead network engineer for University of Kentucky HealthCare, where he focuses on wireless networks in a large medical environment. David holds bachelor's and master's degrees in electrical engineering. He has been authoring Cisco Press titles for 20 years. David lives in Kentucky with his wife, Marci, and two daughters.

About the Technical Reviewers

Samuel Clements is a Mobility Practice Manager for Presidio (www.presidio.com), a VAR in the United States. He is CCIE #40629 (Wireless) and CWNE #101 and is active in all things Wi-Fi. You can find him blogging at www.sc-wifi.com or on Twitter at @samuel_clements. When he's not doing Wi-Fi things, he's spending time in Tennessee with his wife, Sara, and his two children, Tristan and Ginny.

Dedications

Jerome Henry:

In many ways, this century (and probably the previous ones) resembles Wi-Fi. Every few years, new developments fundamentally change the way we work and communicate. Each time we look back a few years, we realize that today we have more information to absorb and more new technologies to understand. What was concluded as impossible is now experimented with or achieved sooner and faster than we thought. As you open this book, dear reader, to prepare for the CCNP exam, you know that this step may look steep today, but it will soon be just a memory of a time you knew less and could do less. Your will to excel and deepen your knowledge is what you, dear reader, give to us, the authors, as a reason to continue sharpening our expertise and share what we have learned on the way. So this book is for you, dear reader, and your aspiration to excellence. As my family blazon says, "sic itur ad astro"—this is how you reach for the stars!

Robert Barton:

When you come to the end of a long book project, it's an interesting experience to step back and reflect on your memories of the many hours spent over weekends, evenings, and holidays to accomplish a work such as this. For me, my enduring memory will be a connection to the early days of the coronavirus stay-at-home period, trying to balance all the unexpected new demands of life with finishing a book. During this time of change we found ways to support each other—physically, emotionally, and spiritually. For this, I dedicate our book to the three most important people in my life—my beautiful wife, Loretta, and my two boys, Adrian and Matthew.

David Hucaby:

As always, my work is dedicated to my wife and my daughters, for their love and support, and to God, who has blessed me with opportunities to learn, write, and work with so many friends—abundant life indeed!

Acknowledgments

My dear wife, Corinne, often says that she knows "that look," she knows "that pace," when I walk back and forth in the corridor of our home leading to my office. She knows when I am not satisfied with a sentence, critical of an explanation that I do not find clear enough, or unhappy with an example or an analogy that does not quite work like it should. Each time, she patiently throws me a question to help me verbalize the problem and, in the end, puts her finger on what was missing. This book would not have been possible without her patience. "Patience made human" is also how I see Brett Bartow, who helped us navigate the complexity of changing exam scopes, and Ellie Bru, who week after week herded us, her authors, corrected our mistakes, and patted our backs to help us stay at the level of quality she expected. If this book is not a collection of disorganized notes on pieces of napkins, it is thanks to them. And, of course, flying with three pilots only works if each of them mixes excellence in their domain, acceptance that another one may be covering the left or the right field, and a permanent re-assessment of who is where, who has covered what, and who has left what gap or ground to complete. I could not dream of better co-pilots than Rob and Dave—two top guns who were kind enough to accept me and enjoy this flight together.

—Jerome Henry

Writing a book can be a monumental undertaking. As we started writing this book in mid-2019, we set out with a firm plan that went through more changes than any of us ever expected. However, for every challenge and curve ball we encountered, we adapted, came together as a team, and rose to the challenge. I am forever grateful to have worked with such incredible co-authors like Jerome and David. Together, we elevated our game and brought out the best in each other. I am truly appreciative to have worked with you both—like Proverbs says, "There is accomplishment through many advisers." You set the bar higher than I could have imagined, and in the end, we crafted an exceptional piece of work together. Thank you, guys!! I would also like to express my deep appreciation to Ellie Bru for her enduring patience, especially for keeping us focused during the hardest days of the coronavirus stay-at-home period—when work got crazy and our chapter deadlines seemed to loom every day. The sloth emojis and memes really helped illuminate a bright spot of humor during those toughest days.

—Robert Barton

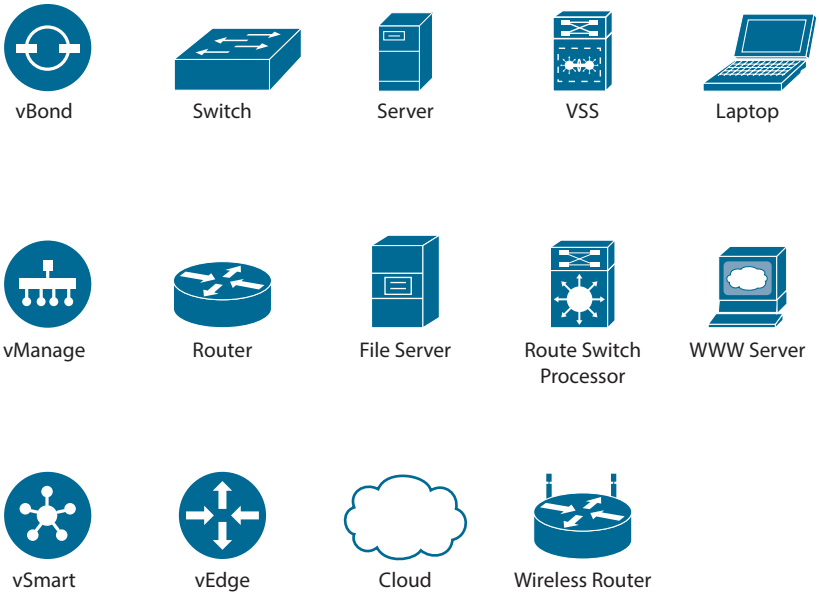
I am very grateful to Brett Bartow for giving me the opportunity to work on this project. An unexpected blessing was for two wireless projects to merge into one, allowing me to write alongside Jerome Henry and Rob Barton—two legends and now two friends! They have been great to work with, patient to help me when I needed it, and gracious to make me feel welcome on the team. Ellie Bru has been an awesome development editor and has kept us motivated all along the way with encouragement and funny GIFs. Nancy Davis joined us late in the game and has been a welcome addition to the editorial staff. Many thanks to Samuel Clements for his fine technical editing and review. I have graduated from reading his blog to reading his comments and suggestions. Finally, I would like to thank Eldad Perahia for graciously explaining some complex concepts when I was stuck.

—David Hucaby

Contents at a Glance

Contents

Icons Used in This Book



Command Syntax Conventions

The conventions used to present command syntax in this book are the same conventions used in the IOS Command Reference. The Command Reference describes these conventions as follows:

- **Boldface** indicates commands and keywords that are entered literally as shown. In actual configuration examples and output (not general command syntax), boldface indicates commands that are manually input by the user (such as a **show** command).
- *Italic* indicates arguments for which you supply actual values.
- Vertical bars (|) separate alternative, mutually exclusive elements.
- Square brackets ([ ]) indicate an optional element.
- Braces ({ }) indicate a required choice.
- Braces within brackets ([{ }]) indicate a required choice within an optional element.

Introduction

Congratulations! If you are reading this Introduction, then you have probably decided to obtain a Cisco certification. Obtaining a Cisco certification will ensure that you have a solid understanding of common industry protocols along with Cisco's device architecture and configuration. Cisco has a high market share of network infrastructure of routers, switches, and firewalls, with a global footprint.

Professional certifications have been an important part of the computing industry for many years and will continue to become more important. Many reasons exist for these certifications, but the most popularly cited reason is credibility. All other factors being equal, a certified employee/consultant/job candidate is considered more valuable than one who is not certified.

Cisco provides three levels of certifications: Cisco Certified Network Associate (CCNA), Cisco Certified Network Professional (CCNP), and Cisco Certified Internetwork Expert (CCIE). Cisco made changes to all three certifications, effective February 2020. The following are the most notable of the many changes:

- The exams will include additional topics, such as programming.
- The CCNA certification is not a prerequisite for obtaining the CCNP certification.
- CCNA specializations will not be offered anymore.
- The exams will test a candidate's ability to configure and troubleshoot network devices in addition to answering multiple-choice questions.
- The CCNP is obtained by taking and passing a Core exam and a Concentration exam.
- The CCIE certification requires candidates to pass the Core written exam before the CCIE lab can be scheduled.

CCNP Enterprise candidates need to take and pass the Implementing and Operating Cisco Enterprise Network Core Technologies ENCOR 350-401 examination. Then they need to take and pass one of the following Concentration exams to obtain their CCNP Enterprise:

- 300-410 ENARSI: Implementing Cisco Enterprise Advanced Routing and Services (ENARSI)
- 300-415 ENSDWI: Implementing Cisco SD-WAN Solutions (ENSDWI)
- 300-420 ENSLD: Designing Cisco Enterprise Networks (ENSLD)
- 300-425 ENWLSD: Designing Cisco Enterprise Wireless Networks (ENWLSD)
- 300-430 ENWLSI: Implementing Cisco Enterprise Wireless Networks (ENWLSI)
- 300-435 ENAUTO: Automating and Programming Cisco Enterprise Solutions (ENAUTO)

This book helps you study for the CCNP ENWLSD 300-425 and ENWLSI 300-430 exams. The time allowed to take each test is 90 minutes to complete about 60 questions. Testing is done at Pearson VUE testing centers.

Be sure to visit www.cisco.com to find the latest information on CCNP Concentration requirements and to keep up to date on any new Concentration exams that are announced.

Goals and Methods

The most important and somewhat obvious goal of this book is to help you pass the Designing Cisco Enterprise Wireless Networks ENWLSD 300-425 and Implementing Cisco Enterprise Wireless Networks ENWLSI 300-430 exams. In fact, if the primary objective of this book was different, then the book's title would be misleading; however, the methods used in this book to help you pass the ENWLSD 300-425 and ENWLSI 300-430 exams are designed to also make you much more knowledgeable about how to do your job. While this book and the companion website together have more than enough questions to help you prepare for the actual exam, the method in which they are used is not to simply make you memorize as many questions and answers as you possibly can.

One key methodology used in this book is to help you discover the exam topics you need to review in more depth, to help you fully understand and remember those details, and to help you prove to yourself that you have retained your knowledge of those topics. So, this book does not try to help you pass by memorization, but helps you truly learn and understand the topics. Designing and implementing enterprise wireless networks are two of the concentration areas you can focus on to obtain the CCNP certification, and the knowledge contained within is vitally important to consider yourself a truly skilled Enterprise Wireless Networks engineer. This book will help you pass the ENWLSD 300-425 and ENWLSI 300-430 exams by using the following methods:

- Helping you discover which test topics you have not mastered
- Providing explanations and information to fill in your knowledge gaps
- Supplying exercises and scenarios that enhance your ability to recall and deduce the answers to test questions

Who Should Read This Book?

This book is not designed to be a general wireless networking topics book, although it can be used for that purpose. This book is intended to tremendously increase your chances of passing the Designing Cisco Enterprise Wireless Networks ENWLSD 300-425 and Implementing Cisco Enterprise Wireless Networks ENWLSI 300-430 CCNP specialization exams. Although other objectives can be achieved from using this book, the book is written with one goal in mind: to help you pass the exams.

Strategies for Exam Preparation

The strategy you use to study for the ENWLSD or ENWLSI exam might be slightly different than strategies used by other readers, mainly based on the skills, knowledge, and experience you already have obtained. For instance, if you have attended the ENWLSD or ENWLSI course, then you might take a different approach than someone who learned based on job experience alone.

Regardless of the strategy you use or the background you have, the book is designed to help you get to the point where you can pass the exam with the least amount of time required. For instance, there is no need for you to practice or read about IP addressing and subnetting if you fully understand it already. However, many people like to make sure they truly know a topic and thus read over material they already know. Several book features will help you gain the confidence you need to be convinced that you know some material already and to also help you know what topics you need to study more.

The Companion Website for Online Content Review

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

How to Access the Companion Website

To access the companion website, which gives you access to the electronic content with this book, start by establishing a login at www.ciscopress.com and registering your book. To do so, simply go to www.ciscopress.com/register and enter the ISBN of the print book: 9780136600954. After you have registered your book, go to your account page and click the Registered Products tab. From there, click the Access Bonus Content link to get access to the book's companion website.

Note that if you buy the Premium Edition eBook and Practice Test version of this book from Cisco Press, your book will automatically be registered on your account page.

Simply go to your account page, click the Registered Products tab, and select Access Bonus Content to access the book's companion website.

How to Access the Pearson Test Prep (PTP) App

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

- **Print book**: Look in the cardboard sleeve in the back of the book for a piece of paper with your book's unique PTP code.
- **Premium Edition**: If you purchase the Premium Edition eBook and Practice Test directly from the Cisco Press website, the code will be populated on your account page after purchase. Just log in at www.ciscopress.com, click Account to see details of your account, and click the digital purchases tab.

- **Amazon Kindle:** For those who purchase a Kindle edition from Amazon, the access code will be supplied directly from Amazon.
- **Other Bookseller eBooks:** Note that if you purchase an eBook version from any other source, the practice test is not included because other vendors to date have not chosen to vend the required unique access code.

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

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

Step 1. Open this book's companion website, as shown earlier in this Introduction under the heading "How to Access the Companion Website."

Step 2. Click the Practice Exams button.

Step 3. Follow the instructions listed there both for installing the desktop app and for using the web app.

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

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

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

How This Book Is Organized

Although this book could be read cover to cover, it is designed to be flexible and allow you to easily move between chapters and sections of chapters to cover just the material you need more work with. Chapters 1 through 9 cover wireless design topics that are relevant for the ENWLSD 300-425 exam, while Chapters 10 through 17 cover topics related to implementing wireless networks for the ENWLSI 300-430 exam.

The core chapters, Chapters 1 through 17, cover the following topics:

- **Chapter 1, "Wireless Design Requirements"** This chapter covers important wireless aspects of customer networks, access points, and client devices that can drive an effective network design.
- **Chapter 2, "Conducting an Offsite Site Survey"** This chapter describes how to prepare for an offsite site survey, by looking at common verticals requirements, determining obstacles' signal absorption, and conducting a predictive site survey.
- **Chapter 3, "Conducting an Onsite Site Survey"** This chapter discusses the onsite survey process, including the survey tools and the survey methodology. This chapter also provides recommendations on survey settings for data, voice, and location services.
- **Chapter 4, "Physical and Logical Infrastructure Requirements"** This chapter discusses the physical infrastructure, such as power and cabling, mounting, and grounding. The chapter also discusses the logical infrastructure components that support wireless services.
- **Chapter 5, "Applying Wireless Design Requirements"** This chapter discusses the behavior of specific applications and traffic types being carried over a wireless network, along with the network design guidelines and best practices for each.
- **Chapter 6, "Designing Radio Management"** This chapter explains Radio Resource Management (RRM) and how you can leverage it to automatically manage AP transmit power levels and channel assignments, along with adjustments for changing RF conditions.
- **Chapter 7, "Designing Wireless Mesh Networks"** This chapter introduces wireless mesh technology and details how mesh networks are designed. The chapter reviews mesh components and architecture and key design recommendations for outdoor mesh environments.
- **Chapter 8, "Designing for Client Mobility"** This chapter covers wireless client mobility, or the roaming process, along with ways to make it more efficient and seamless.
- **Chapter 9, "Designing High Availability"** This chapter introduces the features and strategies you can leverage to improve wireless LAN controller availability in case of equipment or link failure.
- **Chapter 10, "Implementing FlexConnect"** This chapter looks at branch office wireless deployments with a focus on FlexConnect. The chapter discusses how FlexConnect groups can be implemented as well as key features of FlexConnect. This chapter also discusses Office Extend APs (OEAP).
- **Chapter 11, "Implementing Quality of Service on a Wireless Network"** This chapter begins with a review of wireless QoS standards and how these are implemented in Cisco wireless controllers. The chapter also looks at key QoS capabilities such as Application Visibility and Control (AVC).

- **Chapter 12, "Implementing Multicast"** This chapter explains multicast traffic delivery in a wireless network, along with the features that can make it more efficient. Also covered are methods to handle multicast DNS as well as video stream delivery.
- **Chapter 13, "Location Services Deployment"** This chapter discusses how location is achieved using Wi-Fi technologies. This chapter also explains how to deploy location engines, such as CMX/MSE and DNA Spaces, and how to use them to track clients, interferers, and rogues.
- **Chapter 14, "Advanced Location Services Implementation"** This chapter explains how to make the most of your location engine, by implementing advanced features such as location-aware guest services and wireless intrusion protection systems (WIPSs). This chapter also discusses the implementation of Analytics and Presence services.
- **Chapter 15, "Security for Wireless Client Connectivity"** This chapter discusses wireless client authentication methods, such as Extensible Authentication Protocol (EAP). The chapter also discusses guest wireless access and how bring your own devices (BYODs) can be securely onboarded to a network.
- **Chapter 16, "Monitoring and Troubleshooting WLAN Components"** This chapter covers report and alarm management on Cisco Prime Infrastructure and DNA Center (DNAC). This chapter also discusses how to troubleshoot client connectivity and performance on the wireless LAN controller (WLC), Prime Infrastructure, and DNAC.
- **Chapter 17, "Device Hardening"** This chapter looks at how the security of wireless devices can be improved by controlling access to the wireless infrastructure and how APs can authenticate to a network.

Certification Exam Topics and This Book

The questions for each certification exam are a closely guarded secret. However, Cisco has published exam blueprints that list which topics you must know to *successfully* complete the exam. Table I-1 lists each exam topic listed in the blueprint along with a reference to the book chapter that covers the topic. These are the same topics you should be proficient in when designing and implementing Cisco Enterprise wireless networks in the real world.

Table I-1 ENWLSD 300-425 and ENWLSI 300-430 Exam Topics and Chapter References

Exam	Exam Topic	Chapter(s) in Which Topic Is Covered
ENWLSD 300-425	1.1 Collect design requirements and evaluate constraints	1
ENWLSD 300-425	1.2 Describe material attenuation and its effect on wireless design	2

Exam	Exam Topic	Chapter(s) in Which Topic Is Covered
ENWLSD 300-425	1.3 Perform and analyze a Layer 1 site survey	3
ENWLSD 300-425	1.4 Perform a pre-deployment site survey	3
ENWLSD 300-425	1.5 Perform a post-deployment site survey	3
ENWLSD 300-425	1.6 Perform a predictive site survey	2
ENWLSD 300-425	1.7 Utilize planning tools and evaluate key network metrics (Ekahau, AirMagnet, PI, Chanalyzer, Spectrum Analyzer)	2
ENWLSD 300-425	2.1 Determine physical infrastructure requirements such as AP power, cabling, switch port capacity, mounting, and grounding	4
ENWLSD 300-425	2.2 Determine logical infrastructure requirements such as WLC/AP licensing requirements based on the type of wireless architecture	4
ENWLSD 300-425	2.3 Design radio management	6
ENWLSD 300-425	2.4 Apply design requirements for these types of wireless networks	5
ENWLSD 300-425	2.5 Design high-density wireless networks and their associated components (campus, lecture halls, conference rooms)	5
ENWLSD 300-425	2.6 Design wireless bridging (mesh)	7
ENWLSD 300-425	3.1 Design mobility groups based on mobility roles	8
ENWLSD 300-425	3.2 Optimize client roaming	8
ENWLSD 300-425	3.3 Validate mobility tunneling for data and control path	8
ENWLSD 300-425	4.1 Design high availability for controllers	9
ENWLSD 300-425	4.2 Design high availability for APs	9
ENWLSI 300-430	1.1 Deploy FlexConnect components such as switching and operating modes	10
ENWLSI 300-430	1.2 Deploy FlexConnect capabilities	10
ENWLSI 300-430	1.3 Implement Office Extend	10
ENWLSI 300-430	2.1 Implement QoS schemes based on requirements including wired-to-wireless mapping	11
ENWLSI 300-430	2.2 Implement QoS for wireless clients	11
ENWLSI 300-430	2.3 Implement AVC including Fastlane (only on WLC)	11
ENWLSI 300-430	3.1 Implement multicast components	12
ENWLSI 300-430	3.2 Describe how multicast can affect wireless networks	12

Exam	Exam Topic	Chapter(s) in Which Topic Is Covered
ENWLSI 300-430	3.3 Implement multicast on a WLAN	12
ENWLSI 300-430	3.4 Implement mDNS	12
ENWLSI 300-430	3.5 Implement Multicast Direct	12
ENWLSI 300-430	4.1 Deploy MSE and CMX on a wireless network	13
ENWLSI 300-430	4.2 Implement location services	13
ENWLSI 300-430	5.1 Implement CMX components	14
ENWLSI 300-430	5.2 Implement location-aware guest services using custom portal and Facebook Wi-Fi	14
ENWLSI 300-430	5.3 Troubleshoot location accuracy using Cisco Hyperlocation	14
ENWLSI 300-430	5.4 Troubleshoot CMX high availability	14
ENWLSI 300-430	5.5 Implement WIPS using MSE	14
ENWLSI 300-430	6.1 Configure client profiling on WLC and ISE	15
ENWLSI 300-430	6.2 Implement BYOD and guest	15
ENWLSI 300-430	6.3 Implement 802.1X and AAA on different wireless architectures and ISE	15
ENWLSI 300-430	6.4 Implement Identity-Based Networking on different wireless architectures (VLANs, QoS, ACLs)	15
ENWLSI 300-430	7.1 Utilize reports on PI and Cisco DNA-C	16
ENWLSI 300-430	7.2 Manage alarms and rogues (APs and clients)	16
ENWLSI 300-430	7.3 Manage RF Interferers	16
ENWLSI 300-430	7.4 Troubleshoot client connectivity	16
ENWLSI 300-430	8.1 Implement device access controls (including RADIUS and TACACS+)	17
ENWLSI 300-430	8.2 Implement access point authentication (including 802.1X)	17
ENWLSI 300-430	8.3 Implement CPU ACLs on the controller	17

Each version of the exam can have topics that emphasize different functions or features, and some topics can be rather broad and generalized. The goal of this book is to provide the most comprehensive coverage to ensure that you are well prepared for the exam. Although some chapters might not address specific exam topics, they provide a foundation that is necessary for a clear understanding of important topics. Your short-term goal might be to pass this exam, but your long-term goal should be to become a qualified CCNP Enterprise wireless engineer.

It is also important to understand that this book is a "static" reference, whereas the exam topics are dynamic. Cisco can and does change the topics covered on certification exams often.

This exam guide should not be your only reference when preparing for the certification exam. You can find a wealth of information available at Cisco.com that covers each topic in great detail. If you think you need more detailed information on a specific topic, read the Cisco documentation that focuses on that topic.

Note that as CCNP Enterprise wireless network technologies continue to evolve, Cisco reserves the right to change the exam topics without notice. Although you can refer to the list of exam topics in Table I-1, always check Cisco.com to verify the actual list of topics to ensure you are prepared before taking the exam. You can view the current exam topics on any current Cisco certification exam by visiting the Cisco.com website, choosing Menu, clicking Training & Events, and then selecting from the Certifications list. Note also that, if needed, Cisco Press might post additional preparatory content on the web page associated with this book at www.ciscopress.com/title/9780136600954. It's a good idea to check the website a couple of weeks before taking your exam to be sure that you have up-to-date content.

This page intentionally left blank

CHAPTER 4

Physical and Logical Infrastructure Requirements

This chapter discusses the following topics:

Physical Infrastructure Requirements: Powering an access point with Power over Ethernet (PoE) has several variants, including delivering power directly from a switch or through a power injector. However, PoE itself comes in several flavors that have cabling infrastructure dependencies. This section discusses the main types of PoE, including PoE, PoE+, UPoE, and UPoE+, and the types of cables that support them. In addition, as modern 802.11 standards begin to push beyond 1Gbps, traditional Ethernet connections over twisted pair cable is no longer enough to support the maximum performance capabilities of the access point. This section discusses the improved performance characteristics of mGig and the network requirements necessary. This section also discusses AP mounting and grounding strategies.

Logical Infrastructure Requirements: This section discusses the logical elements of a wireless network, such as the communication flow of the CAPWAP control and data channels as they traverse the network, and their implications on the underlying physical infrastructure. In addition, this section discusses controller and AP licensing mechanisms.

This chapter covers the following ENWLSD exam topics:

- 2.1 Determine physical infrastructure requirements such as AP power, cabling, switch port capacity, mounting, and grounding
- 2.2 Determine logical infrastructure requirements such as WLC/AP licensing requirements based on the type of wireless architecture

The focus of wireless network design often revolves around the RF aspects of the deployment—and indeed, as discussed throughout this book, RF design is the foundation of any successful wireless network and almost always involves a robust site survey. However, there are key infrastructure components that are just as important in any wireless design exercise. These are generally grouped into two major classes: the physical infrastructure components and logical infrastructure components.

The physical infrastructure includes components of the physical networking gear. This involves the physical gear itself, as well as how the access points are cabled, powered, mounted, and even grounded. This design aspect goes far beyond just the access points and the controller. For example, if a switch is used to deliver PoE to an AP, the switch must be able to accommodate the power requirements of the AP. If it cannot, either the AP will not power on or certain capabilities (such as secondary radios) will not work.

Additionally, the reachability of the APs over standard Ethernet cabling becomes a design criterion as distances from the switch grow and as higher data rates are used. When the existing cable plant cannot support the distances demanded by the placement of APs, suboptimal AP placement may be used, which in turn may lead to poor RF coverage. Understanding the design requirements of the physical infrastructure is a crucial aspect of developing a successful wireless design.

The second infrastructure aspect is the logical network—in other words, the path the communication flows take through the network, regardless of the underlying physical infrastructure. Controller-based wireless networks use CAPWAP (Control And Provisioning of Wireless Access Points), both as a control channel as well as to encapsulate client data traffic, effectively tunneling client traffic directly from the AP to the controller, and vice versa. This gives the logical appearance that the APs and controller are Layer 2 adjacent, when in reality they may be traversing many hops of the underlying physical network. Understanding the behavior and function of these logical elements introduces important considerations when developing the infrastructure side of the wireless design.

This chapter focuses on these two infrastructure aspects, beginning with the physical infrastructure and followed by the logical infrastructure.

"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 4-1 lists the major headings in this chapter and their corresponding "Do I Know This Already?" quiz questions. You can find the answers in Appendix D, "Answers to the 'Do I Know This Already?' Quizzes and Review Questions."

Table 4-1 "Do I Know This Already?" Section-to-Question Mapping

Foundation Topics Section	Questions
Physical Infrastructure Requirements	1–4
Logical Infrastructure Requirements	5–6

1. An access point has been deployed with full features, including dual radios and hyperlocation. The AP requires 38W of power. Which of the following Power over Ethernet capabilities should you recommend be used?
   a. PoE
   b. PoE+
   c. UPOE
   d. UPOE+
2. A group of new Wi-Fi 6 (IEEE 802.11ax) APs has just been installed in a building to replace the older Wi-Fi 5 (802.11ac wave 1) APs. What is a design consideration you need to be aware of when deploying the physical infrastructure?
   a. Mounting of the new APs to reflect changes in the 802.11ax RF radiation pattern.
   b. An increase of power will be required. The switch will need to be upgraded to support either UPOE or UPOE+.

   c. The number of Wi-Fi 6 APs required will be less than the older APs thanks to better performance and coverage patterns.
   d. The switch connected to the APs may need to be upgraded to support mGig.

3. For security reasons, the building facilities team abides by a policy that no devices (APs included) may be visible from the office floor. As an alternative, the network team is looking to deploy the APs above the suspended ceiling. What should they be aware of?
   a. Positioning APs above the ceiling will result in significant RF degradation, so a new site survey may be required.
   b. This configuration is not supported by Cisco.
   c. Specialized mounting brackets will be needed.
   d. The APs should be positioned as close to the T-bar rails as possible.
4. When deploying higher throughput wireless technologies in Local mode, what design aspect must be considered related to possible oversubscription of the physical infrastructure?
   a. Uplink capabilities of the access switch should be considered.
   b. Physical connections between the access switch and AP should be considered.
   c. Performance of the backbone network connecting to the controller should be aligned with overall wireless performance demands.
   d. Performance capabilities of the controller should be considered.
   e. All of the above.
5. What interfaces on a physical controller (such as the WLC 5520) are used to communicate to key services such as ISE and CMX? (Choose two.)
   a. The service port
   b. The Management Interface
   c. The virtual port
   d. Any LAN interface port on the controller
   e. The AP-Manager interface
6. Which Cisco wireless licensing model involves pooling of licenses?
   a. Right-to-Use (RTU) licensing
   b. Perpetual licensing
   c. Term licensing
   d. Product Activation Key (PAK) licensing
   e. Smart Licensing

Foundation Topics

Physical Infrastructure Requirements

The physical infrastructure of a wireless network includes all physical elements, including the access points, controllers, switches and routers, and any other physical network devices that facilitate communication between the wireless users and the network they are trying to access. In addition to networking devices, the physical infrastructure includes power delivery, cabling, mounting, and grounding of access points.

PoE and PoE+

Power over Ethernet (PoE) is a widely used infrastructure technology that allows DC power to be provided to an endpoint over a twisted pair Ethernet cable. Power is passed from power sourcing equipment (PSE), such as a PoE-capable switch, over the existing twisted pair Ethernet cable that carries data communications to powered devices (PDs), such as IP phones, video cameras, wireless access points, point-of-sale machines, access control card readers, LED luminaires, and many more. Through the use of PoE, external powering of endpoints is not required, thus greatly reducing the cost and effort required to deploy electrical power throughout the infrastructure. Typically, for a company to deploy electrical cabling in the ceiling requires a certified electrician to perform the task, whereas the deployment of Ethernet cables (which can run PoE) can be done by anyone, thus greatly simplifying the job of deploying access points wherever they need to go.

The power requirements of endpoints varies based on their power consumption requirements, which is typically a function of the physical function, application, and complexity of the device. For example, basic IP phones might draw approximately 6W of power, whereas contemporary LED lighting fixtures can draw up to 50W for routine operation. Wireless APs draw different power levels depending on which features are enabled and how many radios are concurrently active. For example, the Cisco 3800 typically draws ~30W with all features turned on.

Power delivery over Ethernet twisted pair is based on the IEEE 802.3af (2003) standard and delivers up to 15.4W of DC power per port of the PSE; however, due to power dissipation in the cable, only 12.95W of this is available to the PD.

After the initial introduction of PoE in 2003, endpoints were soon demanding greater power than 802.3af could deliver. Thus, in 2009, IEEE 802.3at was standardized, known as PoE Plus (PoE+). PoE+ delivers up to 30W of DC power per port, ensuring 25.5W of power to a PD due to power dissipation.

In both of these cases, PoE delivers power over two of the four twisted pairs of Class D/Category 5e or better cabling. The PSE uses only signal pairs—that is, the pairs formed by pins 1 and 2 and pins 3 and 6—to transport power from the PSE to the PD and leaves the spare pairs idle (consisting of pins 4 and 5 and pins 7 and 8). Note that PoE does not affect the network performance of Ethernet links to the PD.

UPOE and UPOE+

In recent years the enterprise workspace has continued to evolve, resulting in increasing numbers of devices and workloads converging onto the IP network. This has fueled increasing demand for higher PD power draw, far in excess of what PoE and PoE+ can offer (more than 25.5W).

To meet this demand, Cisco has developed extended PoE capabilities, including Universal PoE (UPOE), capable of delivering 60W per port, and Universal PoE Plus (UPOE+), which is capable of delivering up to 90W per port. Note that while PoE and PoE+ have been standardized by the IEEE, UPOE and UPOE+ are Cisco proprietary. In 2018, the IEEE defined 802.3bt as a standard to deliver up to 90W (sometimes referred to as PoE++).

The network's ability to deliver higher levels of power to endpoints has, in turn, significantly expanded the PoE-capable endpoint landscape. Thanks to these higher PoE capabilities, a wide variety of devices with higher power requirements can now be powered over Ethernet

without requiring separate electrical wiring. These include video endpoints, LED lighting fixtures, digital signage, compact switches, and, of course, larger and more robust access points.

802.3bt, UPOE, and UPOE+ all use the same cabling standard as PoE/PoE+; however, instead of delivering power over just two of the twisted pairs, these higher power embodiments of PoE utilize all four twisted pairs of standard Ethernet cabling (Category 5e or better). They does this by using two PSE controllers to power both the signal pairs and the spare pairs. Figure 4-1 presents the difference between PoE/PoE+ and Cisco UPOE/UPOE+.

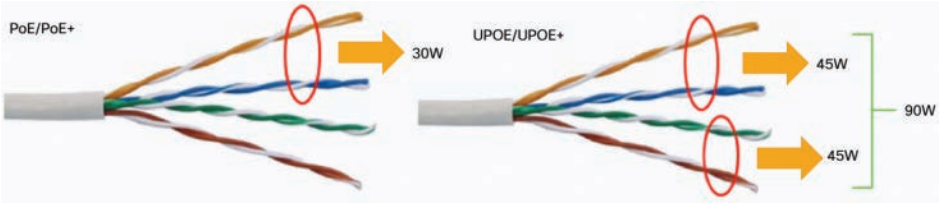


Figure 4-1 *Comparing PoE/PoE+ with UPOE/UPOE+*

In the case of PoE, PoE+, or UPOE, the minimum Ethernet cable type is Category 5e. In the case of UPOE+, Category 6a is required at a minimum. Regardless of the method of power over Ethernet, the maximum cable distance remains the same at 100 meters.

It is also important to note that support for the type of PoE desired depends on the capabilities of the Ethernet switch. For example, older switches may only support PoE/PoE+; however, modern switches (such as the Catalyst 9300) support UPOE, and certain higher-end switches support UPOE+ (such as the Catalyst 9400).

Table 4-2 summarizes the various PoE options available to power network devices.

Key Topic

Table 4-2 A Summary of Power over Ethernet Standards and Capabilities

	PoE	PoE+	UPOE	UPOE+	PoE++ (802.3bt class 4)
Minimum Cable Type	Cat5e	Cat5e	Cat5e	Cat6a	Cat6a
IEEE Standard	IEEE 802.3af	IEEE 802.3at	Cisco proprietary	Cisco proprietary	IEEE 802.3bt
Maximum Power per PoE Port	15.4W	30W	60W	90W	100W (class 4)
Maximum Power to PD	12.95W	25.5W	51W	71W	71W
Twisted Pairs Used	Two pairs	Two pairs	Four pairs	Four pairs	Four pairs
Distance	<100 meters	<100 meters	<100 meters	<100 meters	<100 meters

Power Injectors

PoE delivered by an access switch is a natural choice to power APs in most wireless deployments. This greatly reduces the wiring required and allows flexible AP placement throughout a building. That being said, there are still use cases where PoE delivered by the access switch is not practical, and power injectors must be considered. For example, there may be places where the switch simply doesn't support the necessary PoE mode, or perhaps the switch has no available PoE-capable ports, or it may even have a severely limited power budget due to too many other PDs. In some cases, certain APs with full features enabled may have greater power demands than a legacy PoE switch can offer. In these situations, using a power injector is a simple and often appealing alternative.

Power injectors generally have two Ethernet inputs: one connected to the upstream switch and another connected to the PD (that is, the access point). The power injector is also plugged into a power source via the 48V DC power supply, which then injects power into the two pairs, supporting PoE and PoE+.

Cisco power injectors are offered in two form factors. The first variant supports copper Category 5e or better cables both on the input and output (connected to the switch and to the access point). In this case, maximum cable distance from switch to AP remains at 100 meters—that is, the power injector does not function as a repeater and increase the maximum transmission distance over the twisted pair cable.

The second variant is a fiber optic link between the switch and the power injector. In this case, the power injector functions as a media converter and injects power onto the twisted pair cable that connects to the access point. Using single-mode fiber allows the power injector to be placed up to 2 kilometers from the switch, making it a practical option for places where the AP is far away, such as large factories, warehouses, and other places with sparse wiring closets.

Figure 4-2 illustrates the two power injector options for Cisco access points.

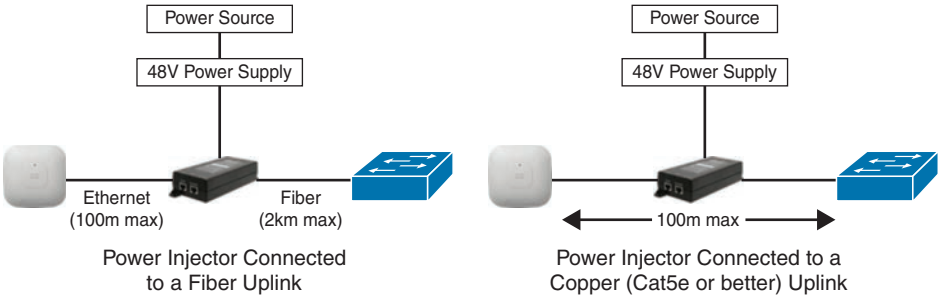


Figure 4-2 *Power Injector Deployment Options*

MultiGigabit

With increasing performance speeds of 802.11ac Wave 2 (Wi-Fi 5) and more recently 802.11ax (Wi-Fi 6), the maximum theoretical wireless throughput of an access point is pushing well beyond the 1Gpbs capability of traditional Ethernet access, potentially making the single wired uplink between the AP and switch a chokepoint.

To solve this problem, Cisco has championed the development of MultiGigabit (mGig) technology that delivers speeds of 2.5Gbps, 5Gbps, or 10Gbps on existing cables. The NBASE-T Alliance (created in 2014) initially led the standards development of MultiGigabit over Ethernet, but it was eventually merged with the Ethernet Alliance in April 2019 and is now marketed as mGig by Cisco. In addition to traditional Ethernet speeds over Category 5e cable, Cisco mGig supports speeds of 2.5Gbps, 5GBps, and 10Gbps. The technology also supports PoE, PoE+, and Cisco UPOE.

The main characteristics mGig are as follows:

- **Variable speeds:** Cisco mGig technology supports auto-negotiation of multiple speeds on switch ports (100Mbps, 1Gbps, 2.5Gbps, and 5bps on Cat 5e cable, and up to 10Gbps over Cat 6a cabling).
- **Flexible cable types:** mGig supports a wide range of cable types, including Cat 5e, Cat 6, and Cat 6a or above.
- **PoE power:** The technology supports PoE, PoE+, and UPOE (up to 60W) for all the supported speeds and cable types, providing access points with additional power for advanced features, such as hyperlocation and modularity.

Figure 4-3 illustrates the use of mGig between a capable access switch and an access point.

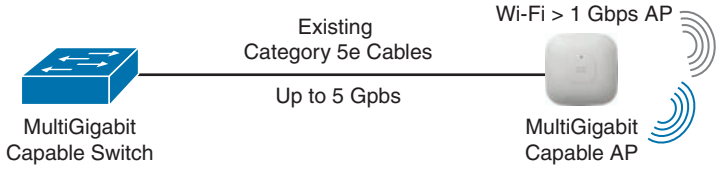


Figure 4-3 *MultiGigabit Connection to an Access Point*

Cisco 3800 and 4800 series access points (802.11ac Wave 2) and Cisco Catalyst 9100 series APs (Wi-Fi 6 / 802.11ax) support Cisco mGig technology at speeds of 2.5Gbps and 5Gbps. This technology protects the investment in the cabling infrastructure, allowing for newer and faster wireless technologies to be transported over the same physical Ethernet infrastructure without becoming a chokepoint.

To summarize, Table 4-3 illustrates the different mGig speeds and supported cable categories.

Key Topic

Table 4-3 Supported mGig Speeds with Associated Cable Categories

	1G	2.5G	5G	10G
Cat5e	Yes	Yes	Yes	N/A
Cat6	Yes	Yes	Yes	Yes (up to 55m)
Cat6a	Yes	Yes	Yes	Yes

Mounting Access Points

Wireless deployments often require a variety of different AP mounting options depending on the physical attributes and accessibility of each location. To address this, Cisco offers

several different mounting bracket options. In addition, several third-party vendors provide mounting brackets and enclosures for less common scenarios.

This section discusses the three most common options for mounting Cisco APs:

- Ceiling and wall mounting
- Mounting below ceiling tiles
- Mounting above ceiling tiles

Ceiling and Wall Mounting Access Points

When mounting on a horizontal or vertical surface, you can use one of the two standard mounting brackets:

- **AIR-AP-BRACKET-1**: This mounting option features a low profile, making it a popular choice for ceilings.
- **AIR-AP-BRACKET-2**: This is a universal mounting bracket that is often used if the AP will be mounted on the wall or placed in a NEMA (National Electrical Manufacturers Association) enclosure.

Figure 4-4 illustrates the two mounting bracket options.

AIR-AP-BRACKET-1 (low profile) AIR-AP-BRACKET-2 (universal)

Figure 4-4 *Cisco Access Point Mounting Bracket Options*

When wall mounting is desired, the installer should understand that walls can be a physical obstacle to the RF signal; therefore, maintaining 360-degree coverage can be compromised by the wall if the AP is not placed correctly. If the wall is an outside wall and/or if the goal is to transmit the signal in a narrower beam (such as down a food aisle in a grocery store), a directional antenna may be a better choice, assuming the external antenna model of an AP is used.

In most cases, it is recommended to avoid wall-mounting APs with internal antennas, as the antenna orientation of these APs is optimally designed for ceiling mount, providing RF coverage in a 360-degree pattern to the space below the floor. If the AP is wall mounted, it is recommended to use either a right-angle mount (where the AP is still oriented downward) or external antennas that project the RF energy into the space as expected. For this reason, it is generally recommended to mount indoor APs on the ceiling rather than on a wall.

Mounting Access Points Below a Suspended Ceiling

To facilitate mounting APs below a suspended ceiling, specialized mounting brackets are available that clip onto the rail of a T-bar ceiling. Figures 4-5 and 4-6 illustrate the mounting bracket for these types of ceilings.

Figure 4-5 *T-Bar Ceiling Mounting Bracket Options*

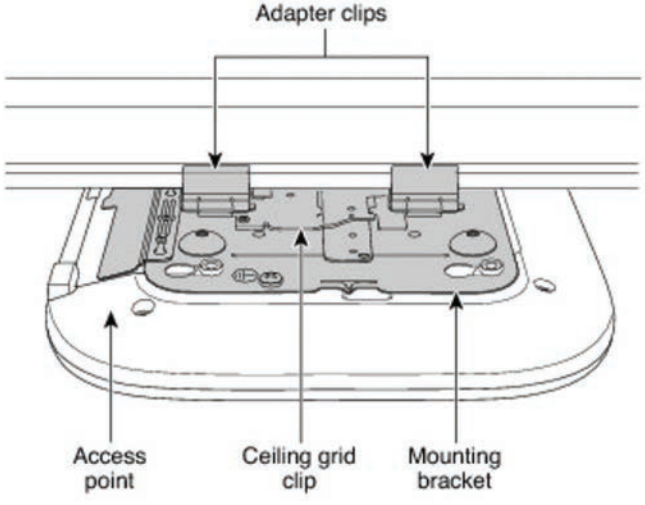
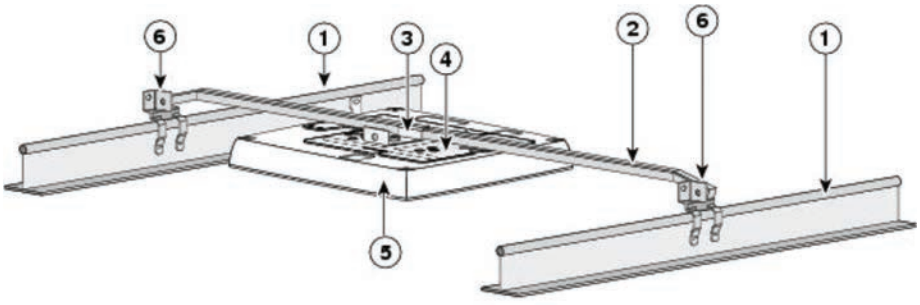


Figure 4-6 *Mounting an AP on a T-Bar Ceiling*

Mounting Access Points Above the Ceiling Tiles

Mounting access points below the ceiling tiles is the preferred option; however, in some cases, wireless engineers may prefer to position the access points so that nothing is visible from the ground, or there may be a building facilities policy that prohibits any device from attaching to the suspended ceiling. Mounting above the ceiling tiles may also be preferred for aesthetic reasons, or it may be done as a way to reduce theft in vulnerable areas (such as public hotspots where theft or damage may be a problem). In such circumstances, Cisco indoor access points (such as the Catalyst 9120i and 9120e) are rated for installation in the plenum area above the suspended ceiling (UL-2043), allowing them to be attached to the T-bar mesh but suspended above the tile.

Figure 4-7 illustrates a mounting schematic for an AP above the ceiling tiles.



1	Suspended ceiling T-rail	4	Mounting bracket
2	Box hanger	5	Access point
3	Box hanger clip	6	T-rail clip

Figure 4-7 *Mounting the Access Point Above the Ceiling Tiles*

When mounting the AP above the ceiling tiles, it is important to remember that the tiles must not be conductive, as this would have a degrading effect on the RF performance of the AP and may interfere with wireless LAN features that depend on uniform coverage, such as voice and location services. Additionally, the AP should be mounted as close to the center of the ceiling tile as possible and away from any possible obstructions that could interfere with RF performance.

Grounding and Securing Access Points

Grounding is not always required for indoor installations because access points are classified as low-voltage devices and do not contain internal power supplies. However, electrical grounding is always recommended for outdoor access points. It is always best to check with local electrical standards to determine if grounding is necessary.

Although grounding is not mandatory for most indoor access points, it is required in certain scenarios. For example, in unground scenarios such as mining operations, indoor access points that are mounted too close to an electromagnetic source of interference may reboot suddenly or suffer hardware damage (such as APs deployed near a fluorescent light). This may occur even if the AP is not physically touching the electrical source but is just in close proximity to the electromagnetic source of interference. Grounding this access point or the mounting bracket helps prevent this issue from occurring. It is recommended that a certified electrical technician verify whether the installation requires grounding.

Figure 4-8 shows an outdoor access point with the grounding connector.

Figure 4-8 *An Outdoor Access Point with Electrical Grounding (Photo Credit: Ian Procyk)*

Logical Infrastructure Requirements

The path in which traffic flows through a network appears differently depending on your point of view. For example, from a network technician's point of view, a packet travels through the network in a hop-by-hop path across each physically connected device. However, from a wireless end user's perspective, if traffic is tunneled in an overlay, the user may only see one hop between an access point and the controller, when in reality numerous physical hops were encountered along the path of the underlying network. This is the difference between the physical and logical network.

Traffic also flows differently depending on the deployment model chosen: autonomous access points act as direct links between the wireless and the wired sides of the network, whereas centrally controlled access points in Local mode must forward all wireless client traffic to the controller over an encapsulated CAPWAP tunnel. In FlexConnect mode, some WLANs may be locally switched at the AP, while others may be centrally switched on the controller.

The following section will explore some of the logical infrastructure characteristics of a wireless network, including flow of the CAPWAP channels, logical connections to services supporting the wireless infrastructure such as AAA and DHCP servers, and finally the licensing options that are available to support the wireless deployment.

CAPWAP Flow

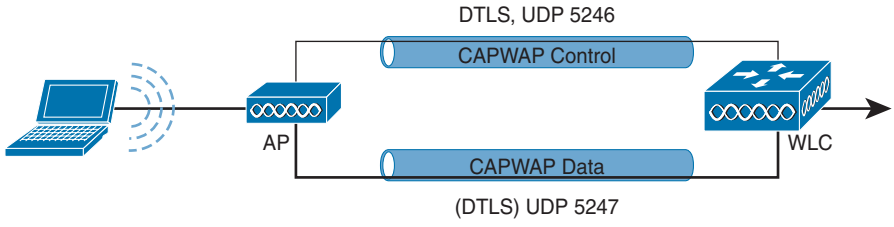
CAPWAP is a logical network connection between access points and a wireless LAN controller. CAPWAP is used to manage the behavior of the APs as well as tunnel encapsulated 802.11 traffic back to the controller.

CAPWAP sessions are established between the AP's logical IP address (gained through DHCP) and the controller's **management interface**. (In older versions of AireOS, the CAPWAP session terminated on the **ap-manager** interface; however, this has been changed to the management interface in more recent versions of AireOS.)

Whether in Local or FlexConnect mode, CAPWAP sessions between the controller and AP are used to manage the behavior of the AP. When in Local mode, CAPWAP is additionally

used to encapsulate and tunnel all wireless client traffic so that it can be centrally processed by the controller. CAPWAP sessions use UDP for both the control and data channels, as follows:

- **CAPWAP Control Channel:** Uses UDP port 5246
- **CAPWAP Data Channel:** Uses UDP port 5247 and encapsulates (tunnels) the client's 802.11 frames
- Figure 4-9 illustrates the different CAPWAP channels between an AP and a controller.



Key Topic

Figure 4-9 *CAPWAP Control and Data Plane Channels*

If there is a firewall or router with access control lists (ACLs) along the logical path between the AP and the controller, it is important to ensure that rules are in place to allow both the CAPWAP control and data channel ports through the firewall so that the AP and controller are able to communicate correctly. A complete list of recommended firewall rules can be found here:

https://www.cisco.com/c/en/us/support/docs/wireless/5500-series-wireless-controllers/113344-cuwn-ppm.html

As the number of APs grows, so does the number of CAPWAP tunnels terminating on the controller. Figure 4-10 illustrates the logical connection of multiple CAPWAP sessions over the physical infrastructure.

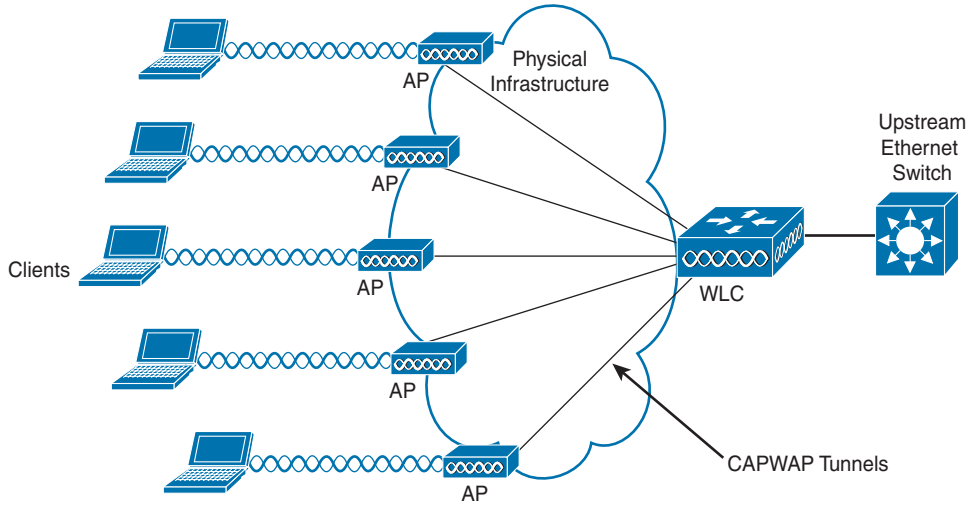


Figure 4-10 *CAPWAP Sessions Between the APs and the Controller*

NOTE In Autonomous mode, the AP switches all traffic locally and CAPWAP is not used. In FlexConnect mode, wireless client traffic is switched locally while control of the AP is managed over the CAPWAP control channel. Only centrally controlled APs in Local mode use both the CAPWAP control and data channels. FlexConnect mode may use a hybrid—some WLANs may be locally switched while others are centrally switched, where the data traffic comes back to the controller over the CAPWAP data channel. In either case, FlexConnect APs are still managed by the CAPWAP control channel.

Considering that all APs in Local mode use CAPWAP to tunnel 802.11 client traffic back to the controller, an important design criterion related to traffic load must be considered. With 802.11ac Wave 2, the maximum theoretical throughput of a single AP is ~1.3Gbps. 802.11ax (Wi-Fi 6) promises even greater speeds, with the theoretical throughput expected to be in excess of 10Gbps from a single AP (based on multiple streams). Considering the CAPWAP data channel will need to support increasing levels of data throughput (not to mention framing and packet overhead), the demands of the logical infrastructure have a direct correlation to capabilities of the underlying physical infrastructure. In this vein, careful analysis must be taken at various places in the network to determine if the performance demands of the wireless network can be met. This includes the following design aspects:

- The physical connection between the AP and the access switch (evaluate if mGig is required)
- An estimation of oversubscription of the uplink of the access switch to the network
- Backbone capacity of the core network
- WAN connection speeds if the controllers are centralized and APs are in Local mode
- Network access speeds to the controller
- Performance capabilities of the controller

From a design perspective, the theoretical maximum bandwidth consumption of an AP is usually never attained. However, if enough APs are simultaneously generating a high volume of traffic, a controller can quickly run out of resources. Take the example of a controller that is licensed for 500 APs. If these were all Wi-Fi 6 APs passing an excessively high volume of traffic, the aggregate bandwidth capacity of the physical connection to the controller could be quickly exhausted, meaning more controllers wither fewer APs may be necessary.

Performance issues at the controller may manifest in two possible ways: (1) the underlying network's ability to aggregate all CAPWAP data traffic and forward it without oversubscription of the physical links connected to the controller, and (2) the controller's own performance limitations in being able to process the volume of data it is receiving.

If either of these two cases emerges, certain design changes can be considered. One change is decentralizing and splitting the function of the controllers such that less data is being managed by a single controller. Another option is to simply reduce the number of APs that each controller manages. If decentralizing the controllers is preferred, the roaming path must also be considered. While roaming between APs connected to the same controller is simple and

should be seamless, if clients roam to an AP connected to a different controller, the roaming path will involve intercontroller communication and greater network complexity.

Another area where oversubscription may be an issue is on the access switch where the APs are physically connected. Take the example of an access switch with several dozen APs connected with mGig, all running Wi-Fi 6. If the clients associated to these APs are generating large amounts of aggregate data, the throughput demands could quickly exhaust even a 10Gbps uplink from the access switch. Thus, it is imperative to assess not only how many APs are being deployed (and how many of each type), but also careful calculation must be made to determine if the uplink capacity of the access switches can accommodate expected traffic demands, including how much oversubscription is acceptable. If it is found that the oversubscription rate is excessive, then either multiple uplinks will be needed (which requires port channeling) or a fewer number of APs should be deployed on each access switch.

NOTE Oversubscription of centrally controlled APs over the WAN can be addressed using FlexConnect mode, which is discussed in detail in Chapter 10, "Implementing FlexConnect."

AAA and DHCP Services Logical Path

Another area where the logical path requires careful consideration is the path between the controller and the key services, such as the AAA and DHCP servers. Services such as AAA (ISE), DHCP, DNS, MSE/CMX, DNA Spaces, and many more may be placed at locations throughout the network that have firewalls protecting them. Understanding the logical path between these services will often require opening of firewall rules for the service to interface with the controller.

As with CAPWAP, the controller's **management interface** is used to communicate with AAA servers, as well as a host of other services, including MSE/CMX, directory servers, other controllers, and more.

For DHCP, controllers proxy communication to the DHCP sever on behalf of clients using the controller's IP address in the VLAN associated to the WLAN of those clients.

Table 4-4 summarize the ports that must be open to allow the controller to communicate with key services.

Key Topic

Table 4-4 Summary of AAA and DHCP Services and Ports Used for the Wireless Infrastructure

Service	Port
RADIUS Authentication	UDP port 1812 (some older versions use UDP port 1645)
RADIUS Authorization	UDP port 1813 (some older versions use UDP port 1646)
DHCP Server	UDP port 67
DHCP Client	UDP port 68

Licensing Overview

In addition to purchasing the controller itself, Cisco wireless deployments require licenses to activate the use of the access points. The following section provides a summary of how Cisco wireless controllers and APs are licensed.

Cisco AireOS wireless controllers support two types of licensing models: Right to Use (RTU) licensing and Smart Licensing.

Right to Use Licensing

Right to Use (RTU) licensing is an honor-based licensing mechanism that allows AP licenses to be enabled on AireOS controllers (such as the 5520 and 8500 series controllers) with end user license agreement (EULA) acceptance. The RTU license scheme simplifies the addition, deletion, and transfer of AP licenses and does not require specialized license keys or product activation key (PAK) licenses.

With RTU licensing, there are three types of licenses:

- **Permanent licenses:** The AP count is programmed into nonvolatile memory at the time of manufacturing. These licenses are not transferable from one controller to another.
- **Adder access point count licenses:** These are additional licenses that can be activated through the acceptance of the agreement. These licenses are also transferable between controllers and types of AireOS controllers.
- **Evaluation licenses:** These are used for demo and/or trial periods and are valid for 90 days, and they default to the full capacity of the controller. The evaluation license activation is performed through the AireOS command-line interface (CLI).

Smart Licensing

In addition to the RTU licensing model, AireOS controllers support Smart Licensing. Smart Licensing is a cloud-based flexible licensing model that simplifies the way licenses are managed across an organization rather than on a per-controller basis. The intent of Smart Licensing is to make it easier to manage and deploy Cisco software licenses from a central repository without having to track how licenses are used on individual products.

Instead of using product activation keys (PAKs) or RTU licensing, Smart Licenses establish a central pool of AP software licenses in a customer-defined Smart Account that can be used across the enterprise and across all controllers or APs. Smart Licensed products self-register upon configuration and activation with a single token, removing the need to register products individually with separate PAKs or to accept a license agreement. Thus, instead of licensing each individual controller for the number of APs that the administrator anticipates it to manage, the pool of licenses can be shared across all controllers in the enterprise and be used as needed. This approach has a distinct advantage over legacy licensing models by greatly simplifying and optimizing the use of licenses.

In the RTU model, one controller may be licensed for far more APs than it is currently managing, whereas another controller may not have enough licenses for what it needs. Smart Licensing eliminates the overhead and waste by simply putting all AP licenses in a central pool that can be managed and budgeted for as the need arises. As new APs are added or moved across the organization, the administrator no longer needs to determine the current license count on a per-controller basis—only the Smart Licensing pool of AP licenses needs to be monitored and maintained. This not only provides better utilization of licenses but also it makes it easier to procure and deploy licenses as the organization grows.

To use Smart Licensing, the following steps must be followed:

Step 1. Create a Smart Account:

- **a.** Create a Smart Account at the following link: https://software.cisco.com/software/company/smartaccounts/home#accountcreation-account.
- **b.** Go to Cisco Software Central at software.cisco.com.
- **c.** An editable profile appears.
- **d.** An email is automatically sent to the customer Smart Account administrator.

Step 2. Register the Cisco controller using the Smart Account.

- **a.** For existing customers, deposit existing licenses, if any, into the Smart Account.
- **b.** For a new purchase, purchase a Cisco DNA license for access points connecting to the Cisco Catalyst controller.

Step 3. Configure the license level on the controller, as desired.

NOTE Unlike AireOS controllers, Catalyst 9800 controllers require mandatory Smart Licensing. While no licenses are required to boot up the controller, in order to connect any access points, Cisco DNA licenses managed through Smart Licensing are required for each access point that connects to the controller.

Summary

This chapter focused on both the physical and logical infrastructure requirements of wireless LAN deployments. In this chapter you have learned the following:

- The various PoE options available for different APs as well as the capabilities and function of each PoE mechanism.
- How higher-performance wireless standards, such as 802.11ac Wave 2 (Wi-Fi 5) and 802.11ax (Wi-Fi 6), can be supported through mGig
- AP mounting options, including above and below a tile ceiling mount and wall mount options
- The importance of grounding APs in certain situations
- The need to consider the logical path and its impact on the underlying physical infrastructure, including the CAPWAP control and data channels as well as AAA and DHCP services
- Different types of licensing models available for different Cisco Wireless LAN controllers, including RTU licensing and Smart Licensing, which is as a method of pooling licenses across the enterprise

References

For additional information, refer to these resources:

Cisco Enterprise Wireless—Intuitive Wi-Fi Starts Here: https://www.cisco.com/c/dam/en/us/products/collateral/wireless/nb-06-wireless-wifi-starts-here-ebook-cte-en.pdf

Catalyst 9120 Access Point Deployment Guide: https://www.cisco.com/c/en/us/products/collateral/wireless/catalyst-9100ax-access-points/guide-c07-742311.html

Network World—Best Practices When Cabling an Access Point: https://www.networkworld.com/article/3290459/what-are-the-best-practices-when-cabling-for-wi-fi.html

Power over Ethernet: Empowering Digital Transformation: https://www.cisco.com/c/dam/en/us/products/collateral/switches/catalyst-9000/nb-06-upoe-plus-wp-cte-en.pdf

Transform the Workspace with Cisco MultiGigabit Ethernet White Paper: https://www.cisco.com/c/en/us/solutions/collateral/enterprise-networks/catalyst-multigigabit-switching/white-paper-c11-733705.html

Cisco Smart Licensing Overview: https://www.cisco.com/c/dam/en/us/products/collateral/software/smart-accounts/q-and-a-c67-741561.pdf

Exam Preparation Tasks

As mentioned in the section "How to Use This Book" in the Introduction, you have a few choices for exam preparation: the exercises here, Chapter 18, "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 Topic icon in the outer margin of the page. Table 4-5 lists these key topics and the page numbers on which each is found.

Key Topic

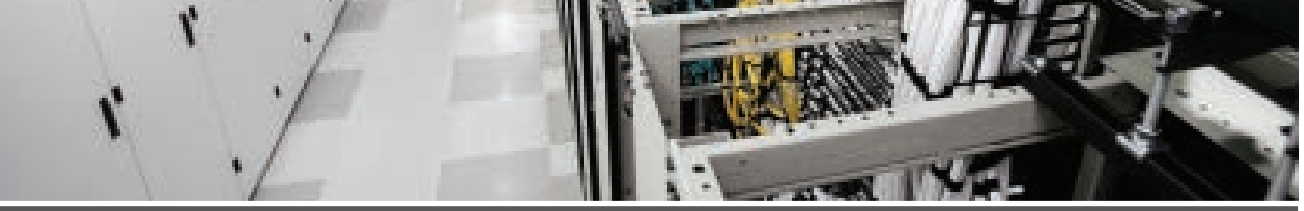
Table 4-5 Key Topics for Chapter 4

Key Topic Element	Description	Page Number
Table 4-2	Summary of Power over Ethernet Standards and Capabilities	70
Table 4-3	Supported mGig Speeds with Associated Cable Categories	72
Figure 4-9	CAPWAP Control and Data Plane Channels	77
Table 4-4	Summary of AAA and DHCP Services and Ports Used for the Wireless Infrastructure	79

Define Key Terms

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

PoE, PoE+, UPOE, UPOE+, Power Sourcing Equipment (PSE), Powered Device (PD), Power Injector, Cisco MultiGigabit, Right to Use (RTU), End User License Agreement (EULA), Smart Licensing



Index

Numerics

A

B

C

D

E

F

G

H

I

J-K-L

M

N

O

P

Q

R

S

T

U

V

W

X-Y-Z