



Official Cert Guide

Learn, prepare, and practice for exam success



CCNA Wireless 200-355

ciscopress.com

DAVID HUCABY, CCIE® No. 4594

FREE SAMPLE CHAPTER



SHARE WITH OTHERS

CCNA Wireless 200-355 Official Cert Guide

DAVID HUCABY, CCIE NO. 4594

Cisco Press

800 East 96th Street
Indianapolis, IN 46240

CCNA Wireless 200-355 Official Cert Guide

David Hucaby

Copyright© 2016 Pearson Education, Inc.

Published by:

Cisco Press

800 East 96th Street

Indianapolis, IN 46240 USA

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

Printed in the United States of America

First Printing December 2015

Library of Congress Control Number: 2015955570

ISBN-13: 978-1-58714-457-8

ISBN-10: 1-58714-457-3

Warning and Disclaimer

This book is designed to provide information about preparing for the CCNA Wireless 200-355 exam. Every effort has been made to make this book as complete and as accurate as possible, but no warranty or fitness is implied.

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

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

Trademark Acknowledgments

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

Special Sales

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

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

For questions about sales outside the U.S., please contact international@pearsoned.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.

Publisher: Paul Boger

Associate Publisher: Dave Dusthimer

Business Operation Manager, Cisco Press: Jan Cornelssen

Executive Editor: Mary Beth Ray

Managing Editor: Sandra Schroeder

Senior Development Editor: Christopher Cleveland

Senior Project Editor: Tonya Simpson

Copy Editor: Bill McManus

Technical Editor: Jerome Henry

Editorial Assistant: Vanessa Evans

Cover Designer: Mark Shirar

Composition: Studio Galou

Indexer: Publishing Works

Proofreader: Laura Hernandez



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.

CCDE, CCENT, Cisco Eos, Cisco HealthPresence, the Cisco logo, Cisco Lumin, Cisco Nexus, Cisco StadiumVision, Cisco TelePresence, Cisco WebEx, DCE, and Welcome to the Human Network are trademarks; Changing the Way We Work, Live, Play, and Learn and Cisco Store are service marks; and Access Registrar, Aironet, AsyncOS, Bringing the Meeting To You, Catalyst, CCDA, CCDP, CCIE, CCIQ, CCNA, CCNP, CCSP, CCVP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Collaboration Without Limitation, EtherFast, EtherSwitch, Event Center, Fast Step, Follow Me Browsing, FormShare, GigaDrive, HomeLink, Internet Quotient, IOS, iPhone, iQuick Study, IronPort, the IronPort logo, LightStream, Linksys, MediaTone, MeetingPlace, MeetingPlace Chime Sound, MGX, Networkers, Networking Academy, Network Registrar, PCNow, PIX, PowerPanels, ProConnect, ScriptShare, SenderBase, SMARTnet, Spectrum Expert, StackWise, The Fastest Way to Increase Your Internet Quotient, TransPath, WebEx, and the WebEx logo are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0812R)

About the Author

David Hucaby, CCIE No. 4594, is a network engineer for a large university healthcare network based on Cisco wireless products. David has bachelor's and master's degrees in electrical engineering from the University of Kentucky. He is the author of several Cisco Press titles, including *CCNP SWITCH Exam Certification Guide*; *Cisco LAN Switching Video Mentor*; *CCNP Security FIREWALL Exam Certification Guide*; *Cisco ASA, PIX, and FWSM Firewall Handbook*, Second Edition; and *Cisco Firewall Video Mentor*.

David lives in Kentucky with his wife, Marci, and two daughters.

About the Technical Reviewer

Jerome Henry, CCIE Wireless No. 24750, is a technical marketing engineer in the Wireless Enterprise Networking Group at Cisco systems. Jerome has close to 17 years of experience teaching technical Cisco courses in more than 15 different countries and 4 different languages, to audiences ranging from bachelor degree students to networking professionals and Cisco internal system engineers.

Focusing on his wireless experience, Jerome joined Cisco in 2012. Before that time, he was consulting and teaching Heterogeneous Networks and Wireless Integration with the European Airespace team, which Cisco later acquired to become its main wireless solution. He then spent several years with a Cisco Learning Partner developing wireless courses and working on training material for new wireless technologies. In addition to his CCIE Wireless certification, Jerome is a Certified Wireless Networking Expert (CWNE No. 45) and has developed several Cisco courses focusing on wireless topics (IUWNE, IUWMS, IUWVN, CUWSS, IAUWS, LBS, CWMN lab guide, and so on) and authored several Wireless books (*CCNP Wireless IUWMS Quick Reference*, *CCNP Wireless CUWSS Quick Reference*, and so on). Jerome also is an IEEE 802.11 group member and participant of 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 in 2009. He is based in the Research Triangle Park in North Carolina.

Dedications

As always, this book is dedicated to the most important people in my life: my wife, Marci, my two daughters, Lauren and Kara, and my parents, Reid and Doris Hucaby. Their love, encouragement, and support carry me along. I'm so grateful to God, who gives endurance and encouragement (Romans 15:5), who has allowed me to enjoy networking and working on projects like this, and who invented wireless communication. With a higher purpose.

As the sign in front of a church near my home says: "Prayer: The world's greatest wireless connection."

Acknowledgments

It has been my great pleasure to work on another Cisco Press project. I've now been writing Cisco Press titles continuously for more than 15 years. I have physically worn out several laptop keyboards and probably several Cisco Press editors in the process. I am most thankful that Chris Cleveland has never worn out—he has been the development editor for almost every project I have ever worked on. I can't say enough good things about working with him. I am grateful to Mary Beth Ray for inviting me back to revise this book, Tonya Simpson as the project editor, Bill McManus for raising the copy editing bar to an amazing height, and many other Cisco Press folks who have worked hard to make this book happen.

I am very grateful for the insight, knowledge, and helpful comments that Jerome Henry has provided. He is a tremendous resource for wireless networking expertise and training. Jerome's input has made this a more well-rounded book and me a more educated author.

As always, I have enjoyed the good discussions with my dad, Reid Hucaby, a fellow EE and a seasoned RF engineer, that this book has prompted about all things wireless.

Finally, I am indebted to my co-worker and good friend, Rick Herring, who has been saying for years that I should write a wireless book one day. I always thought he was joking until now.

Contents at a Glance

	Introduction	xxi
Chapter 1:	RF Signals and Modulation	3
Chapter 2:	RF Standards	37
Chapter 3:	RF Signals in the Real World	71
Chapter 4:	Understanding Antennas	91
Chapter 5:	Wireless LAN Topologies	111
Chapter 6:	Understanding 802.11 Frame Types	129
Chapter 7:	Planning Coverage with Wireless APs	153
Chapter 8:	Understanding Cisco Wireless Architectures	183
Chapter 9:	Implementing Autonomous and Cloud Deployments	211
Chapter 10:	Implementing Controller-based Deployments	231
Chapter 11:	Understanding Controller Discovery	265
Chapter 12:	Understanding Roaming	281
Chapter 13:	Understanding RRM	305
Chapter 14:	Wireless Security Fundamentals	327
Chapter 15:	Configuring a WLAN	353
Chapter 16:	Implementing a Wireless Guest Network	371
Chapter 17:	Configuring Client Connectivity	385
Chapter 18:	Managing Cisco Wireless Networks	409
Chapter 19:	Dealing with Wireless Interference	429
Chapter 20:	Troubleshooting WLAN Connectivity	449
Chapter 21:	Final Review	475
Appendix A:	Answers to the “Do I Know This Already?” Quizzes	487
Appendix B:	Modulation and Coding Schemes	505
Appendix C:	CCNA Wireless 200-355 Exam Updates	513
	Key Terms Glossary	515
	Index	529

On the DVD

Appendix D: Study Planner

Key Terms Glossary

Contents

Introduction	xxi
Chapter 1 RF Signals and Modulation	3
“Do I Know This Already?” Quiz	3
Foundation Topics	7
Comparing Wired and Wireless Networks	7
Understanding Basic Wireless Theory	7
Understanding Frequency	9
Understanding Phase	14
Measuring Wavelength	14
Understanding RF Power and dB	15
<i>Important dB Laws to Remember</i>	17
<i>Comparing Power Against a Reference: dBm</i>	19
<i>Measuring Power Changes Along the Signal Path</i>	20
<i>Understanding Power Levels at the Receiver</i>	23
Carrying Data Over an RF Signal	24
FHSS	26
DSSS	27
1-Mbps Data Rate	28
2-Mbps Data Rate	28
5.5-Mbps Data Rate	29
11-Mbps Data Rate	30
OFDM	30
Modulation Summary	32
Exam Preparation Tasks	34
Review All Key Topics	34
Key Terms	34
Chapter 2 RF Standards	37
“Do I Know This Already?” Quiz	37
Foundation Topics	41
Regulatory Bodies	41
ITU-R	41
FCC	42
ETSI	44
Other Regulatory Bodies	45

IEEE Standards Body	45
802.11 Channel Use	47
Channels in the 2.4-GHz ISM Band	47
Channels in the 5-GHz U-NII Bands	49
IEEE 802.11 Standards	50
802.11-1997	51
802.11b	51
802.11g	52
802.11a	53
802.11n	54
<i>Channel Aggregation</i>	55
<i>Spatial Multiplexing</i>	57
<i>MAC Layer Efficiency</i>	58
<i>Transmit Beamforming</i>	59
<i>Maximal-Ratio Combining</i>	60
802.11n Modulation and Coding Schemes	60
802.11ac	60
<i>Robust Channel Aggregation</i>	61
<i>Dense Modulation</i>	63
<i>MAC Layer Efficiency</i>	63
<i>Explicit Transmit Beamforming</i>	64
<i>Scalable MIMO</i>	64
<i>Multi-user MIMO</i>	64
802.11ac Implementation	65
802.11 in Other Frequency Bands	65
Wi-Fi Alliance	66
Exam Preparation Tasks	68
Review All Key Topics	68
802.11 Protocol Summary	68
Define Key Terms	69
Chapter 3	RF Signals in the Real World
	71
“Do I Know This Already?” Quiz	71
Foundation Topics	74
Interference	74
Co-Channel Interference	74
Neighboring Channel Interference	75
Non-802.11 Interference	76

Free Space Path Loss	77
Mitigating the Effects of Free Space Path Loss	79
Effects of Physical Objects	80
Reflection	81
Absorption	82
Scattering	83
Refraction	83
Diffraction	84
Fresnel Zones	84
Exam Preparation Tasks	88
Review All Key Topics	88
Define Key Terms	88

Chapter 4 Understanding Antennas 91

“Do I Know This Already?” Quiz	91
Foundation Topics	94
Antenna Characteristics	94
Radiation Patterns	94
Gain	97
Beamwidth	97
Polarization	98
Antenna Types	99
Omnidirectional Antennas	99
Directional Antennas	103
Antenna Summary	107
Adding Antenna Accessories	107
Exam Preparation Tasks	109
Review All Key Topics	109
Define Key Terms	109

Chapter 5 Wireless LAN Topologies 111

“Do I Know This Already?” Quiz	111
Foundation Topics	114
Types of Wireless Networks	114
Wireless LAN Topologies	115
Basic Service Set	116
Distribution System	118
Extended Service Set	120
Independent Basic Service Set	122

Other Wireless Topologies	122
Repeater	122
Workgroup Bridge	123
Outdoor Bridge	124
Mesh Network	125
Exam Preparation Tasks	126
Review All Key Topics	126
Define Key Terms	126
Chapter 6	Understanding 802.11 Frame Types 129
“Do I Know This Already?” Quiz	129
Foundation Topics	132
802.11 Frame Format	132
802.11 Frame Addressing	134
Accessing the Wireless Medium	136
Carrier Sense	137
Collision Avoidance	137
802.11 Frame Types	140
Management Frames	140
Control Frames	141
Data Frames	142
Client Housekeeping	142
A Client Scans for APs	143
A Client Joins a BSS	144
A Client Leaves a BSS	145
A Client Moves Between BSSs	146
A Client Saves Power	147
Exam Preparation Tasks	151
Review All Key Topics	151
Define Key Terms	151
Chapter 7	Planning Coverage with Wireless APs 153
“Do I Know This Already?” Quiz	153
Foundation Topics	157
AP Cell Size	157
Tuning Cell Size with Transmit Power	157
Tuning Cell Size with Data Rates	159

Adding APs to an ESS	162
The Roaming Process	163
WLAN Channel Layout	165
Designing and Validating Coverage with Site Surveys	169
Applications and Their Requirements	169
Site Survey Types and Tools	171
Predictive or Planning Surveys	172
Passive Site Surveys	174
Active Site Surveys	175
Developing a Complete Survey Strategy	178
Exam Preparation Tasks	180
Review All Key Topics	180
Define Key Terms	180
Site Survey Type and Application Highlights	180
Chapter 8 Understanding Cisco Wireless Architectures	183
“Do I Know This Already?” Quiz	183
Foundation Topics	187
Distributed Architectures	187
Autonomous Architecture	187
Cloud-based Architecture	190
Split-MAC Architectures	192
Centralized Wireless Network Architecture	197
Converged Wireless Network Architecture	200
FlexConnect Wireless Network Architecture	204
Cisco Wireless Network Building Blocks	205
Cisco Wireless LAN Controllers	205
Cisco APs	206
Exam Preparation Tasks	209
Review All Key Topics	209
Chapter 9 Implementing Autonomous and Cloud Deployments	211
“Do I Know This Already?” Quiz	211
Foundation Topics	214
Initially Configuring an Autonomous AP	215
Connecting the AP	215
Initially Configuring the AP	217
Upgrading an Autonomous AP	221

Initially Configuring Cloud-based APs 223

Exam Preparation Tasks 228

Review All Key Topics 228

Define Key Terms 228

Chapter 10 Implementing Controller-based Deployments 231

“Do I Know This Already?” Quiz 231

Foundation Topics 235

Connecting a Centralized Controller 235

 Using Controller Ports 235

 Using Controller Interfaces 237

Performing an Initial Setup 238

 Initial Setup of a Centralized Controller with the Configuration Wizard 239

 Initial Setup of a Converged Controller with the Configuration Wizard 247

 Initial Setup of a Centralized Controller with WLAN Express Setup 254

 Initial Setup of a Centralized Controller with the CLI 257

Maintaining a Wireless Controller 258

 Backing Up Controller Configurations 258

 Updating Wireless LAN Controller Code 259

 Updating Wireless Control Module Code 262

Exam Preparation Tasks 263

Review All Key Topics 263

Define Key Terms 263

Chapter 11 Understanding Controller Discovery 265

“Do I Know This Already?” Quiz 265

Foundation Topics 268

Discovering a Controller 268

 AP States 268

 Discovering a WLC 270

 Selecting a WLC 271

 Designing High Availability 272

 Detecting a Controller Failure 274

 Building Redundancy 274

N+1 Redundancy 274

N+N Redundancy 275

N+N+1 Redundancy 276

SSO Redundancy 277

Exam Preparation Tasks 279

Review All Key Topics 279

Define Key Terms 279

Chapter 12 Understanding Roaming 281

“Do I Know This Already?” Quiz 281

Foundation Topics 285

Roaming Overview 285

Roaming Between Autonomous APs 285

Intracontroller Roaming 288

Roaming Between Centralized Controllers 290

Layer 2 Roaming 290

Layer 3 Roaming 292

Scaling Mobility with Mobility Groups 296

Roaming Coordination with Centralized Controllers 298

Roaming Between Converged Controllers 300

Exam Preparation Tasks 303

Review All Key Topics 303

Define Key Terms 303

Chapter 13 Understanding RRM 305

“Do I Know This Already?” Quiz 305

Foundation Topics 308

Configuring 802.11 Support 308

Configuring Data Rates 309

Configuring 802.11n and 802.11ac Support 310

Understanding RRM 311

RF Groups 313

TPC 315

DCA 318

Coverage Hole Detection Mitigation 320

Manual RF Configuration 322

Verifying RRM Results 323

Exam Preparation Tasks 325

Review All Key Topics 325

Define Key Terms 325

Chapter 14 Wireless Security Fundamentals 327

“Do I Know This Already?” Quiz 327

Foundation Topics	331
Anatomy of a Secure Connection	331
Authentication	332
Message Privacy	333
Message Integrity	334
Intrusion Protection	335
Wireless Client Authentication Methods	336
Open Authentication	336
WEP	337
802.1x/EAP	338
LEAP	339
EAP-FAST	339
PEAP	340
EAP-TLS	340
Wireless Privacy and Integrity Methods	341
TKIP	341
CCMP	342
WPA and WPA2	342
Securing Management Frames with MFP	343
Configuring Wireless Security	344
Configuring WPA2 Personal	344
Configuring WPA2 Enterprise Mode	346
Configuring WPA2 Enterprise with Local EAP	348
Exam Preparation Tasks	351
Review All Key Topics	351
Define Key Terms	351
Chapter 15 Configuring a WLAN	353
“Do I Know This Already?” Quiz	353
Foundation Topics	355
WLAN Overview	355
Configuring a WLAN	356
Configuring a RADIUS Server	356
Creating a Dynamic Interface	358
Creating a New WLAN	360
Configuring WLAN Security	362
Configuring WLAN QoS	364
Configuring Advanced WLAN Settings	365
Finalizing WLAN Configuration	366

Exam Preparation Tasks 368

Review All Key Topics 368

Chapter 16 Implementing a Wireless Guest Network 371

“Do I Know This Already?” Quiz 371

Foundation Topics 374

Guest Network Overview 374

Scaling the Guest Network 375

Configuring a Guest Network 377

Exam Preparation Tasks 382

Review All Key Topics 382

Define Key Terms 382

Chapter 17 Configuring Client Connectivity 385

“Do I Know This Already?” Quiz 385

Foundation Topics 388

Configuring Common Wireless Clients 388

Considering Wireless Client Requirements 388

Understanding Windows Wi-Fi 389

Understanding Android Wi-Fi 395

Understanding MacOS X Wi-Fi 397

Understanding Apple iOS Wi-Fi 400

Cisco Compatibility Extensions 402

Exam Preparation Tasks 406

Review All Key Topics 406

Define Key Terms 406

Chapter 18 Managing Cisco Wireless Networks 409

“Do I Know This Already?” Quiz 409

Foundation Topics 412

Cisco Unified Access Overview 412

Using Prime Infrastructure 414

Alarms in the Dashboard 417

Monitoring a Wireless Network with Prime Infrastructure 419

Using Prime Infrastructure Maps 420

Configuring Devices with PI 426

Exam Preparation Tasks 427

Review All Key Topics 427

Chapter 19	Dealing with Wireless Interference	429
	“Do I Know This Already?” Quiz	429
	Foundation Topics	432
	Understanding Types of Interference	432
	Bluetooth	432
	ZigBee	433
	Cordless Phones	434
	Microwave Ovens	434
	WiMAX	434
	Other Devices	435
	Using Tools to Detect and Manage Interference	436
	Spectrum Analyzers	436
	Cisco CleanAir	439
	Enabling CleanAir	440
	Air-Quality Index	443
	Using Event-Driven RRM	445
	Exam Preparation Tasks	447
	Review All Key Topics	447
	Define Key Terms	447
Chapter 20	Troubleshooting WLAN Connectivity	449
	“Do I Know This Already?” Quiz	449
	Foundation Topics	453
	Troubleshooting Client Connectivity	453
	Troubleshooting Clients from PI	454
	Testing a Client from PI	459
	Troubleshooting Clients from the Controller	461
	Verifying Client WLAN Settings	462
	Viewing Controller Logs	463
	Troubleshooting AP Connectivity	464
	Verifying AP-to-WLC Connectivity	464
	Verifying AP-to-Network Connectivity	465
	Verifying the AP and Antenna Orientation	467
	Checking the RF Environment	468
	Exam Preparation Tasks	472
	Review All Key Topics	472

Chapter 21 Final Review 475

- Advice About the Exam Event 475
 - Learn the Question Types Using the Cisco Certification Exam Tutorial 475
 - Think About Your Time Budget 480
 - Other Pre-Exam Suggestions 481
- Exam Engine and Questions on the DVD 482
 - Install the Exam Engine 482
 - Activate and Download the Practice Exam 483
 - Activating Other Exams 483
 - Premium Edition 484
 - Using the Exam Engine 484
- The Cisco Learning Network 485
- Final Thoughts 485

Appendix A Answers to the “Do I Know This Already?” Quizzes 487

Appendix B Modulation and Coding Schemes 505

Appendix C CCNA Wireless 200-355 Exam Updates 513

- Always Get the Latest at the Companion Website 513
 - Technical Content 513

Key Terms Glossary 515




















Index 528

On the DVD

Appendix D Study Planner

Key Terms Glossary

Icons Used in This Book

Wireless Device 	Wireless Signal 	Wireless Access Point 	Lightweight Access Point 
Directional Antenna 	Wireless LAN Controller 	Wireless Bridge 	CAPWAP Tunnel 
Layer 2 Switch 	Multilayer Switch 	Wireless Client 	Mesh Access Point 
Mobility Services Engine 	Real Time Location Service 	Authentication Service 	Spectrum Analysis 
Wireless Cell 	AAA 	Server 	

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

Welcome to the world of Cisco Certified Network Associate (CCNA) Wireless! As technology continues to evolve, wireless technologies are finding their way to the forefront. This clearly indicates the progression from a fixed wired type of connectivity to a more fluid, mobile workforce that can work when, where, and how they want. Regardless of your background, one of the primary goals of the CCNA Wireless certification is to introduce you to the Cisco Unified Wireless Network (CUWN).

This book is designed to help you prepare for the Cisco CCNA Wireless 200-355 WIFUND (Implementing Cisco Wireless Networking Fundamentals) certification exam. To achieve the CCNA Wireless specialization, you must first pass the CCENT, CCNA Routing and Switching, or any CCIE certification.

Who Should Read This Book

Wireless networking is a complex business. The CCNA Wireless specialization was developed to introduce wireless LANs, the CUWN, and Cisco's wireless product line. The certification tests for proficiency in designing, installing, configuring, monitoring, and troubleshooting wireless networks in an enterprise setting.

How to Use This Book

The book consists of 21 chapters. Each chapter tends to build upon the chapter that precedes it. The chapters of the book cover the following topics:

- **Chapter 1, “RF Signals and Modulation”:** This chapter covers the basic theory behind radio frequency (RF) signals and the methods used to carry data wirelessly.
- **Chapter 2, “RF Standards”:** This chapter covers the agencies that regulate, standardize, and validate the correct use of wireless LAN devices.
- **Chapter 3, “RF Signals in the Real World”:** This chapter explores many of the conditions that can affect wireless signal propagation.
- **Chapter 4, “Understanding Antennas”:** This chapter explains some basic antenna theory, in addition to various types of antennas and their application.
- **Chapter 5, “Wireless LAN Topologies”:** This chapter explains the topologies that can be used to control access to the wireless medium and provide data exchange between devices.
- **Chapter 6, “Understanding 802.11 Frame Types”:** This chapter covers the frame format and frame types that APs and clients must use to communicate successfully. It also discusses the choreography that occurs between an AP and its clients.
- **Chapter 7, “Planning Coverage with Wireless APs”:** This chapter explains how wireless coverage can be adjusted to meet a need and how it can be grown to scale over a greater area and a greater number of clients. It also explains how coverage can be measured, surveyed, and validated.

- **Chapter 8, “Understanding Cisco Wireless Architectures”:** This chapter describes the autonomous, cloud-based, centralized, and converged wireless architectures and how you can leverage their respective strengths to solve some fundamental problems.
- **Chapter 9, “Implementing Autonomous and Cloud Deployments”:** This chapter discusses basic operation of an autonomous AP and how you can connect to it and convert it to lightweight mode, to become a part of a larger, more integrated wireless network. It also provides an introduction of Cisco Meraki cloud-based APs.
- **Chapter 10, “Implementing Controller-based Deployments”:** This chapter covers the wireless controller’s role in linking wired and wireless networks. It also covers the minimal initial configuration needed to get a controller up on the network where you can manage it more fully.
- **Chapter 11, “Understanding Controller Discovery”:** This chapter explains the process that each lightweight AP must go through to discover and bind itself with a controller before wireless clients can be supported.
- **Chapter 12, “Understanding Roaming”:** This chapter discusses client mobility from the AP and controller perspectives so that you can design and configure your wireless network properly as it grows over time.
- **Chapter 13, “Understanding RRM”:** This chapter covers Radio Resource Management (RRM), a flexible and automatic mechanism that Cisco wireless LAN controllers can use to make wireless network operation more efficient.
- **Chapter 14, “Wireless Security Fundamentals”:** This chapter covers many of the methods you can use to secure a wireless network.
- **Chapter 15, “Configuring a WLAN”:** This chapter explains how to define and tune a wireless LAN to support wireless clients and connectivity with a wired infrastructure.
- **Chapter 16, “Implementing a Wireless Guest Network”:** This chapter discusses the steps you can take to configure a guest network as an extension to your wireless infrastructure.
- **Chapter 17, “Configuring Client Connectivity”:** This chapter introduces some of the most common types of wireless clients and how to configure them to join a wireless LAN.
- **Chapter 18, “Managing Cisco Wireless Networks”:** This chapter provides an overview of Prime Infrastructure, how you can configure controllers and APs with it, and how you can use it to monitor a variety of things in your network.
- **Chapter 19, “Dealing with Wireless Interference”:** This chapter covers some common types of devices that can cause interference and the Cisco CleanAir features that can detect and react to the interference sources.

- **Chapter 20, “Troubleshooting WLAN Connectivity”:** This chapter helps you get some perspective about wireless problems, develop a troubleshooting strategy, and become comfortable using the tools at your disposal.
- **Chapter 21, “Final Review”:** This short chapter lists the exam preparation tools useful at this point in the study process. It also provides a suggested study plan now that you have completed all of the earlier chapters in this book.
- **Appendix A, “Answers to the ‘Do I Know This Already?’ Quizzes”:** This appendix provides the correct answers to the “Do I Know This Already?” quizzes that you will find at the beginning of each chapter. Brief explanations for the correct answers will also help you complete your understanding of topics covered.
- **Appendix B, “Modulation and Coding Schemes”:** This appendix outlines the direct-sequence spread spectrum (DSSS) and orthogonal frequency-division multiplexing (OFDM) data rates used for 802.11b/g and 802.11a; the modulation and coding schemes and data rates used for 802.11n; and the modulation, coding schemes, and data rates used for 802.11ac.
- **Appendix C, “CCNA Wireless 200-355 Exam Updates”:** This appendix is a living document that provides you with updated information if Cisco makes minor modifications to the exam upon which this book is based. Be sure to check the online version of this appendix at <http://www.ciscopress.com/title/9781587144578> for any updates.
- **Appendix D, “Study Planner”:** This spreadsheet is designed as a tool to help you plan and track major study milestones as you prepare for the CCNA Wireless exam.
- **Key Terms Glossary:** The glossary defines all WLAN-related terms that you were asked to define at the end of each chapter.

Each chapter follows the same format and incorporates the following tools to assist you by assessing your current knowledge and emphasizing specific areas of interest within the chapter:

- **Do I Already Know This Quiz?:** Each chapter begins with a quiz to help you assess your current knowledge of the subject. The quiz is divided into specific areas of emphasis that enable you to best determine where to focus your efforts when working through the chapter.
- **Foundation Topics:** The foundation topics are the core sections of each chapter. They focus on the specific protocols, concepts, or skills that you must master to successfully prepare for the examination.
- **Exam Preparation:** Near the end of each chapter, this section highlights the key topics from the chapter and the pages where you can find them for quick review. This section also provides a list of key terms that you should be able to define in preparation for the exam. It is unlikely that you will be able to successfully complete the certification exam by just studying the key topics and key terms, although they are a good tool for last-minute preparation just before taking the exam.

- DVD-based practice exam:** This book includes a DVD containing several interactive practice exams. It is recommended that you continue to test your knowledge and test-taking skills by using these exams. You will find that your test-taking skills will improve by continued exposure to the test format. Remember that the potential range of exam questions is limitless. Therefore, your goal should not be to “know” every possible answer but to have a sufficient understanding of the subject matter so that you can figure out the correct answer with the information provided.

Certification Exam Topics and This Book

The questions for each certification exam are a closely guarded secret. However, we do know which topics you must know to *successfully* complete this exam. Cisco publishes them as an exam blueprint for Implementing Cisco Wireless Networking Fundamentals (WIFUND), exam 200-355. 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 working with Cisco wireless LANs in the real world.

Tip At the time this book is being published, the WIFUND exam is based on Cisco Wireless LAN Controller software release 8.0 and Cisco Prime Infrastructure release 2.2.

Table I-1 WIFUND Exam 200-355 Topics and Chapter References

WIFUND 200-355 Exam Topic	Chapter(s) in Which Topic Is Covered
1.0 RF Fundamentals	
<i>1.1 Describe the propagation of radio waves</i>	
1.1.a Frequency, amplitude, phase, wavelength (characteristics)	1
1.1.b Absorption, reflection, diffraction, scattering, refraction, fading, free space path loss, multipath	3
<i>1.2 Interpret RF signal measurements</i>	
1.2.a Signal strength (RSSI, Transmit power, receive sensitivity)	1
1.2.b Differentiate interference vs. noise	1, 3, 19
1.2.c Device capabilities (smartphones, laptops, tablets)	17
1.2.d Define SNR	1
<i>1.3 Explain the principles of RF mathematics</i>	
1.3.a Compute dBm, mW, Law of 3s and 10s,	1
<i>1.4 Describe Wi-Fi antenna characteristics</i>	
1.4.a Ability to read a radiation pattern chart	4
1.4.b Antenna types and uses	4

WIFUND 200-355 Exam Topic	Chapter(s) in Which Topic Is Covered
1.4.c dBi, dBd, EIRP	1, 4
2.0 802.11 Technology Fundamentals	
<i>2.1 Describe basic Wi-Fi governance</i>	
2.1.a Describe regional regulatory bodies (such as, FCC / ETSI/ NTT)	2
2.1.b IEEE 802.11	2
2.1.c Wi-Fi Alliance	2
<i>2.2 Describe usable channel and power combination</i>	
2.2.a Regional EIRP limitation examples	2
2.2.b ISM, UNII frequency bands	2
2.2.c Describe RRM fundamental	13
<i>2.3 Describe 802.11 fundamentals</i>	
2.3.a Modulation techniques	1, 2
2.3.b Channel width	2
2.3.c MIMO / MU-MIMO	2
2.3.c (i) MRC	2
2.3.c (ii) Beam forming	2
2.3.c (iii) Spatial streams	2
2.3.d Wireless topologies	5
2.3.d (i) IBSS	5
2.3.d (ii) BSS	5
2.3.d (iii) ESS	5
2.3.e Frame types	6
2.3.e (i) Management	6
2.3.e (ii) Control	6
2.3.e (iii) Data	6
3.0 Implementing a Wireless Network	
<i>3.1 Describe the various Cisco wireless architectures</i>	
3.1.a Cloud	8
3.1.b Autonomous	8
3.1.c Split MAC	8

WIFUND 200-355 Exam Topic	Chapter(s) in Which Topic Is Covered
3.1.c (i) FlexConnect	8
3.1.c (ii) Centralized	8
3.1.c (iii) Converged	8
<i>3.2 Describe physical infrastructure connections</i>	
3.2.a Wired infrastructure (AP, WLC, access/trunk ports, LAG)	10
<i>3.3 Describe AP and WLC management access connections</i>	
3.3.a Management connections (Telnet, SSH, HTTP, HTTPS, console)	9, 10
3.3.b IP addressing: IPv4 / IPv6	9, 10
3.3.c Management via wireless	15
4.0 Operating a Wireless Network	
<i>4.1 Execute initial setup procedures Cisco wireless infrastructures</i>	
4.1.a Cloud	9
4.1.b Converged	10
4.1.c Centralized	10
4.1.d Autonomous	9
<i>4.2 Describe the Cisco implementation of the CAPWAP discovery and join process</i>	
4.2.a DHCP	11
4.2.b DNS	11
4.2.c Master-controller	11
4.2.d Primary-secondary-tertiary	11
<i>4.3 Distinguish different lightweight AP modes</i>	8
<i>4.4 Describe and configure the components of a wireless LAN access for client connectivity using GUI only</i>	15
<i>4.5 Identify wireless network and client management and configuration platform options</i>	
4.5.a Controller GUI and CLI	10
4.5.b Prime infrastructure	18
4.5.c Dashboard	9
4.5.d ISE	18
<i>4.6 Maintain wireless network</i>	

WIFUND 200-355 Exam Topic	Chapter(s) in Which Topic Is Covered
4.6.a Perform controller configuration backups	10
4.6.b Perform code updates on controller, APs, and converged access switches	10
4.6.b (i) AireOS: boot loader (FUS), image	10
4.6.b (ii) IOS-XE: bundle, unbundle	10
4.6.b (iii) Autonomous	9
5.0 Configuration of Client Connectivity	
<i>5.1 Identify authentication mechanisms</i>	
5.1.a LDAP, RADIUS, local authentication, WebAuth, 802.1X, PSK	14, 16
<i>5.2 Configuring WLAN authentication mechanisms on the controller</i>	
5.2.a WebAuth, 802.1X, PSK	14, 16
5.2.b TKIP deprecation	14
<i>5.3 Configure client connectivity in different operating systems</i>	
5.3.a Android, MacOS, iOS, Windows	17
<i>5.4 Describe roaming</i>	
5.4.a Layer 2 and Layer 3	12
5.4.b Intracontroller and intercontroller	12
5.4.c Centralized mobility	12
5.4.d Converged mobility	12
<i>5.5 Describe wireless guest networking</i>	
5.5.a Anchor controller	16
5.5.b Foreign controller	16
6.0 Performing Client Connectivity Troubleshooting	
<i>6.1 Validating WLAN configuration settings at the infrastructure side</i>	
6.1.a Security settings	20
6.1.b SSID settings	20
<i>6.2 Validating AP infrastructure settings</i>	
6.2.a Port level configuration	20
6.2.b Power source	20
6.2.c AP and antenna orientation and position	20

WIFUND 200-355 Exam Topic	Chapter(s) in Which Topic Is Covered
6.3 Validate client settings	
6.3.a SSID	17, 20
6.3.b Security	17, 20
6.3.c Device driver version	17
6.4 <i>Employ appropriate controller tools to assist troubleshooting</i>	
6.4.a GUI logs	20
6.4.b CLI show commands	20
6.4.c Monitor pages	
6.4.c (i) CleanAir (controller GUI)	19
6.5 <i>Identify appropriate third-party tools to assist troubleshooting</i>	
6.5.a OS-based Client utilities	20
6.5.b Wi-Fi scanners	20
6.5.c RF mapping tool	20
7.0 Site Survey Process	
7.1 <i>Describe site survey methodologies and their purpose</i>	
7.1.a Offsite (predictive / plan)	7
7.1.b Onsite	7
7.1.b (i) Predeployment (AP on a stick)	7
7.1.b (ii) Post deployment (validation)	7
7.2 <i>Describe passive and active site surveys</i>	7
7.3 <i>Identify proper application of site survey tools</i>	
7.3.a Spectrum analyzer	19
7.3.b Site surveying software	7
7.4 <i>Describe the requirements of client real-time and non-real-time applications</i>	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 wireless networking professional.

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 that you need more detailed information on a specific topic, read the Cisco documentation that focuses on that topic.

Note that as wireless technologies continue to develop, 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 that 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, hovering over Training & Events, and 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 <http://www.ciscopress.com/title/9781587144578>. 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.

Taking the CCNA Wireless Certification Exam

As with any Cisco certification exam, you should strive to be thoroughly prepared before taking the exam. There is no way to determine exactly what questions are on the exam, so the best way to prepare is to have a good working knowledge of all subjects covered on the exam. Schedule yourself for the exam and be sure to be rested and ready to focus when taking the exam.

The best place to find out the latest available Cisco training and certifications is under the Training & Events section at Cisco.com.

Tracking Your Status

You can track your certification progress by checking <http://www.cisco.com/go/certifications/login>. You must create an account the first time you log in to the site.

How to Prepare for an Exam

The best way to prepare for any certification exam is to use a combination of the preparation resources, labs, and practice tests. This guide has integrated some practice questions and example scenarios to help you better prepare. If possible, get some hands-on experience with CUWN equipment. There is no substitute for real-world experience; it is much easier to understand the designs, configurations, and concepts when you can actually work with a live wireless network.

Cisco.com provides a wealth of information about wireless LAN controllers, access points (APs), and wireless management products, and wireless LAN technologies and features.

Assessing Exam Readiness

Exam candidates never really know whether they are adequately prepared for the exam until they have completed about 30 percent of the questions. At that point, if you are not prepared, it is too late. The best way to determine your readiness is to work through the “Do I Know This Already?” quizzes at the beginning of each chapter and review the foundation and key topics presented in each chapter. It is best to work your way through the entire book unless you can complete each subject without having to do any research or look up any answers.

Cisco Wireless Certifications in the Real World

Cisco has one of the most recognized names on the Internet. Cisco Certified wireless specialists can bring quite a bit of knowledge to the table because of their deep understanding of wireless technologies, standards, and networking devices. This is why the Cisco certification carries such high respect in the marketplace. Cisco certifications demonstrate to potential employers and contract holders a certain professionalism, expertise, and dedication required to complete a difficult goal. If Cisco certifications were easy to obtain, everyone would have them.

Exam Registration

The CCNA Wireless WIFUND 200-355 exam is a computer-based exam, with around 60 to 70 multiple-choice, fill-in-the-blank, list-in-order, and simulation-based questions. You can take the exam at any Pearson VUE (<http://www.pearsonvue.com>) testing center. According to Cisco, the exam should last about 90 minutes. Be aware that when you register for the exam, you might be told to allow a certain amount of time to take the exam that is longer than the testing time indicated by the testing software when you begin. This discrepancy is because the testing center will want you to allow for some time to get settled and take the tutorial about the test engine.

Book Content Updates

Because Cisco occasionally updates exam topics without notice, Cisco Press might post additional preparatory content on the web page associated with this book at <http://www.ciscopress.com/title/9781587144578>. It is a good idea to check the website a couple of weeks before taking your exam, to review any updated content that might be posted online. We also recommend that you periodically check back to this page on the Cisco Press website to view any errata or supporting book files that may be available.



This chapter covers the following topics:

- **Configuring 802.11 Support**—This section explains how to configure the data rates in the 2.4- and 5-GHz bands and support for 802.11n high throughput (HT) and 802.11ac very high throughput (VHT) functionality.
- **Understanding RRM**—This section describes the algorithms that can monitor and adjust radio frequency parameters automatically in a wireless network.

This chapter covers the following exam topics:

- 2.2—Describe usable channel and power combination
 - 2.2c—Describe RRM fundamentals

Understanding RRM

In Chapter 7, “Planning Coverage with Wireless APs,” you learned how to size access point (AP) cells appropriately by disabling data rates and changing the transmit power levels. You also learned how important a proper channel layout is to promote efficient roaming and minimize co-channel interference. You probably also realized how difficult these tasks are when you have to tune the radio frequency (RF) parameters manually across a large number of APs.

In this chapter, you learn about Cisco Radio Resource Management (RRM), a flexible and automatic mechanism that Cisco Wireless LAN controllers can use to make your life much easier.

“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 13-1 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 13-1 “Do I Know This Already?” Section-to-Question Mapping

Foundation Topics Section	Questions
Configuring 802.11 Support	1–4
Understanding RRM	5–10

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.

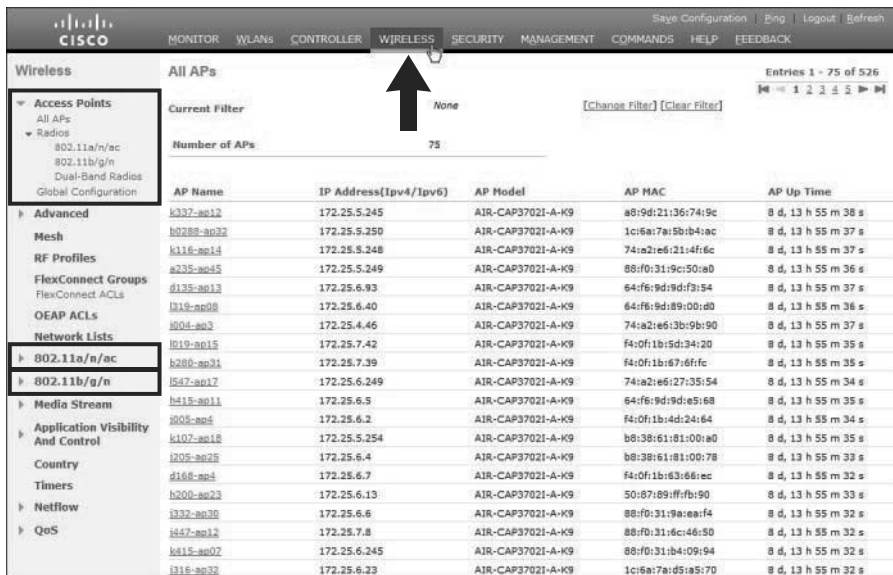
1. Which one of the following correctly describes a mandatory data rate?
 - a. A data rate that must be used by wireless clients all the time
 - b. The highest data rate used by an AP and its clients
 - c. A data rate that must be supported by a client before it can associate with an AP
 - d. A data rate required by the IEEE 802.11 standards body
2. You can configure only one data rate as mandatory on an AP. True or false?
 - a. True
 - b. False
3. An AP sends 802.11 broadcast management frames at which one of the following data rates?
 - a. The highest mandatory data rate
 - b. The lowest mandatory data rate
 - c. The lowest supported data rate
 - d. All supported data rates
4. Which one of the following is the default state of 802.11n and 802.11ac support and the default channel width on a Cisco wireless LAN controller?
 - a. Disabled; 20-MHz channels
 - b. Enabled; 20-MHz channels
 - c. Enabled; 40-MHz channels
 - d. Disabled; 40-MHz channels
 - e. Enabled; 80-MHz channels
5. Which one of the following correctly identifies the scope of the RRM algorithms?
 - a. All APs joined to one controller
 - b. All APs joined to all controllers
 - c. All APs joined to controllers in an RF group
 - d. All APs of a specific model
6. An RF group is automatically formed by which one of the following?
 - a. All APs that share the same channel
 - b. All clients that share the same SSID
 - c. Any controllers that can overhear neighbor messages with identical RF group names sent between their APs
 - d. All controllers that can overhear neighbor messages with identical mobility group names sent between their APs

7. The TPC algorithm is used for which one of the following purposes?
 - a. To adjust the transmission control protocol rate
 - b. To detect problems in transmission perimeter coverage
 - c. To adjust the transmitting primary channel
 - d. To adjust the transmit power level
8. If the DCA algorithm detects that an AP is experiencing interference or excessive noise, what might it do to mitigate the problem?
 - a. Increase the AP's transmit power level
 - b. Decrease the AP's transmit power level
 - c. Change the AP's channel number
 - d. Direct the client to a different band
9. Which one of the following runs the DCA algorithm?
 - a. RF group leader
 - b. Master controller
 - c. Each controller
 - d. NCS or Cisco Prime Infrastructure
10. The 5-GHz radio in one of several APs in a building has failed. Which one of the following algorithms should be able to detect the failure?
 - a. CCA
 - b. DCA
 - c. Dead radio detection
 - d. Coverage hole detection

Foundation Topics

Configuring 802.11 Support

Cisco controllers and most APs can support wireless LANs in both the 2.4- and 5-GHz bands. By default, both bands are enabled; however, you can view or change a number of parameters by browsing to the Wireless tab in the controller, shown in Figure 13-1.



AP Name	IP Address(Ipv4/Ipv6)	AP Model	AP MAC	AP Up Time
k337-ao12	172.25.5.245	AIR-CAP37021-A-K9	a8:9d:21:36:74:9c	8 d, 13 h 55 m 38 s
k028-ao22	172.25.5.250	AIR-CAP37021-A-K9	1c:6a:7a:5b:b4:ac	8 d, 13 h 55 m 37 s
k116-ao14	172.25.5.248	AIR-CAP37021-A-K9	74:a2:e6:21:4f:6c	8 d, 13 h 55 m 37 s
a235-ao45	172.25.5.249	AIR-CAP37021-A-K9	88:f0:31:9c:50:a0	8 d, 13 h 55 m 36 s
d133-ao13	172.25.6.93	AIR-CAP37021-A-K9	64:f6:9d:9d:f3:54	8 d, 13 h 55 m 37 s
019-ao08	172.25.6.40	AIR-CAP37021-A-K9	64:f6:9d:89:00:d0	8 d, 13 h 55 m 36 s
004-ao3	172.25.4.46	AIR-CAP37021-A-K9	74:a2:e6:3b:9b:90	8 d, 13 h 55 m 37 s
019-ao15	172.25.7.42	AIR-CAP37021-A-K9	f4:0f:1b:5d:34:20	8 d, 13 h 55 m 35 s
k280-ao31	172.25.7.39	AIR-CAP37021-A-K9	f4:0f:1b:87:6f:fc	8 d, 13 h 55 m 35 s
047-ao17	172.25.6.249	AIR-CAP37021-A-K9	74:a2:e6:27:35:54	8 d, 13 h 55 m 34 s
k416-ao11	172.25.6.5	AIR-CAP37021-A-K9	64:f6:9d:9d:e5:68	8 d, 13 h 55 m 35 s
005-ao4	172.25.6.2	AIR-CAP37021-A-K9	f4:0f:1b:4d:24:64	8 d, 13 h 55 m 34 s
k107-ao18	172.25.5.254	AIR-CAP37021-A-K9	b8:38:61:81:00:a0	8 d, 13 h 55 m 35 s
009-ao25	172.25.6.4	AIR-CAP37021-A-K9	b8:38:61:81:00:78	8 d, 13 h 55 m 33 s
d168-ao4	172.25.6.7	AIR-CAP37021-A-K9	f4:0f:1b:83:86:ec	8 d, 13 h 55 m 32 s
k200-ao23	172.25.6.13	AIR-CAP37021-A-K9	50:87:89:ff:fb:90	8 d, 13 h 55 m 33 s
032-ao30	172.25.6.6	AIR-CAP37021-A-K9	88:f0:31:9a:eaf:4	8 d, 13 h 55 m 32 s
047-ao13	172.25.7.8	AIR-CAP37021-A-K9	88:f0:31:6c:46:50	8 d, 13 h 55 m 32 s
k415-ao07	172.25.6.245	AIR-CAP37021-A-K9	88:f0:31:b4:09:94	8 d, 13 h 55 m 32 s
016-ao32	172.25.6.23	AIR-CAP37021-A-K9	1c:6a:7a:d5:a5:70	8 d, 13 h 55 m 32 s

Figure 13-1 Wireless Tab on a Cisco Controller GUI

The wireless parameters are organized under a list of links that are found on the left side of the web page. At the CCNA level, you should be familiar with the following links:

- **Access Points**—Used to verify and configure RF things like transmit power level and channel number on individual APs
- **802.11a/n/ac**—Used to configure global parameters for the 5-GHz band
- **802.11b/g/n**—Used to configure global parameters for the 2.4-GHz band

The initial web page displays a list of all APs that are currently joined to the controller, as if you had selected **Wireless > Access Points > All APs**. The remaining configuration is covered in the sections that follow.

Configuring Data Rates

You can enable or disable the 2.4- or 5-GHz bands by selecting **802.11b/g/n** or **802.11a/n/ac**, respectively, and then clicking the **Network** link. Figures 13-2 and 13-3 show the two network configuration pages. Make sure that the **802.11b/g** or **802.11a Network Status** check box is checked to enable the 2.4- or 5-GHz radios on all APs.

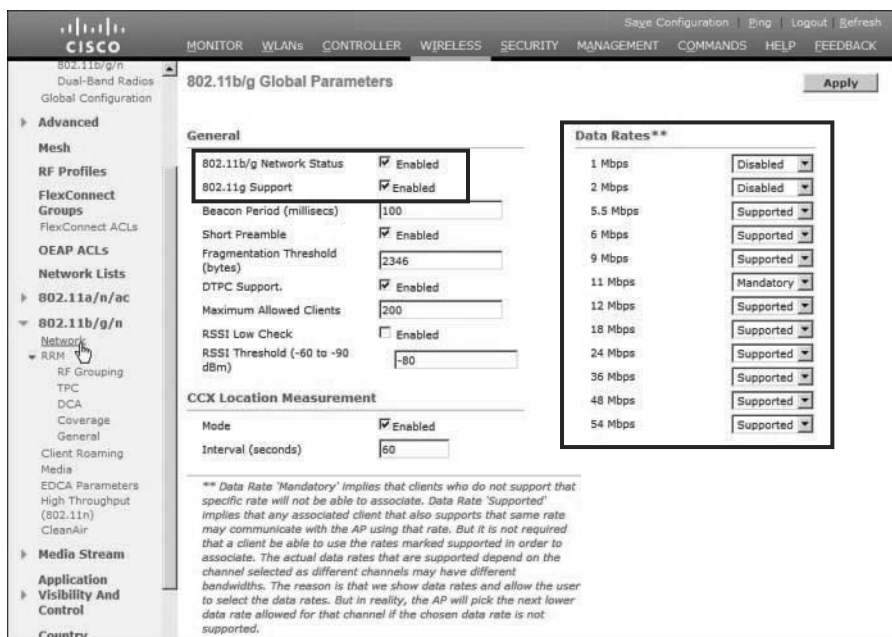


Figure 13-2 Configuring 2.4-GHz Radios

On the right side of the network web pages, as shown in Figures 13-2 and 13-3, you can configure the individual data rates (and the corresponding modulation and coding schemes) that are supported on each band. Each data rate can have one of the following states:

Key Topic

- **Mandatory**—A client must be able to use the data rate and Modulation Coding Scheme (MCS) to associate with an AP.
- **Supported**—A client can associate with an AP even if it cannot use the data rate.
- **Disabled**—An AP will not use the data rate with any clients.

By default, all data rates are enabled and supported. In the 2.4-GHz band, the 1-, 2-, 5.5-, and 11-Mbps rates are all marked as mandatory, based on the initial IEEE requirement that all clients be able to support each possible modulation type defined in 802.11b. In the 5-GHz band, the 6-, 12-, and 24-Mbps rates are marked as mandatory.

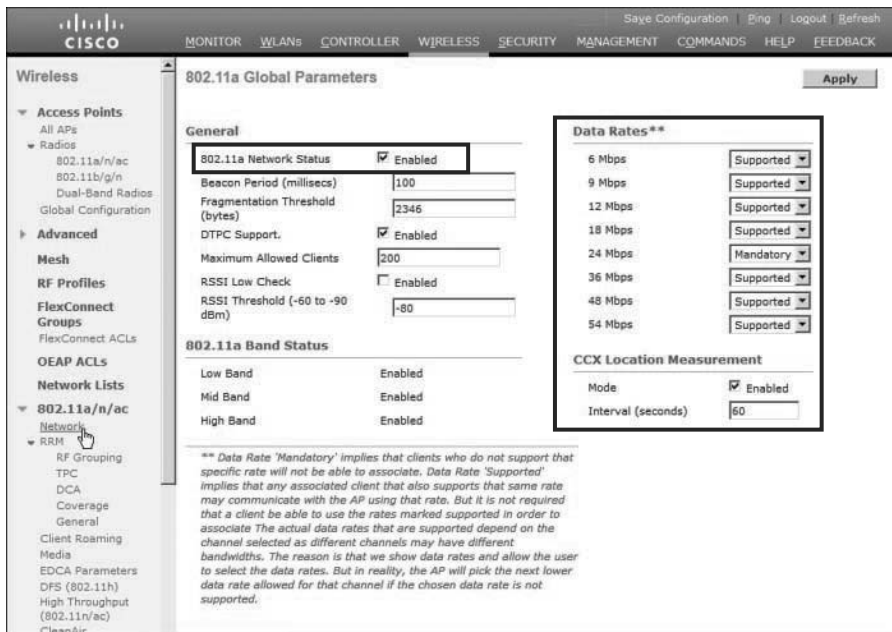


Figure 13-3 Configuring 5-GHz Radios

You can change the state of any data rate by selecting a new state from the drop-down menu. Remember that you can disable lower data rates to decrease the AP cell size and make channel use more efficient. Just make sure that your actions do not shrink the cells too much, leaving holes or gaps in the coverage between APs. Also be sure that all of your wireless clients can use the same set of mandatory and supported data rates.

Be sure to click the **Apply** button to make any configuration changes active. Any wireless networks that are already in production on the controller might be disrupted while the new configuration takes effect.

Configuring 802.11n and 802.11ac Support

You might have noticed that you can configure plenty of data rates, but 802.11n and 802.11ac are never mentioned on the wireless network configuration pages. That is because 802.11n and 802.11ac are considered to be rich sets of high-throughput enhancements and must be configured separately.

By default, 802.11n and 802.11ac are enabled. To check or change their state, go to **Wireless > 802.11a/n/ac** or **802.11b/g/n > High Throughput (802.11n/ac)**. Figure 13-4 shows the 5-GHz 802.11n/ac configuration page. Check the **11n Mode** and **11ac Mode** check boxes to enable 802.11n and 802.11ac, respectively. By default, every possible MCS is enabled and supported.

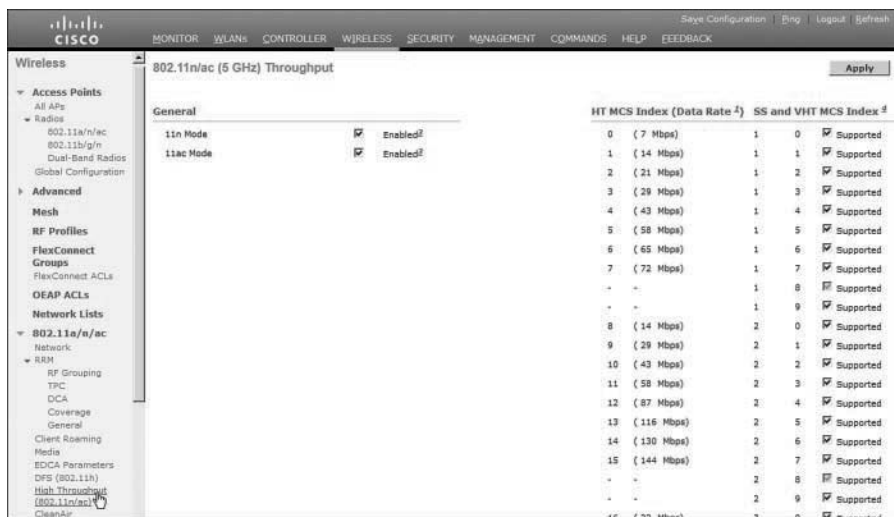


Figure 13-4 Configuring 802.11n and 802.11ac Support

Recall that 802.11n can bond one 20-MHz channel to an adjacent 20-MHz channel to effectively double the channel width; 802.11ac can scale even further. By default, the controller will use only a single 20-MHz channel on each AP. You can configure channel bonding as a part of the dynamic channel allocation (DCA) configuration for the 5-GHz band only, as covered in the following section.

Understanding RRM

Suppose that you need to provide wireless coverage in a rectangular-shaped building. Using the information you have learned from this book, you decide to use six APs and locate them such that they form a staggered, regular pattern. The pattern shown in Figure 13-5 should create optimum conditions for roaming and channel use. (The building dimensions have not been mentioned, just to keep things simple.)

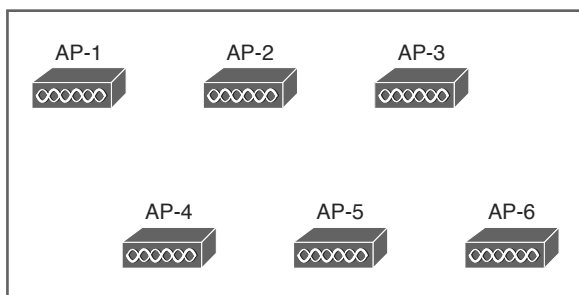


Figure 13-5 Hypothetical AP Layout

So far, you have considered the layout pattern and an average cell size, but you still have to tackle the puzzle of selecting the transmit power level and channel number for each AP. The transmit power level will affect the final cell size, and the channel assignment will affect co-channel interference and roaming handoff. At this point, if all the APs are powered up, they might all end up transmitting at maximum power on the same channel. Figure 13-6 shows one possible scenario; each of the AP cells overlaps its neighbors by about 50 percent, and all the APs are fighting to use channel 1!

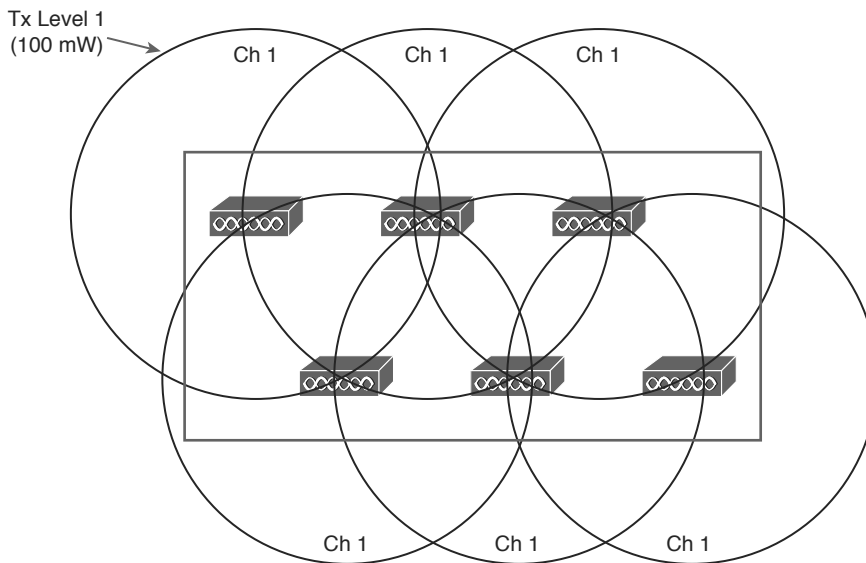


Figure 13-6 *Poorly Configured RF Coverage*

Where do you begin to prevent such mayhem? Because the AP locations are already nailed down, you can figure out the transmit power level that will give the proper cell overlap. Then you can work your way through the AP layout and choose an alternating pattern of channel numbers. With six APs, that might not be a daunting task.

Do not forget to repeat the task for both 2.4- and 5-GHz bands.

Also, if you plan on using 802.11n or 802.11ac with channel widths greater than 20 MHz, do not forget to reserve the extra channels needed for that. Be aware that only the 5-GHz band is capable of supporting wide channels.

If you happen to notice that an AP fails one day, you could always reconfigure its neighboring APs to increase their transmit power level to expand their cells and cover the hole.

If you introduce another AP or two in the future, do not forget to revisit the entire configuration again to make room for cells and channels.

Did your life as the wireless LAN administrator just become depressing and tedious? Cisco Radio Resource Management (RRM) can handle all these tasks regularly and automatically. RRM consists of several algorithms that can look at a large portion of a wireless network and work out an optimum transmit power level and channel number for each AP. If conditions that affect the RF coverage change over time, RRM can detect that and make the appropriate adjustments.

RF Groups

RRM works by monitoring a number of APs and working out optimal RF settings for each one. The APs that are included in the RRM algorithms are contained in a single RF group. An RF group is formed for each band that is supported—one group for 2.4-GHz AP radios and another for 5-GHz AP radios. By default, an RF group contains all the APs that are joined to a single controller.

You can also configure a controller to automatically populate its RF group. In that case, the RF group can expand to include APs from multiple controllers, provided the following two conditions are met:

- The controllers share a common RF group name.
- At least one AP from one controller can be overheard by an AP on another controller.

When an RF group touches more than one controller, the controllers form a type of cluster so that they all participate in any RF adjustments that are needed. Every AP sends a Neighbor Discovery Packet (NDP) at maximum transmit power and at 60-second intervals, by default. If two controllers are close enough in proximity for an AP on one to hear an AP on the other at a received signal strength indicator (RSSI) of -80 dBm or greater, they are close enough to belong to the same RF group. Up to 20 controllers and 1000 APs can join to form a single RF group.

Figure 13-7 shows a simple scenario with four controllers and four APs, resulting in two separate RF groups. AP-1 and AP-2 are both joined to controller WLC-1, so they are members of one RF group by default. AP-3, joined to WLC-2, is located near enough to AP-1 and AP-2 that neighbor advertisements are overheard. As a result, controller WLC-2 joins the RF group with WLC-1. However, AP-4, joined to controller WLC-3, is not close enough to pass the neighbor test. Even though AP-4's cell intersects the cells of AP-2 and AP-3, the APs themselves are not within range. Therefore, controller WLC-3 resides in a different RF group by itself.

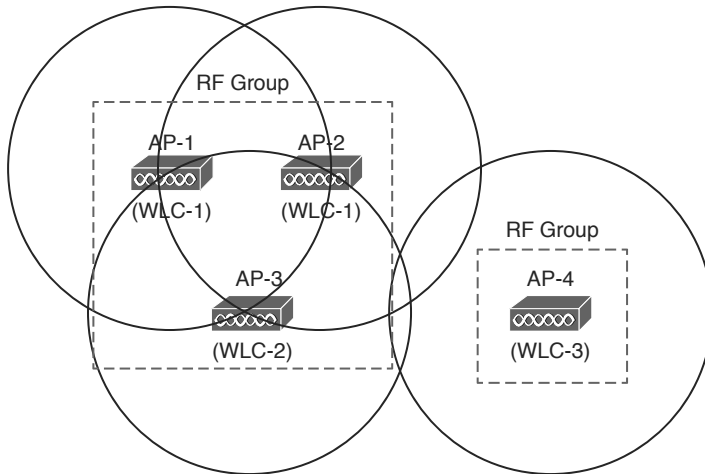
Key
Topic

Figure 13-7 Automatic RF Group Discovery and Formation

One controller in each group is elected as an RF group leader, although you can override that by configuring one controller as a static leader. The leader collects and analyzes information from all APs in the group about their RF conditions in real time. You can access the RF group leader configuration information by selecting **Wireless > 802.11a/n/ac** or **802.11b/g/n > RRM > RF Grouping**. In Figure 13-8, the controller is in automatic RF group mode and is a member of an RF group along with two other controllers. The RF group leader is controller WLC-1.

The screenshot shows the Cisco WMC interface for configuring RF Grouping. The left sidebar shows the navigation tree with '802.11a/n/ac' selected. The main content area displays the 'RF Grouping Algorithm' configuration for the 'MedicalCenter' group. The 'Group Mode' is set to 'auto' and the 'Group Leader' is WLC-1 with IP address 192.168.200.6. The 'RF Group Members' table lists the controllers in the group.

Controller Name	IP Address(Ipv4/Ipv6)
WLC-2	192.168.200.15
WLC-3	192.168.200.16
WLC-1	192.168.200.6

Figure 13-8 Displaying RF Group Information

Radio resource monitoring is used to gather and report information from the APs. Each AP is assigned to transmit and receive on a single channel, so it can easily detect noise and interference on that channel, as well as the channel utilization. The AP can also keep a list of clients and other APs that it hears transmitting on that channel.

Each AP can also spend a short bit of time (less than 60 ms) tuning its receiver to all of the other channels that are available. By scanning channels other than the one normally used, an AP can measure noise and interference all across the band from its own vantage point. The AP can also detect unexpected transmissions coming from rogue clients and APs, or devices that are not formally joined to the Cisco wireless network.

Based on the radio resource monitoring data, RRM can make the following decisions about APs in an RF group:

- **Transmit power control (TPC)**—RRM can set the transmit power level of each AP.
- **Dynamic channel allocation (DCA)**—RRM can select the channel number for each AP.
- **Coverage hole detection mitigation (CHDM)**—Based on information gathered from client associations, RRM can detect an area with weak RF coverage and increase an AP's transmit power level to compensate.

The RRM algorithms are designed to keep the entire wireless network as stable and efficient as possible. The TPC and DCA algorithms run independently because they perform very different functions. By default, the algorithms are run every 600 seconds (10 minutes). If conditions in the RF environment change, such as interference or the addition or failure of an AP, RRM can discover and react to the changes at the next interval. The RRM algorithms are discussed in more detail in the following sections.

TPC

The TPC algorithm focuses on one goal: setting each AP's transmit power level to an appropriate value so that it offers good coverage for clients while avoiding interference with neighboring APs that are using the same channel. Figure 13-9 illustrates this process. APs that were once transmitting too strongly and overlapping each other's cells are adjusted for proper coverage, reducing the cell size more appropriately to support clients.

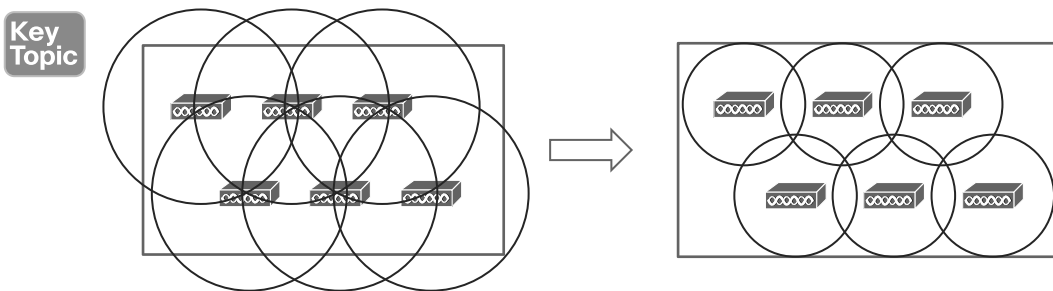


Figure 13-9 Basic Concept of the TPC Algorithm

Controllers have no knowledge of the physical location of each AP. By looking at Figure 13-9, you can see that the APs are arranged in a nice, evenly spaced pattern,

but the controller cannot see that. When an AP joins a controller, only the AP's MAC address, IP address, and some basic information are advertised to the controller. If the locations of neighboring APs cannot be known, each AP must resort to using the RSSI of its neighbors as a measure of how closely their cells touch or overlap its own.

During the time each AP scans the channels to listen for RF conditions and other APs, it forms a list of its neighbors and their RSSI values. Each of those lists is sent to the local controller and on to the RF group leader where they are used by the TPC algorithm.

TPC works on one band at a time, making adjustments to APs as needed. If an AP has been heard with an RSSI above a threshold (-70 dBm by default) by at least three of its neighbors, TPC considers the AP's cell to be overlapping the cells of its three neighbors too much. The AP's transmit power level will be decreased by 3 dB, and then its RSSI will be evaluated again. This process is repeated for all APs at regular intervals until the neighbor that is measuring the third-strongest RSSI value for the AP no longer measures the RSSI greater than the threshold.

Although you probably will not have to make any configuration changes for the TPC algorithm, it is still useful to understand its settings. TPC runs on the 2.4- and 5-GHz bands independently. You can see the settings by selecting **Wireless > 802.11a/n/ac** or **802.11b/g/n > RRM > TPC**. Figure 13-10 shows the TPC configuration for the 5-GHz band.

The screenshot displays the Cisco Wireless configuration interface for the 802.11a/n/ac band, specifically the Tx Power Control (TPC) settings. The left sidebar shows the navigation tree with 'TPC' selected under 'RRM'. The main content area is titled '802.11a > RRM > Tx Power Control(TPC)'. It includes the following configuration details:

- TPC Version:**
 - Interference Optimal Mode (TPCv2)
 - Coverage Optimal Mode (TPCv1)
- Tx Power Level Assignment Algorithm:**
 - Power Level Assignment Method: Automatic (Every 600 secs), On Demand (Invoke Power Update Once), Fixed (1)
 - Maximum Power Level Assignment (-10 to 30 dBm): 30
 - Minimum Power Level Assignment (-10 to 30 dBm): -10
 - Power Assignment Leader: pcf-wism-e-m4-c1 (172.22.253.15)
 - Last Power Level Assignment: 134 secs ago
 - Power Threshold (-80 to -50 dBm): -70
 - Power Neighbor Count: 3

Figure 13-10 *Adjusting the RRM TPC Algorithm Parameters*

Actually, there are two different TPC algorithms as you can see in the figure. TPCv1 (the default), also known as Coverage Optimal Mode, works toward making adjustments that give the best RF coverage, while keeping signals sufficient and stable. TPCv2, also known as Interference Optimal Mode, focuses on avoiding negative impacts that TPCv1 might have had, where the power among AP cells ends up being imbalanced, causing some cells to interfere with others. TPCv2 requires proper tuning of RF parameters in order to work

properly. While TPCv2 might sound superior, it should only be enabled in specific cases that are outside the scope of the CCNA Wireless exam or when directed by Cisco TAC.

By default, TPC runs automatically every 10 minutes. This is the recommended mode because any changes in the RF environment can be detected and compensated for without any intervention. As an alternative, you can select **On Demand** to run the algorithm immediately; then the resulting transmit power levels will be frozen until TPC is manually triggered again. If you would rather have the controller set the transmit power level on all APs to one fixed value, you can select **Fixed** and choose the power level from the drop-down menu.

Cisco controllers determine the transmit power level according to an index from 1 to 8, rather than discrete dBm or mW values. A value of 1 corresponds to the maximum power level that is allowed in the AP's regulatory domain. Each increment in the power level number reduces the transmit power by 3 dBm. You might remember from Chapter 1 that reducing by 3 dBm also means that the power in mW is cut in half. As an example, Table 13-2 lists the power levels used in the 2.4-GHz and 5-GHz bands on a Cisco 3700 AP in the Americas or European domains.

**Key
Topic**

Table 13-2 AP Transmit Power Level Numbers, dBm, and mW Values in the 2.4-GHz Band

Power Level	dBm (2.4 GHz)	dBm (5 GHz)	mW
1	23	23	200
2	20	20	100
3	17	17	50
4	14	14	25
5	11	11	12.5
6	8	8	6.25
7	5	Unused	3.125
8	2	Unused	1.56

With every iteration, the TPC algorithm can continue adjusting the transmit power levels until no further changes are needed. As a result, some APs might end up higher or lower than you might want. For example, it is usually best to match the AP transmit power level with that of the clients. Suppose that some of the clients have a fixed power level of 25 mW; if TPC ends up reducing some APs to 10 mW, the AP and client power levels will be mismatched.

To prevent such a condition, you can set minimum and maximum power level boundaries for the TPC algorithm. By default, the minimum level is set to -10 dBm and the maximum to 30 dBm, as shown in Figure 13-10.

Whenever you change the TPC parameters in a controller configuration, remember to make the same changes to all controllers that might be members of the same RF group. No matter which controller might become the RF group leader, the parameters should be identical.

Tip What transmit power level does an AP use when it first powers up? A new AP right out of the box will power up at its maximum power level. After the TPC algorithm has run and adjusted an AP's power level, that level is remembered the next time the AP is power cycled.

DCA

Recall from Chapter 7, “Planning Coverage with Wireless APs,” and Chapter 12, “Understanding Roaming,” that a proper channel assignment is vital for efficient use of air time and for client mobility. When neighboring APs use the same channel, they can interfere with each other. Ideally, adjacent APs should use different, non-overlapping channels. Working out a channel layout for many APs can be a difficult puzzle, but the DCA algorithm can work out optimum solutions automatically for all APs in an RF group.

When a new AP first powers up, it uses the first non-overlapping channel in each band—channel 1 for 2.4 GHz and channel 36 for 5 GHz. Consider a simplistic scenario where all APs are new and powered up for the first time. You would end up with a building full of overlapping cells competing for the use of 2.4-GHz channel 1, as shown in simplified form in Figure 13-11. The DCA algorithm works to correct this situation by finding a channel that each AP in the RF group can use without overlapping or interfering with other APs. Like TPC, DCA works out one channel layout in the 2.4-GHz band and another layout in the 5-GHz band.

Key Topic

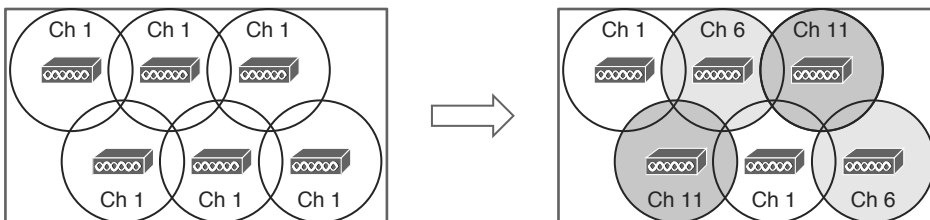


Figure 13-11 Basic Concept of the DCA Algorithm

DCA does not just solve the channel layout puzzle once for all APs. The algorithm runs every 10 minutes by default, so that it can detect any conditions that might require an AP's channel to change. APs in the RF group are monitored for the metrics listed in Table 13-3 that can influence the channel reassignment decision.

Table 13-3 Metrics Affecting DCA Decisions

Metric	Default State	Description
RSSI of neighboring APs	Always enabled	If DCA detects co-channel interference, it may move an AP to a different channel.
802.11 interference	Enabled	If transmissions from APs and devices that are not part of the wireless network are detected, DCA may choose to move an AP to a different channel.

Metric	Default State	Description
Non-802.11 noise	Enabled	If excessive noise is present on a channel, DCA may choose to avoid using it.
AP traffic load	Disabled	If an AP is heavily used, DCA may not change its channel to keep client disruption to a minimum.
Persistent interference	Disabled	If an interference source with a high duty cycle is detected on a channel, DCA may choose to avoid using it.

The DCA algorithm tends to look at each AP individually to find the ones with the worst RF conditions. Changing the channel of even one AP can affect many other APs if there are not other alternative channels available. Channel layout is a puzzle that may require several iterations to solve. For this reason, the controller that is the RF group leader will undergo an RRM startup mode after it is elected. The startup mode consists of ten DCA iterations at 10-minute intervals, or a total of 100 minutes before the channel layout reaches a steady state.

The end result of DCA is a channel layout that takes a variety of conditions into account. The channel layout is not just limited to the two dimensions of a single floor space in a building; it also extends to three-dimensional space because the RF signals from one floor can bleed through to another. As long as the APs on different floors belong to the same RF group, co-channel interference between them should be minimized.

You can display and configure the DCA parameters of either the 2.4- or 5-GHz band by selecting **Wireless > 802.11a/n/ac** or **802.11b/g/n > RRM > DCA**. Figure 13-12 shows the 802.11a/n/ac configuration.

By default, the DCA algorithm runs automatically at 10-minute intervals. You can change the interval time, select **Freeze** to run DCA manually on demand, or turn it **Off** completely. You can also select the conditions to avoid, which will trigger a channel change on an AP.

The DCA parameters also include the 802.11n channel width. By default, 20-MHz channels will be used. If you have enabled 802.11n in the 5-GHz band and want to enable 40-MHz channels, be sure to select **40 MHz** as the channel width. If you have 802.11ac enabled, you can choose between 20-, 40-, and 80-MHz channel width. The DCA algorithm will solve the channel assignment puzzle automatically, even with wide channels.

Tip You might be wondering why 802.11ac can support 80- and 160-MHz channel widths, but 160 MHz is not an option on the controller depicted in Figure 13-12. The reason is twofold: (1) Full 160-MHz channel width is not supported until 802.11ac Wave 2; and (2) the CCNA Wireless 200-355 exam uses AireOS 8.0, which supports only Wave 1. In addition, the available spectrum does not currently support more than two 160-MHz channels. Both reasons will be solved over time, as new hardware is developed and as new spectrum is reclaimed and set aside in the 5-GHz band.

The bottom portion of the web page contains a list of channels that DCA can use as it assigns channels to APs in the respective band. This list is populated with channel numbers by default, but you can edit the list as needed. You can also enable or disable individual channel use by using the list of **Select** check boxes.

The DCA algorithm normally runs on an automatic schedule or manually on demand. Event-Driven RRM (ED-RRM) takes this a step further; DCA can be triggered based on RF events that occur in real time. The CleanAir feature, covered in more detail in Chapter 19, “Dealing with Wireless Interference,” provides the triggers for ED-RRM. By default, ED-RRM is disabled. You can enable it with the **EDRRM** check box at the very bottom of the web page.

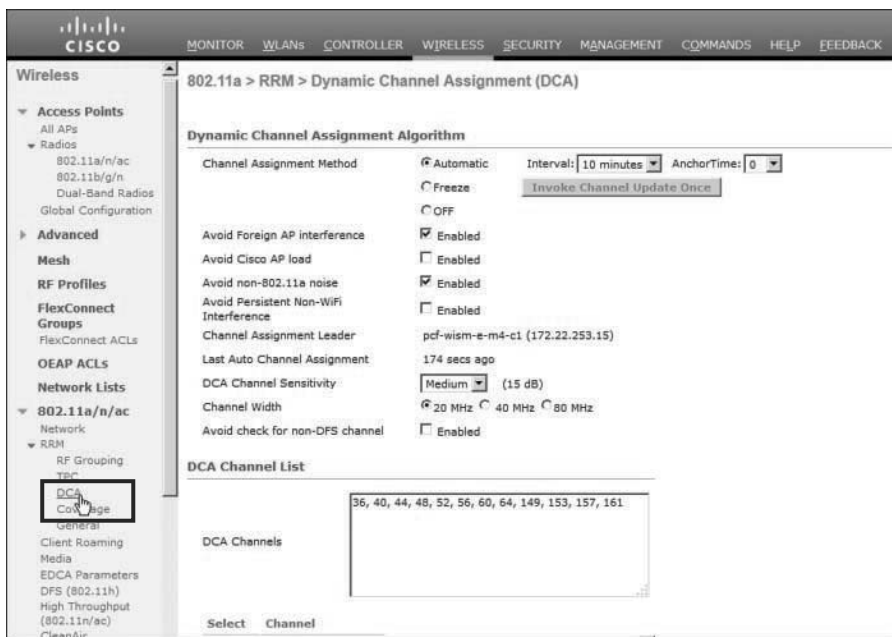


Figure 13-12 *Adjusting the RRM DCA Algorithm Parameters*

Coverage Hole Detection Mitigation

The TPC algorithm normally reduces AP transmit power levels to make cell sizes appropriate. Sometimes you might find that your best intentions at providing RF coverage with a good AP layout still come up short. For example, you might discover that signals are weak in some small area of a building due to the building construction or surrounding obstacles. You might also have an AP radio that happens to fail, causing a larger coverage hole. How would you discover such a condition? You could make a habit of surveying the RF coverage often. More likely, your wireless users will discover a weakness or hole in the coverage and complain to you about it.

A Cisco controller-based wireless network offers an additional RRM algorithm that can detect coverage holes and take action to address them. Coverage hole detection mitigation (CHDM) can alert you to a hole that it has discovered and it can increase an AP's transmit power level to compensate for the hole.

CHDM is useful in two cases:

- Extending coverage in a weak area
- Rapidly healing a coverage hole caused by an AP or radio failure, sooner than the TPC algorithm can detect and correct

The algorithm does not run at regular intervals like TPC and DCA do. Instead, it monitors the RF conditions of wireless clients and decides when to take action. In effect, the algorithm leverages your wireless users who are out in the field and tries to notice a problem before they do.

Every controller maintains a database of associated clients and their RSSI and signal-to-noise ratio (SNR) values. It might seem logical to think that a low RSSI or SNR would mean a client is experiencing a hole in coverage. Assuming the client and its AP are using the same transmit power levels, if the AP is receiving the client at a low level, the client must also be receiving the AP at a low level. This might not be true at all; the client might just be exiting the building and getting too far away from the AP. The client might also have a “sticky” roaming behavior, where it maintains an association with one AP until the RSSI falls to a very low level before reassociating elsewhere.

CHDM tries to rule out conditions that are experienced by small numbers of clients and signal conditions due to client roaming behavior. A valid coverage hole is detected when some number of clients, all associated to the same AP, have RSSI values that fall below a threshold. In addition, the coverage hole condition must exist longer than a threshold of time without the client roaming to a different AP.

**Key
Topic**

By default, the following conditions must all be met for a coverage hole to be detected:

- Client RSSI at the AP is at or below -80 dBm.
- The low RSSI condition must last at least 60 seconds over the past 180 seconds.
- The condition must affect at least three clients or more than 25 percent of the clients on a single AP.

Be aware that CHDM runs on a per-band basis. Unlike TPC and DCA, which operate on the entire RF group of controllers, CHDM runs on each controller independently, on a per-AP radio basis.

You can display and configure the CHDM thresholds by selecting **Wireless > 802.11a/n/ac** or **802.11b/g/n > RRM > Coverage**. Figure 13-13 shows the threshold parameters for the 5-GHz 802.11a band.

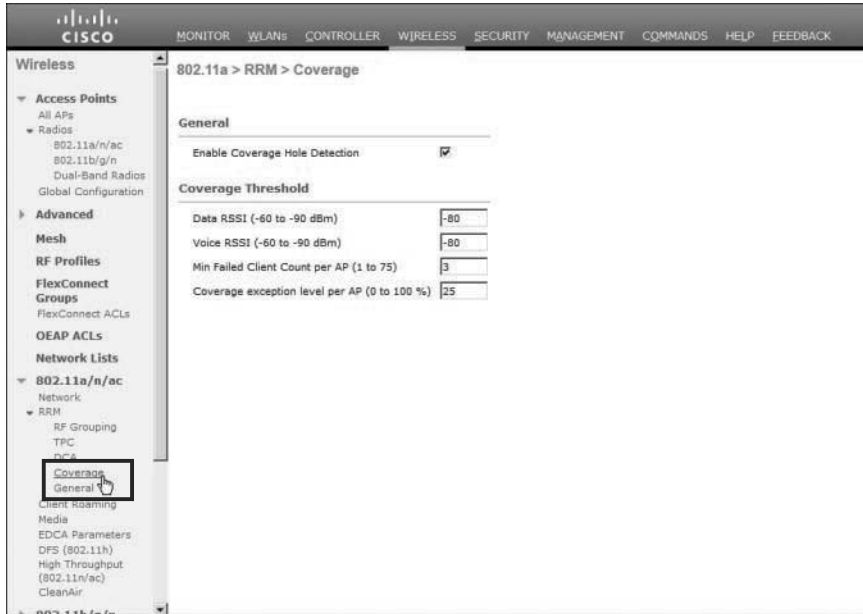


Figure 13-13 Displaying Coverage Threshold Parameters for the 5-GHz 802.11a Band

Manual RF Configuration

You might sometimes want to keep RRM from changing the RF conditions in parts of your wireless network. For instance, you might have client devices that operate at a fixed transmit power level. Ideally, the AP and client power levels should be identical or matched. If RRM raises or lowers AP power levels at a later time, then asymmetric power levels would result.

You can override RRM on a per-AP basis by selecting **Wireless > Access Points > Radios > 802.11a/n/ac** or **802.11b/g/n**. From the list of APs displayed, choose a specific AP and select the drop-down menu at the far-right side of the list. From this menu, select **Configure**, as shown in Figure 13-14.

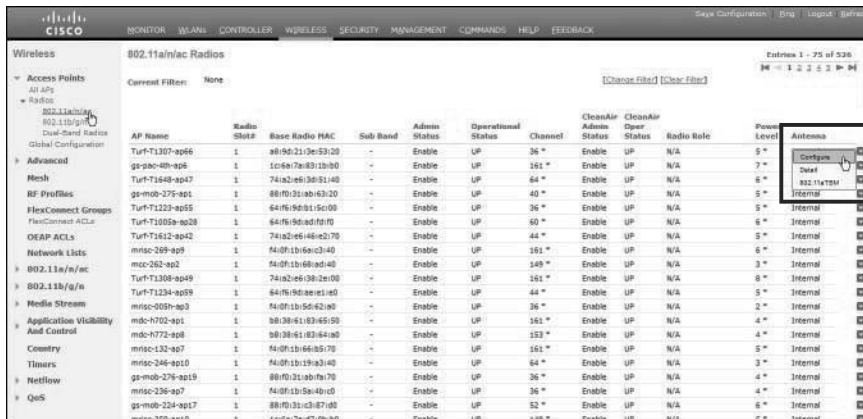


Figure 13-14 Selecting an AP for Manual Configuration

On the AP configuration page, as shown in Figure 13-15, you can set the channel under RF Channel Assignment or the transmit power under Tx Power Level Assignment. By default, the **Global** radio button is selected for each, which allows the value to be determined globally within the RF group. You can set a specific channel or power level by selecting the **Custom** radio button and then choosing a value from the drop-down list. In the figure, the AP's transmit power level has been manually set to 3.

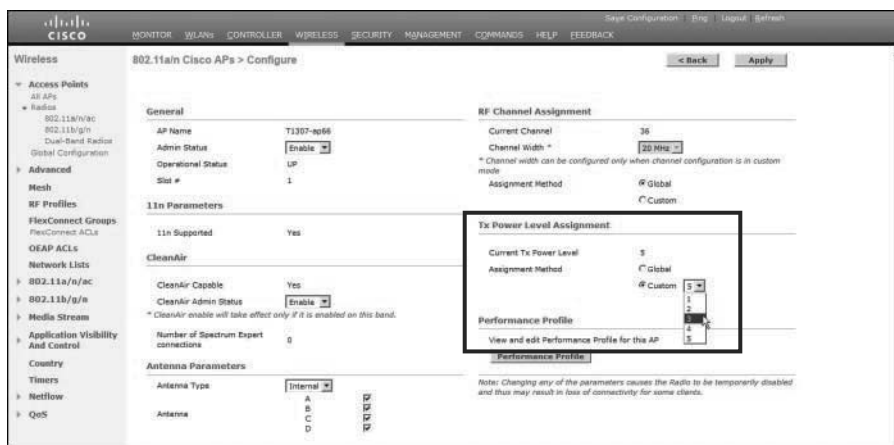


Figure 13-15 Manually Setting the Transmit Power Level of an AP

Tip You should let RRM automatically adjust both channels and transmit power levels whenever possible.

Verifying RRM Results

The RRM algorithms can either run at regular intervals or on demand. You can display the channel number and transmit power level that are being used on every AP by selecting **Wireless > Access Points > Radios > 802.11a/n/ac** or **802.11b/g/n**, as shown in Figure 13-15. The controller displays an asterisk next to values that have been set through RRM. Otherwise, if no asterisk appears, the value has been set manually.

To get a much better feel for the RRM results, you can use the Cisco Prime Infrastructure management system (covered in Chapter 18, “Managing Cisco Wireless Networks”) to view APs on a graphical representation of an area. The map in Figure 13-16 displays each AP's location on a building floor plan, along with its channel number and transmit power level for the 2.4-GHz band. Figure 13-17 shows the same map for the 5-GHz band. Seeing the physical arrangement of APs and their cells can help you get a much better idea how the channels are assigned and reused.

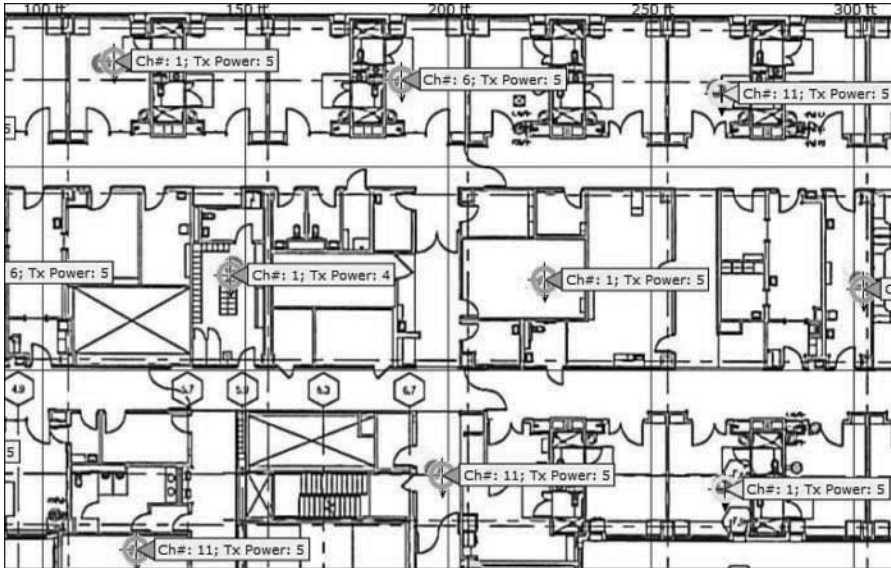


Figure 13-16 *Displaying 2.4-GHz RRM Results in Cisco Prime Infrastructure Maps*

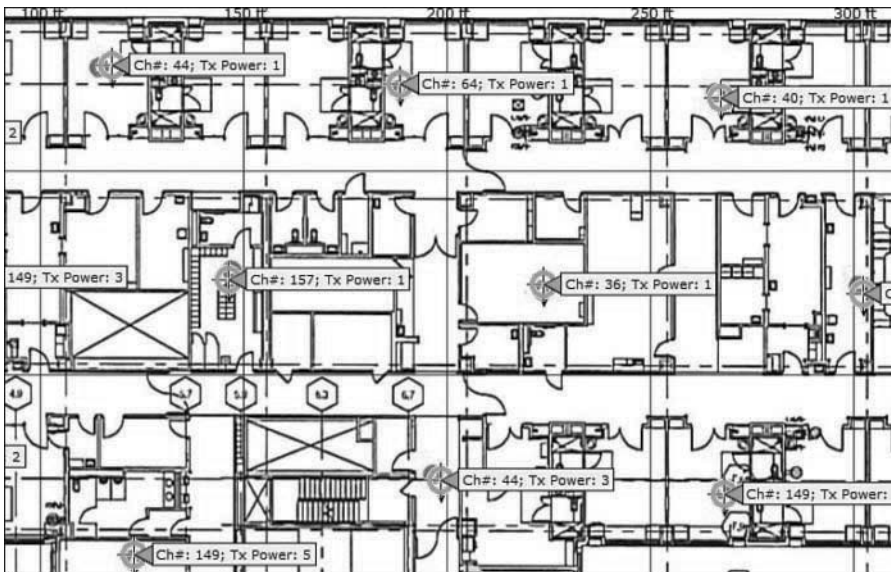


Figure 13-17 *Displaying 5-GHz RRM Results in Cisco Prime Infrastructure Maps*

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 21, “Final Review,” and the exam simulation questions on the DVD.

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 13-4 lists a reference of these key topics and the page numbers on which each is found.

**Key
Topic**

Table 13-4 Key Topics for Chapter 13

Key Topic Element	Description	Page Number
List	Data rate states	309
Figure 13-7	RF group formation	314
Figure 13-9	TPC operation	315
Table 13-2	AP transmit power level numbers	317
Figure 13-11	DCA operation	318
List	Coverage hole detection criteria	321

Define Key Terms

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

coverage hole, dynamic channel allocation (DCA), mandatory data rate, Radio Resource Management (RRM), RF group, RF group leader, supported data rate, transmit power control (TPC)



Index

Symbols

- 1-Mbps data rate, 28
- 2-Mbps data rate, 28
- 2.4-GHz bands, 10
 - 802.11 channels, 47-48
 - 802.11n channel aggregation, 57
 - configuring, 309
 - ETSI requirements, 44
 - FCC requirements, 43
 - free space path loss, 78
 - interference, 74-76
 - RRM results, displaying, 323
- 5-GHz band, 11
 - 802.11 channels, 49-50
 - 802.11ac channels, 61*
 - 802.11n channel aggregation, 56*
 - configuring, 309
 - ETSI requirements, 44
 - FCC requirements, 44
 - free space path loss, 78
 - neighboring channel interference, 76
 - RRM results, displaying, 323
- 5.5-Mbps data rate, 29-30
- 11-Mbps data rate, 30
- 19-dB separation, 75
- 802.1 standard, 46
- 802.1x
 - EAP integration, 338
 - WPA2 enterprise authentication, 346
 - 802.2 standard, 46
 - 802.3 frames, 132
 - 802.3 standard, 46
 - 802.4 standard, 46
 - 802.5 standard, 46
 - 802.11 standards, 46, 50
 - 2.4-GHz ISM channel definitions, 47-48
 - 5-GHz U-NII channel definitions, 49-50
 - amendments, 51
 - BSSs, 116-118
 - centralized controllers, configuring, 245
 - converged WLCs, enabling, 252
 - data rates, configuring, 309
 - device interference, 432
 - DSs, 118-120
 - ESSs, 120-121
 - frames
 - 802.3 frames, compared, 132*
 - addressing, 134-135*
 - control, 141-142*
 - CSMA, 137*
 - data, 142*
 - format, 133*
 - management, 140-141*
 - moving to/from DSs, 133*
 - not moving to/from DSs, 134*
 - timing schemes, 138*
 - transmission failures, 139*

- IBSSs, 122
 - protocols, 68
- 802.11-1997, 51
- 802.11a, 53-54
- 802.11ac, 60
 - channel aggregation, 61-63
 - configuring, 310-311
 - DCA algorithm, 319
 - implementation, 65
 - MAC layers, 63
 - modulation, 63
 - MU-MIMO, 65
 - spatial multiplexing, 64
 - transmit beamforming, 64
- 802.11ad, 66
- 802.11af, 66
- 802.11ah, 66
- 802.11b, 51
- 802.11g, 52-53
- 802.11i, 342-343
- 802.11n, 54-55
 - channel aggregation, 55-57
 - configuring, 310-311
 - DCA algorithm, 319
 - MAC layer efficiency, 58
 - maximal-ratio combining, 60
 - modulation and coding schemes, 60
 - spatial multiplexing, 57-58
 - transmit beamforming, 59-60
- 802.11r, 290
- 802.11w, 344
- 802.15 standard, 46
- 8021X_REQD state, 455
- (Λ) (lambda symbol), 14

A

- absolute power measurements, 16
- absorption (RF signals), 82-83
- access point. *See* AP
- access switches, 201
- accessing
 - iOS device Wi-Fi settings, 400
 - MacOS X configuration utility, 397
 - Meraki Dashboard, 224
 - PI maps, 421
 - protected credentials, 339
 - SNMP, 240
 - SSIDs, controlling, 226
 - switch management web page, 247
 - Wi-Fi Protected. *See* WPA2
 - wireless medium
 - carrier sense multiple access*, 137
 - collision avoidance*, 137-139
 - timing schemes*, 138
 - transmission failures*, 139
- ACK frames, 141
- actions
 - alarms, 419
 - frames, 141
- activating exam engine, 483
- active scans, 143
- active site surveys, 171, 176-178
 - AP signal strength, displaying, 177
 - client roaming behaviors, 178
 - methods, 176
 - ping round-trip times measured, displaying, 177
- ad hoc wireless networks, 122, 391
- adapters, 392
- adaptive modulation and coding (AMC), 79, 160

addresses

802.11 frames, 134-135

DAs, 135

fields, 135

IP

*autonomous APs, finding, 216**centralized controller**parameters, 256**client problems troubleshooting, 458**guest WLANs, 377**management, 189*

MAC, 442

primed, 271

RAs, 135

SAs, 135

sender MAC, 341

TAs, 135

adjacent channel interference, 75-76**administrative users, creating, 249****Advanced Encryption Standard (AES), 342****advice for exam event**

pre-exam suggestions, 481-482

question types, learning, 475

*drag-and-drop, 477-479**fill in the blank, 477**multiple choice, 476-479**simlets, 478-479**simulation, 478-479**testlets, 478-479*

time budget, 480-481

AES (Advanced Encryption Standard), 342**air-quality index (AQI), 443-444****AirMagnet**

spectrum analysis, 437

Spectrum XT, 172

Alarm Browser, 418**alarms, 417**

actions, 419

browsing, 418

managing, 418

severity levels, 417

summary, displaying, 417

algorithms

AES, 342

CCMP, 342

CHDM, 321

DCA, 318-320

*channel layout, solving, 319**channel list, editing, 320**metrics affecting, 318**parameters, 319**time intervals, setting, 319**triggering with ED-RRM, 320**wide channels, 319*

key mixing, 341

RC4 cipher, 337

TPC, 315-317

*parameters, configuring, 316**running, 317**transmit power, 317**versions, 316***AMC (adaptive modulation and coding), 79, 160****amplifiers, 107****amplitude (signals), 15****analyzing**

packets, 470

Wi-Fi

*activity, 469**frames, 470***anchors**

controllers, 293-295

mobility, 376, 380-381

Android devices, 395-396

- available networks, displaying, 395
- connections, verifying, 396
- manually adding networks, 395
- security, 396
- Wifi Analyzer, 468

annotations (alarms), 419**antennas**

- accessories, 107-108
- beamwidth, 97-98
- Cisco, 99
- directional, 103
 - parabolic dish, 105-106*
 - patch, 103-104*
 - Yagi, 104-105*
- ETSI requirements, 44
- FCC regulations, 43
- gain, 97, 107
- isotropic, 21
- omnidirectional, 99
 - dipole, 100-101*
 - integrated, 101-102*
 - monopole, 101*
- orientation, verifying, 467
- polarization, 98-99
- radiation patterns, 94-97
 - cutting with two planes, 95*
 - H/E polar plots, recording, 96*
 - plotting, 94*
- summary, 107
- TNC/RP-TNC connectors, 43

AP (access point), 116

- adjacent AP channels, reusing, 162
- air-quality ratings, displaying, 443
- AP-on-a-stick surveys, 175
- association frames, 141
- authentication/deauthentication, 140, 333

autonomous, 187, 190, 217

- channel selection, 220*
- connecting, 215-217*
- data paths, 188*
- data VLAN, 189*
- Easy Setup page, 218-219*
- GUI tabs, 220*
- lightweight, compared, 192*
- management IP addresses, 189*
- optimizing, 220*
- radios, enabling, 220*
- roaming between, 285-286*
- security, 219*
- single, supporting, 188*
- upgrading, 221-223*
- web interface, 217*

beacons, 140**BSSIDs, 117****cell size, tuning**

- data rates, 159-161*
- transmit power, 157-159*

channel layout, 165-168

- alternating pattern holes, 166*
- channel reuse, 167*
- honeycomb pattern, 167*
- three dimensions, 168*

Cisco, 206-207**CleanAir, 439-440****clients**

- associations, 162-163, 458*
- roaming, 163-165*
- scans, 143*

cloud-based, 190-191

- adding/claiming, 224*
- client roaming, 227*
- connectors, 223*

- Meraki Dashboard, accessing, 224, 227*
- security, 226*
- SSIDs, configuring, 225-226*
- connectivity, verifying, 464
 - antenna orientation, 467*
 - AP orientation, 467*
 - AP-to-network, 465-466*
 - AP-to-WLC, 464-465*
- counts, monitoring, 419
- data rates, 142-143
- deployment phases, 178-179
- disassociation frames, 141
- ESSs, 120-121
- fake, 333
- heatmap contributors, 423
- IBSSs, 122
- information, displaying on PI maps, 424
- layout, 311
- lightweight. *See* LAPs
- management frames, 343-344
- manual configuration
 - selecting, 322*
 - transmit power, 323*
- multiple SSIDs, supporting, 119
- noninfrastructure modes
 - mesh networks, 125*
 - outdoor bridges, 124*
 - repeater, 122-123*
 - WGB, 123*
- orientation, verifying, 467
- passing from one to another. *See* roaming
- passing through, 117
- PI map locations, 421
- probes, 140
- reassociation frames, 141
- rogue
 - detecting/containing, 335-336*
 - interference, 432*
 - PI maps, 426*
- signal strength, displaying, 177
- SSIDs, 117
- SSIDs to VLANs, bridging, 214
- states, 268-270
- AP-manager interfaces (controllers), 237**
- AP-to-network connectivity, verifying, 465-466**
- AP-to-WLC connectivity, verifying, 464-465**
- Apple iOS devices, 400**
 - available networks, displaying, 401
 - connection information, 402
 - security, 402
 - Wi-Fi settings, accessing, 400
- applications**
 - location services, 170
 - real-time/non-real-time, 388
 - wireless requirements, 169-170
- AQI (air-quality index), 443-444**
- architectures**
 - autonomous, 187-190
 - data paths, 188*
 - data VLAN, 189*
 - management IP addresses, 189*
 - single autonomous APs, supporting, 188*
 - centralized, 197-200
 - traffic paths, 198-199*
 - user mobility, 198*
 - WLC location, 197*
 - Cisco Unified Access, 412-413
 - cloud-based, 190-191
 - converged, 200-202

- access switch capacities, 201*
- scalability, 202*
- traffic paths, 202*
- user mobility, 202*
- WLC location, 201*
- FlexConnect, 204-205
- split-MAC, 192-197
 - CAPWAP, 193*
 - centralized, 197-200*
 - converged, 200-202*
 - digital certificates, 194*
 - FlexConnect, 204-205*
 - LAPs to central WLC, connecting, 195*
 - VLAN 100, 194*
 - WLC activities, 196*
- AS (authentication server), 339
- Association tab, 221
- associations
 - BSSs, 117
 - clients, managing, 461
 - request frames, 141
- asymmetric power problems, 158
- attacks
 - detecting, 336
 - man-in-the-middle, 333
 - protection against, 335
- attenuators, 108
- AUTHCHECK state, 455
- authentication
 - APs, 333
 - central web, 375
 - clients, 332, 347
 - EAP, 338-339
 - 802.1x integration, 338*
 - EAP-FAST, 339-340*
 - EAP-TLS, 340*
 - LEAP, 339*
 - PEAP, 340*
 - frames, 140
 - local EAP, enabling, 350
 - local web, 375
 - open, 336, 379
 - servers (ASs), 339
 - web, 336, 375, 379
 - WEP, 337-338
 - WLANs, 346, 363
 - WLCs, 197
 - WPA/WPA2, 343, 346
- authenticators, 339
- autonomous APs, 187, 190
 - configuring, 217
 - channel selection, 220*
 - Easy Setup page, 218-219*
 - GUI tabs, 220*
 - optimization, 220*
 - radios, enabling, 220*
 - security, 219*
 - web interface, 217*
 - connecting, 215
 - BVI, 217*
 - CDP neighbor information, displaying, 216*
 - IP address, finding, 216*
 - port availability, 215*
 - data paths, 188
 - management IP addresses, 189
 - roaming between, 285-286
 - single, supporting, 188
 - upgrading, 221-223
 - VLAN, 189
- autonomous architecture, 187-190
 - data paths, 188
 - management IP addresses, 189

single APs, supporting, 188
VLANs, 189

avoiding collisions, 137-139

timing schemes, 138
transmission failures, 139

B

backoff timers, 138

bands

2.4-GHz

802.11 channels, 47-48
802.11n channel aggregation, 57
co-channel interference, 74
configuring, 309
ETSI requirements, 44
FCC requirements, 43
free space path loss, 78
neighboring channel interference, 76
non-802.11 device interference, 76
RRM results, displaying, 323

5-GHz

802.11 channels, 49-50
802.11ac channels, 61
802.11n channel aggregation, 56
configuring, 309
ETSI requirements, 44
FCC requirements, 44
free space path loss, 78
neighboring channel interference, 76
RRM results, displaying, 323

extended, 44

frequencies, 10

2.4-GHz, 10

5-GHz, 11

channels, 12-13

ISM (industrial, scientific, and medical), 42

licensed, 41

U-NII, 42

unlicensed, 42

bandwidth, 12, 25

Barker 11 code, 28

base-10 logarithm (log₁₀), 17

basic service area (BSA), 117. *See also* cells

basic service sets. *See* BSSs

beacons, 140

beamwidth, 97-98

bidirectional communication, 115

BLE (Bluetooth Low Energy), 433

block ACK frames, 141

block acknowledgment, 58

Bluetooth

interference, 432-433

Low Energy (BLE), 433

Special Interest Group (SIG), 433

bridged-virtual interface (BVI), 217

bridges, 219

broadcasting SSIDs, 362

BSA (basic service area), 117. *See also* cells

BSSIDs (BSS identifiers), 117, 176

BSSs (basic service sets), 116-118

APs, 116

associations, 117

clients

joining, 144-145

leaving, 145-146

roaming between, 146

discovering, 143

DSs, 118-120

stations, 117

traffic flows, 117

building blocks, 207

BVI (bridged-virtual interface), 217

C

CA (certificate authority), 340

calculating

antenna beamwidth, 98

dB, 17

free space path loss, 78

canopy interference, 435

CAPWAP (Control and Provisioning of Wireless Access Points) tunneling protocol

Discovery Requests, 270

Join Requests, 271

LAPs

central WLC, connecting, 195

WLCs, linking, 193

carrier sense multiple access (CSMA), 137

carrier signals, 24

constant frequency, 24

modulation/demodulation, 25-26

CCA (clear channel assessment), 137

CCK (Complementary Code Keying), 30, 51

CCKM (Cisco Centralized Key Management), 290

CCMP (Counter/CBC-MAC Protocol), 342

CCX (Cisco Compatibility Extensions), 403

goals, 403

Lite, 404

MFP, 403

security support, 404-405

Version 5 (CCXv5), 344

versions, 403-404

CDP (Cisco Discovery Protocol), 216

cells

channel layout, 165-168

alternating pattern holes, 166

channel reuse, 167

honeycomb pattern, 167

three dimensions, 168

client associations, 162-163

optimizing, 220

overlap, 165

size, tuning

data rates, 159-161

transmit power, 157-159

central web authentication (CWA), 375

centralized architectures, 197-200

traffic paths, 198-199

user mobility, 198

WLC location, 197

centralized controllers

dynamic interfaces, creating, 358-360

initial setup with CLI, 257

initial setup with Configuration Wizard, 239-247

802.11 support, 245

LAG mode, 241

management interface, 241

RADIUS server, 244

rebooting, 246

RF mobility domain, 242

service port, 240

SNMP access, 240

system access, 239

system clock, 246

virtual interface, 243

WLAN, 243

initial setup with WLAN Express Setup, 254

- controller identification*, 254
- starting*, 254
- verifying*, 256
- VLAN/IP address parameters*, 256
- WLANs*, 255
- RADIUS servers, configuring, 356
- roaming
 - coordination*, 298-300
 - Layer 2*, 290-292
 - Layer 3*, 292-296
 - mobility groups*, 296-298
- WLAN security, 364
- certificate authorities (CAs), 340
- Chanalyzer, 437
- channels, 12
 - 2.4-GHz ISM band, 47-48
 - 5-GHz U-NII band, 49-50
 - 802.11ac, 61-63
 - 802.11n, 55-57
 - adjacent APs, reusing, 162
 - dynamic allocation. *See* DCA
 - dynamic assignment, 196
 - interference
 - co-channel*, 74-75
 - neighboring channel*, 75-76
 - non-802.11 devices*, 76
 - invalid, 435
 - layout, 165-168
 - alternating pattern holes*, 166
 - channel reuse*, 167
 - honeycomb pattern*, 167
 - three dimensions*, 168
 - quality information, 439
 - reusing, 167
 - scanning
 - client roaming*, 165
 - tools*, 468
 - selecting, 220
 - spacing, 13
 - transmission requirements, 138
- CHDM (coverage hole detection mitigation), 315, 321
- chips, 27
- Cisco
 - APs, 206-207
 - Centralized Key Management (CCKM), 290
 - Certification Exam Tutorial, 475
 - drag-and-drop*, 477-479
 - fill in the blank*, 477
 - multiple choice*, 476-479
 - simlets*, 478-479
 - simulation*, 478-479
 - testlets*, 478-479
 - CleanAir. *See* CleanAir
 - ClientLink, 60
 - Compatibility Extensions. *See* CCX
 - Discovery Protocol, 216
 - LAPs, 207-208
 - Learning Network website, 485
 - Meraki, 190
 - Meraki Dashboard
 - accessing*, 224
 - tabs*, 227
 - Mobility Services Engine (MSE), 208, 412
 - Prime Infrastructure. *See* PI
 - Prime Infrastructure Maps, 323
 - Unified Access architecture, 412-413
 - WLC/WCM platforms/capabilities, 205-206
- CleanAir, 439-440
 - detection reports, 442
 - enabling, 440
 - interference types, 441
 - overview, 440

- clear channel assessment (CCA), 137
- CLI, 257
- click-and-go mode (passive site surveys), 175
- client-based OS troubleshooting tools, 468
- ClientLink, 60
- clients
 - Android, 395-396
 - available networks, displaying, 395*
 - connections, verifying, 396*
 - manually adding networks, 395*
 - security, 396*
 - AP
 - associations, 162-163*
 - scanning, 143*
 - Apple iOS, 400
 - available networks, displaying, 401*
 - connection information, 402*
 - security, 402*
 - Wi-Fi settings, accessing, 400*
 - associations, managing, 461
 - authentication, 332
 - EAP, 338-340*
 - open, 336*
 - WEP, 337-338*
 - WLANs, 347*
 - channel layout, 165-168
 - alternating pattern holes, 166*
 - channel reuse, 167*
 - honeycomb pattern, 167*
 - three dimensions, 168*
 - connectivity, troubleshooting, 454
 - AP associations, 458*
 - client locations, displaying, 457*
 - controller logs, viewing, 463*
 - from controllers, 461*
 - device inspection, 453*
 - displaying clients in PI, 454*
 - information gathering, 453*
 - IP addressing problems, 458*
 - mobility details, 456*
 - PI client searches, 454*
 - policy states, 455*
 - RF history, 457*
 - RF problems, 458*
 - RF statistics, 456*
 - RSSI/SNR problems, 459*
 - successful wireless association conditions, 453*
 - testing clients from PI, 459-460*
 - WLAN settings, verifying, 462-463*
 - counts, monitoring, 419
 - Layer 3 roam, 294-295
 - load balancing, 196
 - locations, 424
 - MacOS X, 397
 - configuration utility, accessing, 397*
 - discovered networks, displaying, 397*
 - new network profiles, creating, 399*
 - preferred networks list, displaying, 398*
 - system information, displaying, 399*
 - MFP, 343
 - mobility details, displaying, 456
 - networks
 - joining, 144-145*
 - leaving, 145-146*
 - roaming between, 146*

PI

- AP associations, 458*
- details, displaying, 455*
- displaying, 454*
- location, 457*
- RF history, 457*
- RF statistics, 456*
- searching, 454*

policy states, 455

power, saving, 147-150

- DTIMs, 149*
- legacy method, 147*
- radio sleeping, 147*
- U-APSD method, 149*
- whole device sleeping, 147*

roaming, 163-165

- behaviors, displaying, 178*
- cell overlap, 165*
- cloud-based APs, 227*
- conditions, 164*
- correctly between APs, 164*
- flexibility, 196*
- scanning other channels, 165*

rogue, 335, 426

status information, 461

testing from PI, 459-460

Windows, 389-390

- ad hoc networks, 391*
- adapter settings, 392*
- available SSIDs, 389*
- connections, verifying, 393*
- drivers, 394*
- manually configuring, 391*
- preferred networks list, manually populating, 391*
- wireless status icon, finding, 389*

wireless requirements, 388-389

WLAN, 365

clocks

centralized controllers, synching, 246

converged WLCs, 253

cloud-based

APs, configuring

- adding/claiming, 224*
- client roaming, 227*
- connectors, 223*
- Meraki Dashboard, accessing, 224, 227*
- security, 226*
- SSIDs, 225-226*

architecture, 190-191

site survey tools, 171

cluster IDs, 442

co-channel interference, 74-75

code images (controllers), updating, 259-262

coders, 27

coding schemes, 60

collisions

avoidance, 137-139

- timing schemes, 138*

- transmission failures, 139*

wireless medium, 136

communication

bidirectional, 115

passing through, 117

unidirectional, 115

Complementary Code Keying (CCK), 30, 51

Configuration Wizard

centralized controllers initial setup, 239-247

- 802.11 support, 245*

- LAG mode, 241*

- management interface*, 241
- RADIUS server*, 244
- rebooting*, 246
- RF mobility domain*, 242
- service port*, 240
- SNMP access*, 240
- system access*, 239
- system clock*, 246
- virtual interface*, 243
- WLAN*, 243
- converged controllers initial setup, 247-253
 - 802.11, 252
 - administrative users, creating*, 249
 - clock*, 253
 - management ports*, 250
 - mobility*, 251
 - RF mobility*, 251
 - SNMP parameters*, 249
 - switch management web page*, 247
 - verifying*, 253
 - web-based management switch configuration*, 247
 - wireless management*, 250
 - WLAN*, 252
 - WLC management page*, 248
- configuring**
 - 2.4-GHz bands, 309
 - 5-GHz bands, 309
 - 802.11ac, 310-311
 - 802.11n, 310-311
 - Android Wi-Fi, 395-396
 - available networks, displaying*, 395
 - connections, verifying*, 396
 - manually adding networks*, 395
 - security*, 396
 - APs manually
 - selecting*, 322
 - transmit power*, 323
 - Apple iOS Wi-Fi, 400
 - available networks, displaying*, 401
 - connection information*, 402
 - security*, 402
 - settings, accessing*, 400
 - autonomous APs, 217
 - channel selection*, 220
 - connecting*, 215-217
 - Easy Setup page*, 218-219
 - GUI tabs*, 220
 - optimization*, 220
 - radios, enabling*, 220
 - security*, 219
 - web interface*, 217
 - centralized controllers with CLI, 257
 - centralized controllers with Configuration Wizard, 239-247
 - 802.11 support, 245
 - management interface*, 241
 - RADIUS server*, 244
 - rebooting*, 246
 - RF mobility domain*, 242
 - service port*, 240
 - SNMP access*, 240
 - system access*, 239
 - system clock*, 246
 - virtual interface*, 243
 - WLAN*, 243
 - centralized controllers with WLAN Express Setup, 254
 - controller identification*, 254
 - starting*, 254
 - verifying*, 256

- VLAN/IP address parameters, 256
- WLANs, 255
- cloud-based APs
 - adding/claiming, 224
 - client roaming, 227
 - connectors, 223
 - Meraki Dashboard, accessing, 224, 227
 - security, 226
 - SSIDs, 225-226
- converged controllers with Configuration Wizard, 247, 253
 - 802.11, 252
 - administrative users, creating, 249
 - clock, 253
 - management ports, 250
 - mobility, 251
 - RF mobility, 251
 - SNMP parameters, 249
 - switch management web page, 247
 - verifying, 253
 - web-based management switch configuration, 247
 - wireless management, 250
 - WLAN, 252
 - WLC management page, 248
- data rates, 309
- devices with PI, 426
- guest WLANs
 - dynamic interface, 377
 - interface, assigning, 378
 - IP address information, 377
 - mobility anchors, 380-381
 - open authentication, 379
 - SSID, 378
 - web authentication, 379
- MacOS X Wi-Fi, 397
 - configuration utility, accessing, 397
 - discovered networks, displaying, 397
 - new network profiles, creating, 399
 - preferred networks list, displaying, 398
 - system information, displaying, 399
- RADIUS servers, 356-357
 - centralized controllers, 356
 - converged controllers, 357
- RRM TPC algorithm parameters, 316
- security, 344
- Windows Wi-Fi, 389-390
 - ad hoc networks, 391
 - adapter settings, 392
 - available SSIDs, 389
 - connections, verifying, 393
 - drivers, 394
 - manually configuring, 391
 - preferred networks list, manually populating, 391
 - wireless status icon, finding, 389
- WLANs
 - advanced settings, 365-366
 - client session timeouts, 365
 - displaying, 366
 - general parameters, 361
 - management access, 367
 - QoS, 364-365
 - security, 362-364
- WPA2
 - enterprise mode, 346-348
 - Local EAP, 348-350
 - personal mode, 344-345

connected mode (FlexConnect), 205**connectivity**

- APs, verifying, 464
 - antenna orientation, 467*
 - AP orientation, 467*
 - AP-to-network, verifying, 465-466*
 - AP-to-WLC, verifying, 464-465*

autonomous APs, 215

- BVI, 217*
- CDP neighbor information, displaying, 216*
- IP address, finding, 216*
- port availability, 215*

clients, troubleshooting, 454

- AP associations, 458*
- client locations, displaying, 457*
- controller logs, viewing, 463*
- from controllers, 461*
- device inspection, 453*
- displaying clients in PI, 454*
- information, gathering, 453*
- IP addressing problems, 458*
- mobility details, 456*
- PI client searches, 454*
- policy states, 455*
- RF history, 457*
- RF problems, 458*
- RF statistics, 456*
- RSSI/SNR problems, 459*
- successful wireless association conditions, 453*
- testing clients from PI, 459-460*
- WLAN settings, verifying, 462-463*

iOS devices, 402

LAPs to central WLC, 195

verifying

- Android devices, 396*
- Windows wireless, 393*

connectors, 223

console ports, 235

contention windows, 138

continuous scan mode (passive site surveys), 175

continuous transmitter interference, 435

Control and Provisioning of Wireless Access Points. *See* CAPWAP

control frames, 141-142

controllers

air-quality ratings, 443

anchor, 293

AP

- connectivity, verifying, 464-465*
- states, 268-270*

backing up, 258-259

centralized

- dynamic interfaces, creating, 358-360*
- initial setup with CLI, 257*
- initial setup with Configuration Wizard, 239-247*
- initial setup with WLAN Express Setup, 254-256*
- RADIUS servers, configuring, 356*
- WLAN security, 364*

clients, troubleshooting, 461

converged. *See* WCMs

failures, detecting, 274

identifying, 254

IDSs, 335

interfaces, 237-238, 362

LAPs RTT between, 199

- Local EAP profiles, 348
- logs, viewing, 463
- mobility (MCs), 298
- multiple, discovering, 272-273
- platforms/capabilities, 205-206
- ports, 235-236
- primed addresses, 271
- rebooting, 261
- redundancy, 274
 - N+1*, 274-275
 - N+N*, 275-276
 - N+N+1*, 276-277
 - SSO, 277-278
- roaming
 - converged controllers*, 301
 - coordination*, 298-300
 - intracontroller*, 288-290
 - Layer 2*, 290-292
 - Layer 3*, 292-296
 - mobility groups*, 296-298
 - WCMs*, 300-302
- rogue APs, 335-336
- updating, 259-262
- VLANs, mapping, 237
- WCMs, 300-302
- wireless parameters, 308
- WLCs. *See* WLCs
- converged architectures, 200-202**
 - access switch capacities, 201
 - scalability, 202
 - traffic paths, 202
 - user mobility, 202
 - WLC location, 201
- converged controllers. *See* WCM**
- cordless phone interference, 434**
- Counter/CBC-MAC Protocol (CCMP), 342**

- coverage**
 - holes, detecting, 315, 321
 - poorly configured RF, 312
 - self-healing, 196
 - verification
 - active site surveys*, 176-178
 - AP deployment phases*, 178-179
 - AP-on-a-stick surveys*, 175
 - device/application requirements*, 169-170
 - location services*, 170
 - passive site surveys*, 174-175
 - planning surveys*, 172-173
 - site surveys*, 171-172
- Coverage Optimal Mode (TPCv1), 316**
- critical alarms, 417**
- CSMA (carrier sense multiple access), 137**
- CSMA/CA (CSMA/collision avoidance), 138**
- CSMA/CD (CSMA/collision detection), 137**
- CWA (central web authentication), 375**
- cycles (waves), 9**

D

- DA (destination address), 135**
- dashboard (PI)**
 - alarms, 417
 - actions*, 419
 - browsing*, 418
 - managing*, 418
 - severity levels*, 417
 - summary, displaying*, 417
 - dashlets, 416
- dashlets, 416**

data

- frames, 142
- paths, 188
- privacy/integrity, 333-334
 - CCMP*, 342
 - TKIP*, 341-342
- rates
 - 802.11a*, 53
 - 802.11b*, 51
 - 802.11g*, 52
 - AP cell size, tuning*, 159-161
 - APs*, 142-143
 - configuring*, 309
 - disabled*, 309
 - lower, disabling*, 160
 - mandatory*, 309
 - supported*, 309
- sending over RF signals, 24-26
- dB (decibel)**, 17-18
- dB_i (dB-isotropic)**, 20-23
- dB_m (dB-milliwatt)**, 19-20
- DBPSK (differential binary phase shift keying)**, 28
- DCA (dynamic channel allocation)**, 315, 318-319
 - channel layout, solving, 319
 - channel list, editing, 320
 - defined, 315
 - metrics affecting, 318
 - parameters, 319
 - RRM, 320
 - time intervals, setting, 319
 - triggering with ED-RRM, 320
 - wide channels, 319
- DCF (distributed coordination function)**, 136
- deauthentication**
 - BSSs, leaving, 145
 - frames, 140

decibel (dB), 17-18**decryption**, 333**DECT (Digital Enhanced Cordless Telecommunications)**, 434**deleting alarms**, 419**delivery traffic indication messages (DTIM)**, 149**demodulation**, 25**destination address (DA)**, 135**detecting**

controller failures, 274

interference

AQI, 443-444*channel quality*, 439*CleanAir*, 439-442*ED-RRM*, 445*spectrum analyzers*, 436-438**devices**

802.11, 432

Android, 395-396

available networks, displaying, 395*connections, verifying*, 396*manually adding networks*, 395*security*, 396

Apple iOS, 400

available networks, displaying, 401*connection information*, 402*security*, 402*Wi-Fi settings, accessing*, 400

interference

Bluetooth, 432-433*canopy*, 435*channel quality*, 439*continuous transmitters*, 435*cordless phones*, 434*detecting with AQI*, 443-444

- detecting with CleanAir*, 439-442
- detecting with ED-RRM*, 445
- detecting with spectrum analyzers*, 436-438
- invalid channels*, 435
- inverted signals*, 435
- jammers*, 435
- microwave ovens*, 434
- SuperAG*, 435
- video cameras*, 435
- WiMAX*, 434
- Xbox*, 435
- ZigBee*, 433
- location services, 170
- MacOS X, 397
 - configuration utility, accessing*, 397
 - discovered networks, displaying*, 397
 - new network profiles, creating*, 399
 - preferred networks list, displaying*, 398
 - system information, displaying*, 399
- PI
 - configuration*, 426
 - maps, selecting*, 422
- power, saving, 147-150
 - DTIMs*, 149
 - legacy method*, 147
 - radio sleeping*, 147
 - U-APSD method*, 149
 - whole device sleeping*, 147
- transmission requirements, 138
- Windows, 389-390
 - ad hoc networks*, 391
 - adapter settings*, 392
 - available SSIDs*, 389
 - connections, verifying*, 393
 - drivers*, 394
 - manually configuring*, 391
 - preferred networks list, manually populating*, 391
 - wireless status icon, finding*, 389
- wireless requirements, 169-170
- DFS (dynamic frequency selection), 44
- DHCP_REQD state, 455
- differential binary phase shift keying (DBPSK), 28
- differential quadrature phase shift keying (DQPSK), 28
- diffraction, 84
- DIFS (distributed interframe space), 138
- digital certificates, 194
- Digital Enhanced Cordless Telecommunications (DECT), 434
- dipole antennas, 100-101
- direct-sequence spread spectrum. *See* DSSS
- directional antennas, 103
 - parabolic dish, 105-106
 - patch, 103-104
 - Yagi, 104-105
- disabled state, 142
- disabling
 - data rates, 309
 - lower data rates, 160
 - WLANs, 362
- disassociating
 - BSSs, leaving, 145
 - frames, 141
- discovery
 - controllers
 - AP states*, 268-270
 - failures, detecting*, 274

- multiple*, 272-273
 - redundancy*, 274-278
 - WLCs*, 270-271
 - RF groups, 313
 - displaying**
 - alarm summary, 417
 - AP information on PI maps, 424
 - available networks
 - Android devices*, 395
 - iOS devices*, 401
 - MacOS X*, 397
 - clients
 - locations*, 424, 457
 - mobility details*, 456
 - PI*, 454-455
 - status*, 461
 - controller logs, 463
 - interference sources on PI maps, 425
 - MacOS X system information, 399
 - PI maps, 423
 - WLANs
 - controller configured*, 366
 - list*, 360
 - distributed architectures**
 - autonomous, 187-190
 - data paths*, 188
 - data VLAN*, 189
 - management IP addresses*, 189
 - single autonomous APs, supporting*, 188
 - cloud-based, 190-191
 - distributed coordination function (DCF)**, 136
 - distributed interframe space (DIFS)**, 138
 - distribution systems**. *See* DSs
 - domains**, 242, 302
 - DQPSK (differential quadrature phase shift keying)**, 28
 - drag-and-drop questions**, 477-479
 - drivers, verifying**, 394
 - DRS (dynamic rate shifting)**, 79, 160
 - DSs (distribution systems)**, 118-120
 - 802.11 frames, moving to/from, 133
 - 802.11 frames, not moving to/from, 134
 - ports, 235-236
 - DSSS (direct-sequence spread spectrum)**, 27-30
 - 1-Mbps data rate, 28
 - 2-Mbps data rate, 28
 - 5.5-Mbps data rate, 29-30
 - 11-Mbps data rate, 30
 - DTIM (delivery traffic indication message)**, 149
 - duty cycles**, 436, 442
 - DVD questions**. *See* exam engine
 - dynamic channel allocation**. *See* DCA
 - dynamic frequency selection (DFS)**, 44
 - dynamic interfaces**
 - controllers, 238
 - creating, 358-360
 - guest WLANs, 377
 - dynamic rate shifting (DRS)**, 79, 160
-
- E**
- E (elevation) planes**, 96
 - EAP (Extensible Authentication Protocol)**, 338-339
 - 802.1x integration, 338
 - EAP-FAST, 339-340
 - EAP-TLS, 340
 - LEAP, 339

- Local, configuring, 348-350
 - enabling*, 350
 - PEAP configuration*, 349
 - profiles*, 348
 - RADIUS servers*, 349
 - WLANs*, 349
 - PEAP, 340
 - EAP-FAST (EAP Flexible Authentication by Secure Tunneling), 339-340
 - EAP-TLS (EAP Transport Layer Security), 340
 - Easy Setup page (APs), 218-219
 - ED-RRM (Event-Driven RRM), 320, 445
 - EIFS (extended interframe space), 138
 - EIRP (effective isotropic radiated power), 21-22, 43
 - electric waves, traveling, 8
 - elevation (E) planes, 96
 - email notification alarms, 419
 - enabling
 - 802.11 converged WLCs, 252
 - CleanAir, 440
 - ED-RRM, 445
 - Local EAP authentication, 350
 - radios, 220
 - WLANs, 362
 - encryption, 333
 - enterprise mode (WPA2), 346-348
 - enterprise with Local EAP mode (WPA2), 348-350
 - enabling, 350
 - PEAP configuration, 349
 - profiles, 348
 - RADIUS servers, 349
 - WLANs, 349
 - equations
 - dB, 17
 - free space path loss, 78
 - ESS (extended service set), 120-121
 - APs, adding
 - channel layout*, 165-168
 - client associations*, 162-163
 - roaming*, 163-165
 - predictive surveys, 173
 - ETSI (European Telecommunication Standards Institute), 44
 - Event-Driven RRM (ED-RRM), 320, 445
 - Event Log tab, 221
 - exam engine, 482
 - activating, 483
 - installing, 482
 - modes, 484
 - new exams, activating, 483
 - Premium Edition, 484
 - updating, 483
 - exam event advice
 - pre-exam suggestions, 481-482
 - question types, learning, 475-479
 - time budget, 480-481
 - extended bands, 44
 - extended interframe space (EIFS), 138
 - extended service set. *See* ESS
 - Extensible Authentication Protocol. *See* EAP
-
- F**
- failures
 - controllers, 274
 - transmission, 139
 - fake APs, 333
 - FCC (Federal Communication Commission), 42
 - 5-GHz U-NII bands requirements, 44

- DFS, 44
 - power, 43
 - transmitting equipment, 43
 - U-NII frequency space, 42
 - website, 42
 - FHSS (frequency-hopping spread spectrum), 26**
 - fill in the blank questions, 477**
 - filtering client status information, 461**
 - finding**
 - autonomous AP IP addresses, 216
 - wireless status icon (Windows devices), 389
 - FlexConnect, 204-205**
 - Fluke AirMagnet WiFi Analyzer, 469**
 - foreign controllers, 295**
 - foundation module (CCX), 404**
 - frames**
 - 802.11
 - 802.3 frames, compared, 132*
 - addressing, 134-135*
 - control, 141-142*
 - CSMA, 137*
 - data, 142*
 - format, 133*
 - management, 140-141*
 - moving to/from DSs, 133*
 - not moving to/from DSs, 134*
 - timing schemes, 138*
 - transmission failures, 139*
 - aggregation, 63
 - direction bits, 135
 - management, 343-344
 - transmissions, 63
 - Wi-Fi, 470
 - free space path loss, 77**
 - 2.4-GHz versus 5-GHz bands, 78
 - calculating, 78
 - solutions, 79-80
 - wave spreading, 77
 - frequency, 9**
 - 5-GHz band, 11
 - bands, 10
 - 2.4-GHz band, 10*
 - 5-GHz band, 11*
 - channels, 12-13*
 - dynamic selection, 44
 - hertz, 10
 - ISM (industrial, scientific, and medical), 42
 - radio (RF), 10
 - signal bandwidth, 12
 - spectrum, 10
 - U-NII, 42
 - unit names, 10
 - frequency-hopping spread spectrum (FHSS), 26**
 - Fresnel zones, 85-86**
- ## G
-
- gain**
 - antennas, 97
 - increasing, 107
 - Generic Token Cards (GTCs), 340**
 - GHz (gigahertz), 10**
 - GI (guard interval), 58**
 - groups**
 - mobility, 296-298
 - RF, 313-315
 - automatic discovery/formation, 313*
 - information, displaying, 314*
 - leaders, 314*
 - radio resource monitoring, 315*
 - SPGs, 302

GTC (Generic Token Card), 340

guard interval (GI), 58

guest users, 374

guest WLANs

configuring

dynamic interface, 377

interface, assigning, 378

IP address information, 377

mobility anchors, 380-381

open authentication, 379

SSID, 378

web authentication, 379

isolation, 375

Layer 3 roaming, 376

mobility anchors, 376

scaling, 375-376

web authentication, 375

GUI, 220

H

H (horizontal) planes, 96

H-REAP (Hybrid Remote Edge Access Point), 204-205

hardware (Cisco)

APs, 206-207

controllers, 205-206

LAPs, 207-208

heartbeat messages, 274

heatmaps

active site surveys, 177-178

passive site surveys, 175

PI computation, 423-424

hertz (Hz), 10

hierarchy

mobility, 300-301

mobility groups, 297

high throughput (HT), 54

holes (coverage), 321

home page (PI), 415

horizontal (H) planes, 96

HT (high throughput), 54

Hz (hertz), 10

I

IBSS (independent basic service set), 122, 391

Identity Services Engine (ISE), 413

ID numbers (WLANs), 361

IDSs (intrusion detection systems), 335

IEEE (Institute of Electric and Electronic Engineers), 45

802.1x, 338

802.11. *See* 802.11 standards

amendments, 46

website, 45

working groups, 45

independent basic service set (IBSS), 122, 391

industrial, scientific, and medical (ISM) frequencies, 42

infrastructure MFP, 343

infrastructure mode, 116

initial setup

centralized controllers with CLI, 257

centralized controllers with Configuration Wizard, 239-247

802.11 support, 245

LAG mode, 241

management interface, 241

RADIUS server, 244

rebooting, 246

RF mobility domain, 242

service port, 240

- SNMP access, 240
- system access, 239
- system clock, 246
- virtual interface, 243
- WLAN, 243
- centralized controllers with WLAN Express Setup, 254
 - controller identification, 254
 - starting, 254
 - verifying, 256
 - VLAN/IP address parameters, 256
 - WLANs, 255
- converged controllers with Configuration Wizard, 247-253
 - 802.11, 252
 - administrative users, creating, 249
 - clock, 253
 - management ports, 250
 - mobility, 251
 - RF mobility, 251
 - SNMP parameters, 249
 - switch management web page, 247
 - verifying, 253
 - web-based management switch configuration, 247
 - wireless management, 250
 - WLAN, 252
 - WLC management page, 248
- initialization vector (IV), 341
- installing, exam engine, 482
- Institute of Electric and Electronic Engineers. *See* IEEE
- integrated omnidirectional antennas, 101-102
- integrity, 334, 341-342
- intercontroller roaming
 - Layer 2, 290-292
 - Layer 3, 292-296
 - after, 293
 - before, 292
 - clients details on anchor controller, displaying, 295
 - clients details on foreign controllers, displaying, 295
 - clients, displaying, 294
 - mobility groups, 296-298
- interfaces
 - BVI, 217
 - controllers, 237-238, 362
 - dynamic, 358-360
 - converged controllers, 358-360
 - guest WLANs, 377
 - name/VLAN ID, defining, 358
 - parameters, editing, 358
 - guest WLANs, assigning, 378
 - management, 241
 - ports, compared, 235
 - virtual, 243
 - web, 217
- interference
 - 802.11 devices, 432
 - Bluetooth, 432-433
 - canopy, 435
 - channel quality information, 439
 - co-channel, 74-75
 - continuous transmitters, 435
 - cordless phones, 434
 - detecting
 - AQI, 443-444
 - CleanAir, 439-442
 - ED-RRM, 445
 - spectrum analyzers, 436-438

- invalid channels, 435
- inverted signals, 435
- jammers, 435
- microwave ovens, 434
- neighboring channel, 75-76
- noise, 432
- non-802.11 devices, 76
- rogue APs, 432
- simultaneous transmissions, 115
- sources, 425, 432
- SuperAG, 435
- video cameras, 435
- WiMAX, 434
- Xbox, 435
- ZigBee, 433
- Interference Optimal Mode (TPCv2), 316**
- interframe space periods, 138
- interleavers, 27
- International Telecommunication Union Radiocommunication Sector (ITU-R), 41**
- intersymbol interference (ISI), 58
- intracontroller roaming, 288-290
- intrusion detection systems (IDSs), 335
- intrusion protection, 335-336
 - attacks, detecting, 336
 - IDSs, 335
 - PI, 335
 - rogue APs, 335-336
 - WLCs, 197
- invalid channel interference, 435
- inverted signals, 435
- iOS devices, 400
 - available networks, displaying, 401
 - connection information, 402
 - security, 402
 - Wi-Fi settings, accessing, 400

- IP addresses**
 - attacks, detecting, 336
 - autonomous APs, finding, 216
 - centralized controller parameters, 256
 - client problems, troubleshooting, 458
 - guest WLANs, 377
 - management, 189
- ISE (Identity Services Engine), 413**
- ISI (intersymbol interference), 58**
- ISM (industrial, scientific, and medical) frequencies, 42**
- isotropic antennas radiation patterns, 21**
 - cutting with two planes, 95
 - H/E polar plots, recording, 96
 - plotting, 94
- ITU-R (International Telecommunication Union Radiocommunication Sector), 41**
- IVs (initialization vectors), 341**

J

- jammer interference, 435
- jitter, 389
- joining BSSs, 144-145

K

- keepalive messages, 274**
- keys**
 - caching, 290
 - exchanges, 290
 - mixing algorithm, 341
 - PKIs, 341
 - shared-key security, 337
 - TKIP, 341-342
 - WEP, 337
- kHz (kilohertz), 10**

L

L2AUTHCOMPLETE state, 455

labels (PI maps), 422

LAG (link aggregation group), 236, 241

lambda symbol (Λ), 14

LAP (lightweight access point), 193

- autonomous, compared, 192
- central WLC, connecting, 195
- Cisco, 207-208
- client load balancing, 196
- client roaming, 196
- RTT controllers, 199
- self-healing coverage, 196
- WLCs, linking, 193

latency, 388

law of 3s (dB), 18

law of 10s, 18

law of zero (dB), 18

Layer 2 roaming, 290-292

Layer 2 WLAN security types, 362-363

Layer 3 roaming, 292-296

- after, 293
- before, 292
- client details on anchor controller, displaying, 295
- client details on foreign controller, displaying, 295
- clients, displaying, 294
- guest WLANs, 376

layout

APs, 311

channels, 165-168

- alternating pattern holes*, 166
- channel reuse*, 167
- honeycomb pattern*, 167
- three dimensions*, 168

LEAP (Lightweight EAP), 339

leaving BSSs, 145-146

legacy power saves, 147

licenses, 41-42

lightning arrestors, 108

lightweight access point. *See* LAP

Lightweight Access Point Protocol (LWAPP), 194

line-of-sight paths, 85

links

- adaptation, 79, 160
- aggregation group, 236, 241
- budgets, 22

load balancing, 196

Local EAP, 348-350

local-to-local roams, 290-292

local web authentication (LWA), 375

locations

- centralized WLCs, 197
- clients
 - AP associations*, 458
 - displaying*, 457
 - PI maps*, 424
- devices/applications, 170
- module (CCX), 404
- WLCs, 201

log₁₀ (base-10 logarithm), 17

logging in (PI), 414

logical networks, 355

logs, 463

LWA (local web authentication), 375

LWAPP (Lightweight Access Point Protocol), 194

M

MA (Mobility Agent), 298

MAC (media access control), 192

Counter/CBC-MAC Protocol
(CCMP), 342

layers

802.11ac, 63

802.11n, 58

pseudo addresses, 442

sender MAC addresses, 341

split-MAC architectures, 192-197

CAPWAP, 193

centralized, 197-200

converged, 200-202

digital certificates, 194

FlexConnect, 204-205

LAPs to central WLC, connecting, 195

VLAN 100, 194

WLC activities, 196

MacOS X devices, 397

configuration utility, accessing, 397

discovered networks, displaying, 397

new network profiles, creating, 399

preferred networks list, displaying,
398

system information, displaying, 399

magnetic waves, traveling, 8**major alarms, 417****man-in-the-middle attacks, 333****management**

alarms, 418

frames, 140-141, 343-344

interfaces, 237, 241

IP addresses, 189

module (CCX), 404

ports, 250

WLANs, allowing, 367

**Management Frame Protection (MFP),
343, 403****Management tab, 221****mandatory data rates, 309****mandatory state, 142****mapping VLANs, 237****maps (PI), 421**

accessing, 421

AP

information, 424

locations, 421

building example, 421

client locations, 424

devices/labels, selecting, 422

display settings, 423

heatmap computation, 423-424

interference sources, 425

rogue APs/clients, 426

RRM results, 323

maximal-ratio combining (MRC), 60**MC (Mobility Controller), 298****MCS (modulation and coding scheme),
60, 63****media access control. *See* MAC****megahertz (MHz), 10****Meraki, 190, 438****Meraki Dashboard**

accessing, 224

tabs, 227

mesh networks, 125**messages**

integrity, 334, 341

keepalive, 274

logs, 463

privacy/integrity methods, 333-334,
341-342

sending, 8-9

MetaGeek Chanalyzer, 172, 437**MetaGeek in SSIDer Office tool, 468****MFP (Management Frame Protection),
343, 403**

- MHz (megahertz), 10
- MIC (message integrity check), 334, 341
- Microsoft Challenge Authentication Protocol version 2 (MSCHAPv2), 340
- microwave oven interference, 434
- MIMO (multiple-input, multiple-output), 55-57
- minor alarms, 417
- mobility
 - agents, 298
 - anchors, 376, 380-381
 - client details, displaying, 456
 - controllers (MCs), 298
 - converged WLCs, 251
 - domains/subdomains, 302
 - groups, 296-298
 - hierarchy, 300-301
 - RF
 - converged WLCs*, 251
 - mobility domain*, 242
 - Services Engine (MSE), 208, 412
 - users
 - centralized architectures*, 198
 - converged architectures*, 202
- modulation, 25
 - 802.11ac, 63
 - 802.11n, 60
 - bandwidth, 25
 - coding scheme (MCS), 60, 63
 - DSSS, 27-28
 - 1-Mbps data rate*, 28
 - 2-Mbps data rate*, 28
 - 5.5-Mbps data rate*, 29-30
 - 11-Mbps data rate*, 30
 - FHSS, 26
 - goals, 25
 - OFDM, 30-32
 - spread spectrum, 26
 - summary, 32-33
- modulators, 27
- monitoring
 - alarms, 417
 - actions*, 419
 - browsing*, 418
 - managing*, 418
 - severity levels*, 417
 - summary*, 417
 - AP/client counts, 419
 - PI maps, 421
 - accessing*, 421
 - AP information*, 424
 - AP locations*, 421
 - building example*, 421
 - client locations*, 424
 - devices/labels, selecting*, 422
 - display settings*, 423
 - heatmap computation*, 423-424
 - interference sources*, 425
 - rogue APs/clients*, 426
 - RF, 196
 - tasks, 420
- monopole antennas, 101
- MRC (maximal-ratio combining), 60
- MSCHAPv2 (Microsoft Challenge Authentication Protocol version 2), 340
- MSE (Mobility Services Engine), 208, 412
- MU-MIMO (multi-user MIMO), 65
- multipath transmissions, 81-82
- multiple choice questions, 476-479
- multiple-input, multiple-output (MIMO), 55-57

N

- N+1 redundancy, 274-275
- N+N redundancy, 275-276
- N+N+1 redundancy, 276-277
- names
 - 802.11 standards, 46
 - dynamic interfaces, defining, 358
 - WLANs, 361
- narrowband transmissions, 25
- NAV (network allocation vector) timer, 137
- NDP (Null Data Packet), 64
- Near Field Communication (NFC), 436
- neighboring channel interference, 75-76
- Network and Sharing Center (Windows), 391
- Network tab, 221
- Network-wide tab (Meraki Dashboard), 227
- NFC (Near Field Communication), 436
- noise, 23, 432
- non-802.11 device interference, 76
- non-real-time applications, 388
- non-root bridges, 219
- Null Data Packets (NDPs), 64

O

- OFDM (orthogonal frequency-division multiplexing), 30-32
- omnidirectional antennas, 99
 - dipole, 100-101
 - integrated, 101-102
 - monopole, 101
- One Management, 412
- One Network, 412

- One Policy, 412
- open authentication, 336, 379
- Open System authentication, 140
- optimizing
 - autonomous APs, 220
 - transmit power, 196
- Organization tab (Meraki Dashboard), 227
- orthogonal frequency-division multiplexing (OFDM), 30-32
- outdoor bridges, 124
- overriding RRM, 322

P

- packets
 - analyzers, 470
 - loss, 389
- PACs (protected access credentials), 339
- parabolic dish antennas, 105-106
- parameters
 - CHDM, 321
 - controller wireless, 308
 - DCA, 319
 - dynamic interfaces, editing, 358
 - RRM TPC, configuring, 316
 - SNMP converged WLC, 249
 - WLANs
 - broadcasting SSIDs, 362*
 - controller interfaces, 362*
 - enabling/disabling, 362*
 - general, 361*
 - radio selection, 362*
- passing through (communications), 117
- passive scanning, 140, 143
- passive site surveys, 171, 174-175
- patch antennas, 103-104

PEAP (Protected EAP), 340, 349

Pearson Cert Practice Test engine, 482

- activating, 483
- installing, 482
- modes, 484
- new exams, activating, 483
- Premium Edition, 484
- updating, 483

performance verification

- active site surveys, 176-178
- AP deployment phases, 178-179
- AP-on-a-stick surveys, 175
- device/application requirements, 169-170
- location services, 170
- passive site surveys, 174-175
- planning surveys, 172-173
- site surveys, 171-172

personal mode (WPA2), 344-345

physical carrier sense, 137

physical objects effects on RF signals

- absorption, 82-83
- diffraction, 84
- earth curvature, 85
- Fresnel zones, 85-86
- line-of-sight paths, 85
- reflection, 81-82
- refraction, 83
- scattering, 83
- standing obstacle diffraction, 84

PI (Prime Infrastructure), 335, 412

- alarms, 417
 - actions, 419*
 - browsing, 418*
 - managing, 418*
 - severity levels, 417*
 - summary, displaying, 417*

benefits, 414

dashlets, 416

defined, 412

devices, configuring, 426

home page, 415

intrusion protection system, 335

login screen, 414

maps, 421

accessing, 421

AP information, 424

AP locations, 421

building example, 421

client locations, 424

devices/labels, selecting, 422

display settings, 423

heatmap computation, 423-424

interference sources, 425

rogue APs/clients, 426

monitoring

AP/client counts, 419

tasks, 420

rogue APs, 335-336

Task Area, 415

testing clients, 459-460

troubleshooting clients, 454

AP associations, 458

details, displaying, 455

displaying clients, 454

IP addressing problems, 458

location, 457

mobility details, 456

policy states, 455

RF history, 457

RF problems, 458

RF statistics, 456

RSSI/SNR problems, 459

searching for clients, 454

- piconets, 433**
- ping round-trip times measured, displaying, 177**
- PKI (Public Key Infrastructure), 341**
- planning surveys, 171-173**
- PMF (Protected Management Frames), 344**
- PoA (Point of Attachment), 299**
- PoE (Power over Ethernet), 465**
- point-to-multipoint**
 - links, 44
 - outdoor bridges, 124
- point-to-point**
 - links, 44
 - outdoor bridges, 124
- polar plots, 96**
- polarization, 98-99**
- policies, 365**
- PoP (Point of Presence), 299**
- ports**
 - autonomous APs, availability, 215
 - controllers, 235-236
 - interfaces, compared, 235
 - management, 250
 - service, 240
 - switch, 466
- post-deployment site surveys, 179**
- power**
 - asymmetric power problems, 158
 - changes along path, measuring, 20-23
 - dB, 17-18
 - EIRP, 21-22
 - FCC regulations, 43
 - levels, comparing, 18
 - link budgets, 22
 - received signal strength, calculating, 22
 - receivers, 23-24
 - references, comparing, 19-20
 - saving, 147-150
 - DTIMs, 149*
 - legacy method, 147*
 - radio sleeping, 147*
 - U-APSD method, 149*
 - whole device sleeping, 147*
 - signals, 17
 - absolute, 16*
 - reducing, 108*
 - transmitters, comparing, 16*
 - watts, 16*
 - transmit
 - AP cell size, tuning, 157-159*
 - APs, setting manually, 323*
 - optimizing, 196*
 - RRM TPC algorithm, 317*
- Power over Ethernet (PoE), 465**
- Power Save Poll (PS-Poll), 141**
- Practice exam mode (exam engine), 484**
- pre-deployment site surveys, 179**
- predictive surveys, 171-173**
- pre-exam suggestions, 481-482**
- Prime Infrastructure. *See* PI**
- primed addresses, 271**
- privacy**
 - CCMP, 342
 - data, 333-334
 - TKIP, 341-342
- probes, 140**
- protected access credentials (PAC), 339**
- Protected EAP (PEAP), 340**
- Protected Management Frames (PMF), 344**
- protection**
 - 802.11g devices, 52

antennas from lightning, 108
 integrity, 334
 intrusion, 335-336
 attacks, detecting, 336
 IDSs, 335
 PI, 335
 rogue APs, 335-336
 WLCs, 197
 management frames, 343-344
 privacy, 333-334
protocols
 802.11, 68
 CAPWAP
 Discovery Requests, 270
 Join Requests, 271
 LAPs/WLCs, linking, 193
 CCMP, 342
 CDP, 216
 EAP. *See* EAP
 LWAPP, 194
 TKIP, 341-342
 PS-Poll (Power Save Poll) frames, 141
 pseudo-MAC addresses, 442
 Public Key Infrastructure (PKI), 341

Q

QAM (quadrature amplitude modulation), 31
 QoS (Quality of Service), 364-365
 question types, learning, 475
 drag-and-drop, 477-479
 fill in the blank, 477
 multiple choice, 476-479
 simlets, 478-479
 simulation, 478-479
 testlets, 478-479

R

RA (receiver address), 135
radiation patterns
 antennas, 94-97
 cutting with two planes, 95
 H/E polar plots, recording, 96
 plotting, 94
 dipole antennas, 100
 integrated omnidirectional antennas, 102
 parabolic dish antennas, 106
 patch antennas, 104
 Yagi antennas, 105
radios
 frequency. *See* RF
 Resource Management. *See* RRM
 resource monitoring, 315
 sleeping, 147
 WLANs, selecting, 362
RADIUS servers
 centralized controllers, configuring, 244
 client authentication, selecting, 347
 configuring, 356-357
 Local EAP configuration, 349
 WLAN authentication, 363
 WPA2 enterprise authentication, 346
 rate adaptation, 79, 160
 RC4 cipher algorithm, 337
 real-time applications, 388
 real-time location services (RTLS), 170
 reassociation frames, 141
 rebooting controllers, 246, 261
 received signal strength indicator (RSSI), 23-24, 389

receivers

- addresses, 135
- bidirectional communication, 115
- power, 23-24
- unidirectional communication, 115

reduced interframe space (RIFS), 138**redundancy, 274**

- N+1, 274-275
- N+N, 275-276
- N+N+1, 276-277
- ports, 235
- SSO, 277-278

reflection, 81-82**refraction, 83****regulatory agencies**

- ETSI, 44
- FCC, 42
 - 5-GHz U-NII bands requirements, 44*
 - DFS, 44*
 - power, 43*
 - transmitting equipment, 43*
 - U-NII frequency space, 42*
 - website, 42*

ITU-R, 41

regulatory domains, 45**repeaters, 122-123, 219****requirements**

- client wireless, 388-389
- devices/applications wireless, 169-170
- open authentication, 336
- transmissions, 138

reusing channels, 167**reverse polarity TNC (RP-TNC) connectors, 43****RF (radio frequency), 10**

- amplitude, 15

clients

- history, displaying, 457*
- problems, troubleshooting, 458*
- statistics, 456*

coverage. *See* coverage

duty cycle, 436, 442

free space path loss, 77

- 2.4-GHz versus 5-GHz bands, 78*
- calculating, 78*
- solutions, 79-80*
- wave spreading, 77*

groups, 313-315

- automatic discovery/formation, 313*
- information, displaying, 314*
- leaders, 314*
- radio resource monitoring, 315*

mobility

- converged WLCs, 251*
- domain, configuring, 242*

monitoring, 196

phases, 14

physical object effects

- absorption, 82-83*
- diffraction, 84*
- earth curvature, 85*
- Fresnel zones, 85-86*
- line-of-sight paths, 85*
- reflection, 81-82*
- refraction, 83*
- scattering, 83*
- standing obstacle diffraction, 84*

power, 17

- absolute, 16*
- changes along path, measuring, 20-23*
- dB, 17-18*

- EIRP*, 21-22
 - link budgets*, 22
 - received signal strength, calculating*, 22
 - receivers*, 23-24
 - references, comparing*, 19-20
 - transmitters, comparing*, 16
 - watts*, 16
 - regulatory agencies
 - ETSI, 44
 - FCC, 42-44
 - ITU-R, 41
 - regulatory domains, 45
 - signals. *See* signals
 - RIFS (reduced interframe space), 138
 - roaming
 - autonomous APs, 285-286
 - between BSSs, 146
 - centralized controller coordination, 298-300
 - channel layout, 165
 - alternating pattern holes*, 166
 - channel reuse*, 167
 - honeycomb pattern*, 167
 - three dimensions*, 168
 - clients, 163-165
 - behaviors, displaying*, 178
 - cell overlap*, 165
 - cloud-based APs*, 227
 - conditions*, 164
 - correctly between APs*, 164
 - flexibility*, 196
 - scanning other channels*, 165
 - converged controllers, 301
 - defined, 121, 162
 - guest WLANs, 376
 - intercontroller
 - Layer 2*, 290-292
 - Layer 3*, 292-296
 - intracontroller, 288-290
 - mobility groups, 296-298
 - WCMS, 300-302
 - rogue APs
 - detecting/containing, 335-336
 - interference, 432
 - PI maps, 426
 - rogue clients, 335, 426
 - root bridges, 219
 - round-trip time (RTT), 199
 - RP-TNC (reverse polarity-TNC), 43
 - RRM (Radio Resource Management), 313, 439
 - AP manual configuration, 322-323
 - CHDM algorithm, 321
 - DCA algorithm, 318-320
 - overriding, 322
 - results, verifying, 323
 - RF groups, 313-315
 - TPC algorithm, 315-317
 - RSSI (received signal strength indicator), 23-24, 389
 - client roaming, 164
 - client problems, troubleshooting, 459
 - RTLS (real-time location services), 170
 - RTS/CTS frames, 141
 - RTT (round-trip time), 199
 - RUN state, 455
- ## S
-
- SA (source address), 135
 - saving
 - power, 147-150
 - DTIMs*, 149

- legacy method*, 147
- radio sleeping*, 147
- U-APSD method*, 149
- whole device sleeping*, 147

Savvius OmniPeek, 470

scalability

- converged architectures, 202
- guest WLANs, 375-376
- mobility groups, 296-298

scanning

- active, 143
- APs, 143
- autonomous APs, 219
- channels
 - client roaming*, 165
 - tools*, 468
- passive, 140-143

scattering RF signals, 83

scramblers, 27

searching clients, 454

security

- alarms, 417
 - actions*, 419
 - browsing*, 418
 - managing*, 418
 - severity levels*, 417
 - summary, displaying*, 417

- Android devices, 396

attacks

- detecting*, 336
- man-in-the-middle*, 333
- protection against*, 335

authentication

- APs, 333
- central web*, 375
- clients*, 332
- local web*, 375
- open*, 379

- web*, 375, 379

- WLANs, 363

- WPA/WPA2, 343

- autonomous APs, 219

- CCX support, 404-405

- cloud-based APs, 226

- configuring, 344

- encryption/decryption, 333

- fake APs, 333

- guest WLANs, 379

- integrity/privacy, 333-334, 341-342

- intrusion protection, 335-336

- attacks, detecting*, 336

- IDSs*, 335

- PI*, 335

- rogue APs*, 335-336

- WLCs*, 197

- iOS devices, 402

- management frames, 343-344

- MICs, 334

- shared-key, 337

- transmissions reaching unintended recipients, 331

- WLANs, 362-364

- authentication*, 363

- centralized controllers*, 364

- client exclusion policies*, 365

- converged controllers*, 364

- Layer 2 types*, 362-363

- WLC authentication, 197

- WPA/WPA2, 342-343

- enterprise mode*, 346-348

- Local EAP*, 348-350

- personal mode*, 344-345

Security tab, 221

- self-healing coverage, 196

- sender MAC addresses, 341

sending

- data over RF signals, 24-26
- messages, 8-9

sensitivity levels, 23**sequence counters (TKIP), 341****server-based site survey tools, 171****servers**

- authentication (ASs), 339

RADIUS

- centralized controllers, configuring, 244*

- client authentication, selecting, 347*

- configuring, 356-357*

- Local EAP configuration, 349*

- WLAN authentication, 363*

- WPA2 enterprise authentication, 346*

service ports, 235-236, 238-240**service set identifiers. *See* SSIDs****Services tab, 221****session timeouts (WLANs), 365****shared key authentication, 140****shared-key security, 337****SIFS (short interframe space), 138****signal-to-noise ratio. *See* SNR****signals**

- amplitude, 15

- AP strength, displaying, 177

- bandwidth, 12

- carrier, 24

- free space path loss, 77

- 2.4-GHz versus 5-GHz bands, 78*

- calculating, 78*

- solutions, 79-80*

- wave spreading, 77*

- interference

- Bluetooth, 432-433*

- canopy, 435*

- channel quality, 439*

- co-channel, 74-75*

- continuous transmitter, 435*

- cordless phones, 434*

- detecting with AQI, 443-444*

- detecting with CleanAir, 439-442*

- detecting with ED-RRM, 445*

- detecting with spectrum analyzers, 436-438*

- invalid channels, 435*

- inverted signals, 435*

- jammers, 435*

- microwave ovens, 434*

- neighboring channel, 75-76*

- non-802.11 devices, 76*

- SuperAG, 435*

- video cameras, 435*

- WiMAX, 434*

- Xbox, 435*

- ZigBee, 433*

- inverted, 435*

- modulation/demodulation, 25-26*

- narrowband transmissions, 25*

- phases, 14*

- physical object effects*

- absorption, 82-83*

- diffraction, 84*

- earth curvature, 85*

- Fresnel zones, 85-86*

- line-of-sight paths, 85*

- reflection, 81-82*

- refraction, 83*

- scattering, 83*

- standing obstacle diffraction, 84*

- power, 17*

- absolute, 16*

- changes along path, measuring, 20-23*
- dB, 17-18*
- EIRP, 21-22*
- FCC regulations, 43*
- levels, comparing, 18*
- link budgets, 22*
- received signal strength, calculating, 22*
- receivers, 23-24*
- references, comparing, 19-20*
- transmitters, comparing, 16*
- watts, 16*
- sending messages, 8
- strength, reducing, 108
- waves
 - continuous pattern, 8*
 - cycles, 9*
 - electric/magnetic, traveling, 8*
 - electromagnetic, 9*
 - frequency, 9-13*
 - propagation with idealistic antenna, 9*
 - wavelength, 14*
- simlets questions, 478-479**
- simulation questions, 478-479**
- SISO (single-in, single-out), 55**
- site surveys, 171-172**
 - active, 176-178
 - AP signal strength, displaying, 177*
 - client roaming behaviors, 178*
 - methods, 176*
 - ping round-trip times measured, displaying, 177*
 - AP deployment phases, 178-179
 - AP-on-a-stick, 175
 - passive, 174-175
 - predictive, 172-173
 - review, 180
 - tools, 171
 - types, 171
- SNMP**
 - centralized controller access, configuring, 240
 - converged WLC parameters, 249
- SNR (signal-to-noise ratio), 24**
 - clients
 - problems, troubleshooting, 459*
 - RF statistics, 457*
 - roaming, 164*
 - co-channel interference, minimizing, 75
- Software tab, 221**
- source address (SA), 135**
- spacing channels, 13**
- spatial multiplexing**
 - 802.11ac, 64
 - 802.11n, 57-58
- spatial streams, 57**
- spectrum analyzers, 172**
 - AirMagnet, 437
 - interference detection, 436-438
- SPG (Switch Peer Group), 302**
- split-MAC architectures, 192-197**
 - CAPWAP, 193
 - centralized, 197-200
 - traffic paths, 198-199*
 - user mobility, 198*
 - WLC location, 197*
 - converged, 200-202
 - access switch capacities, 201*
 - scalability, 202*
 - traffic paths, 202*
 - user mobility, 202*
 - WLC location, 201*

- digital certificates, 194
 - FlexConnect, 204-205
 - LAPs to central WLC, connecting, 195
 - VLAN 100, 194
 - WLC activities, 196
 - spread spectrum, 26-28**
 - 1-Mbps data rate, 28*
 - 2-Mbps data rate, 28*
 - 5.5-Mbps data rate, 29-30*
 - 11-Mbps data rate, 30*
 - FHSS, 26
 - OFDM, 30-32
 - SSID (service set identifier), 117**
 - access, controlling, 226
 - active site surveys, 176
 - available, listing, 468
 - broadcasting, 362
 - cloud-based APs, configuring, 225-226
 - guest WLANs, 378
 - multiple on one AP, supporting, 119
 - VLANs, bridging, 214
 - Windows device availability, 389
 - SSO (stateful switchover), 277-278**
 - standalone site survey tools, 171**
 - standards**
 - 802.11. *See* 802.11 standards
 - regulatory agencies
 - ETSI, 44*
 - FCC, 42-44*
 - ITU-R, 41*
 - regulatory domains, 45
 - Wi-Fi Alliance, 66-67
 - START state, 455**
 - stateful switchover (SSO), 277-278**
 - states**
 - APs, 268-270
 - common sequence, 268*
 - data rates, 142*
 - machine, 268*
 - software image releases, 269*
 - client policy, displaying, 455
 - stations, 117**
 - status**
 - alarms, changing, 419
 - clients, 461
 - streams, 57**
 - Study mode (exam engine), 484**
 - subdomains mobility, 302**
 - SuperAG interference, 435**
 - supplicants, 339**
 - supported data rates, 309**
 - supported state, 142**
 - Switch Peer Group (SPG), 302**
 - switches**
 - access, 201
 - management web page, 247
 - ports, 466
 - web-based management configuration, 247
 - symbols, 27**
- ## T
-
- T×BF (transmit beamforming)**
 - 802.11ac, 64
 - 802.11n devices, 59-60
 - TA (transmitter address), 135**
 - tabs**
 - Association, 221
 - Event Log, 221
 - Management, 221
 - Meraki Dashboard, 227
 - Network, 221

- Security, 221
- Services, 221
- Software, 221
- Wireless, 221, 308
- Task Area (PI), 415**
- tasks, monitoring, 420**
- Temporal Key Integrity Protocol (TKIP), 341**
- testing clients (PI), 459-460**
- testlet questions, 478-479**
- third-party troubleshooting tools, 471**
- threaded Neill-Concelman (TNC) connectors, 43**
- TIM (traffic indication map), 148**
- time budget (exam event), 480-481**
- time stamps, 341**
- timeslots, 138**
- timing schemes, 138**
- TKIP (Temporal Key Integrity Protocol), 341-342**
- TNC (threaded Neill-Concelman) connectors, 43**
- tools**
 - MICs, 334
 - site surveys, 171
 - spectrum analyzers, 172
 - troubleshooting
 - activity analyzers, 469*
 - client-based OS, 468*
 - frame analyzers, 470*
 - third-party, 471*
 - Wi-Fi scanning, 468*
- topologies**
 - AP noninfrastructure modes
 - mesh networks, 125*
 - outdoor bridges, 124*
 - repeater, 122-123*
 - WGB, 123
 - WLANs
 - BSSs, 116-118*
 - DSSs, 118-120*
 - ESSs, 120-121*
 - IBSSs, 122*
- TPC (transmit power control), 315-317**
 - defined, 315
 - parameters, 316
 - RRM, 317
 - running, 317
 - transmit power, 317
 - versions, 316
- TPCv1 (Coverage Optimal Mode), 316**
- TPCv2 (Interference Optimal Mode), 316**
- traffic**
 - centralized architectures, 198-199
 - converged architectures, 202
 - FLexConnect, 204
 - flows, 117
 - indication maps, 148
 - untagged, 241
- transmissions**
 - bidirectional communication, 115
 - collision avoidance, 137-139
 - CSMA, 137
 - DSSS, 27
 - failures, 139
 - FHSS, 26
 - frame, 63
 - interference, 115
 - multipath, 81-82
 - narrowband, 25
 - power
 - APs, 157-159, 323*
 - control. See TPC*

- optimizing*, 196
 - RRM TPC algorithm*, 317
 - requirements, 138
 - timing schemes, 138
 - transmit beamforming, 64
 - types
 - IEEE 802.11-1997*, 51
 - IEEE 802.11a*, 53
 - IEEE 802.11b*, 51
 - IEEE 802.11g*, 52
 - unidirectional communication, 115
 - unintended recipients, 331
 - voice, 28
 - transmit beamforming**. *See* TxBF
 - transmitters**
 - addresses, 135
 - bidirectional communication, 115
 - ETSI requirements, 44
 - FCC regulations, 43
 - interference
 - co-channel*, 74-75
 - neighboring channel*, 75-76
 - non-802.11 devices*, 76
 - signal strength, reducing, 108
 - unidirectional communication, 115
 - trap logs**, 463
 - troubleshooting**
 - AP connectivity, 464
 - antenna orientation*, 467
 - AP orientation*, 467
 - AP-to-network, verifying*, 465-466
 - AP-to-WLC, verifying*, 464-465
 - asymmetric power problems, 158
 - client connectivity, 454
 - AP associations*, 458
 - client locations, displaying*, 457
 - controller logs, viewing*, 463
 - from controllers*, 461
 - device inspection*, 453
 - displaying clients in PI*, 454
 - information, gathering*, 453
 - IP addressing problems*, 458
 - mobility details*, 456
 - PI client searches*, 454
 - policy states*, 455
 - RF history*, 457
 - RF problems*, 458
 - RF statistics*, 456
 - RSSI/SNR problems*, 459
 - successful wireless association conditions*, 453
 - testing clients from PI*, 459-460
 - WLAN settings, verifying*, 462-463
 - frame transmission failures, 139
 - free space path loss, 79-80
 - tools
 - activity analyzers*, 469
 - client-based OS*, 468
 - frame analyzers*, 470
 - third-party*, 471
 - Wi-Fi scanning*, 468
 - tunneling**
 - LAPs to central WLC, connecting, 195
 - LAPs/WLCs, linking, 193
-
- U**
- U-APSD (unscheduled automatic power save delivery)**, 149
 - U-NII (Unlicensed National Information Infrastructure) frequency space**, 42, 49-50
 - unidirectional communication**, 115

Unified Access architecture, 412-413

**universal workgroup bridge (uWGB),
124, 219**

untagged traffic, 241

updating

autonomous APs, 221-223

controllers, 259-262

exam engine, 483

users

administrative, 249

guest, 374

mobility

centralized architectures, 198

converged architectures, 202

segregating into logical networks, 355

**uWGB (universal workgroup bridge),
124, 219**

V

verifying

Android connections, 396

AP connectivity

antenna orientation, 467

AP orientation, 467

AP-to-network, 465-466

AP-to-WLC, 464-465

centralized controller configuration,
256

client WLAN settings, 462-463

converged WLC configuration, 253

coverage/performance

active site surveys, 176-178

AP deployment phases, 178-179

AP-on-a-stick surveys, 175

*device/application requirements,
169-170*

location services, 170

passive site surveys, 174-175

planning surveys, 172-173

site surveys, 171-172

RRM results, 323

Windows

devices, 394

Wi-Fi connections, 393

VHT (very high throughput), 61

video camera interference, 435

virtual carrier sense, 137

virtual interfaces, 237, 243

VLANs

autonomous APs, 189

centralized controller parameters, 256

converged controllers, defining, 358

dynamic interface ID, defining, 358

mapping, 237

split-MAC architecture, 194

SSIDs, bridging, 214

voice

module (CCX), 404

transmissions, 28

W

W (watts), 16

wavelength, 14

waves

amplitude, 15

continuous pattern, 8

cycles, 9

electric/magnetic, 8

electromagnetic, 9

frequency, 9

2.4-GHz band, 10

5-GHz band, 11

bands, 10

- channels*, 12-13
- hertz*, 10
- radio (RF)*, 10
- signal bandwidth*, 12
- spectrum*, 10
- unit names*, 10
- propagation with idealistic antenna, 9
- spreading, 77
- wavelength, 14
- WCM (Wireless Controller Module)**, 201, 300
 - access switch capacities, 201
 - dynamic interfaces, creating, 358-360
 - initial setup with Configuration Wizard, 247, 253
 - 802.11, 252
 - administrative users, creating*, 249
 - clock*, 253
 - management ports*, 250
 - mobility*, 251
 - RF mobility*, 251
 - SNMP parameters*, 249
 - switch management web page*, 247
 - verifying*, 253
 - web-based management switch configuration*, 247
 - wireless management*, 250
 - WLAN*, 252
 - WLC management page*, 248
 - platforms/capabilities, 205-206
 - RADIUS servers, configuring, 357
 - roaming, 300-302
 - domains/subdomains*, 302
 - mobility hierarchy*, 300-301
 - SPGs*, 302
 - updating, 262
 - WLAN security, 364
- web-based management**, 247
- web interfaces**, 217
- WebAuth (web authentication)**, 336, 375, 379
- WEBAUTH_REQD state**, 455
- websites**
 - AirMagnet Spectrum XT, 172
 - Bluetooth SIG, 433
 - Cisco antennas, 99
 - Cisco Learning Network*, 485
 - ETSI, 44
 - FCC, 42
 - IEEE, 45
 - ITU-R, 41
 - Meraki Dashboard, 224
 - MetaGeek Chanalyzer, 172
 - Wi-Fi Alliance, 66
 - WiMAX Forum, 435
 - ZigBee Alliance, 434
- WEP (Wired Equivalent Privacy)**, 337-338
- WEP_REQD**, 455
- WGB (workgroup bridge)**, 123, 219
- whole device sleeping**, 147
- Wi-Fi**
 - Alliance, 66-67
 - Analyzer, 469
 - Android clients, 395-396
 - available networks, displaying*, 395
 - connections, verifying*, 396
 - manually adding networks*, 395
 - security*, 396
 - Apple iOS clients, 400-402
 - available networks, displaying*, 401

- connection information*, 402
- security*, 402
- Wi-Fi settings, accessing*, 400
- Direct, 396
- MacOS X clients, 397
 - configuration utility, accessing*, 397
 - discovered networks, displaying*, 397
 - new network profiles, creating*, 399
 - preferred networks list, displaying*, 398
 - system information, displaying*, 399
- Multimedia (WMM), 149
- Protected Access (WPA), 342-343
- scanning tools, 468
- Windows clients, 389-390
 - ad hoc networks*, 391
 - adapter settings*, 392
 - available SSIDs*, 389
 - connections, verifying*, 393
 - drivers*, 394
 - manually configuring*, 391
 - preferred networks list, manually populating*, 391
 - wireless status icon, finding*, 389
- WiMAX (Worldwide Interoperability for Microwave Access) interference, 434
- Windows devices, 389-390
 - ad hoc networks*, 391
 - adapter settings*, 392
 - available SSIDs*, 389
 - connections, verifying*, 393
 - drivers*, 394
 - manually configuring*, 391
 - preferred networks list, manually populating*, 391
 - wireless status icon, finding*, 389
- preferred networks list, manually populating, 391
- wireless status icon, finding, 389
- wIPS (wireless intrusion protection system)**, 335-336
- Wired Equivalent Privacy (WEP)**, 337-338
- wired networks**, 7
- Wireless**
 - Controller Modules. *See* WCM
 - intrusion protection system (wIPS), 335-336
 - LAN controllers. *See* WLC
 - local-area networks. *See* WLAN
 - mediums, accessing
 - carrier sense multiple access*, 137
 - collision avoidance*, 137-139
 - timing schemes*, 138
 - transmission failures*, 139
 - metropolitan-area networks (WMANs)*, 114
 - personal-area networks (WPANs)*, 114
 - status icon (Windows devices)*, 389
 - wide-area networks (WWANs)*, 114
- Wireless tab**, 221, 227, 308
- Wireshark**, 470
- WLAN (wireless local-area network)**, 114
 - advanced settings, 365-366
 - authentication, 346
 - centralized controllers, configuring, 243
 - channel layout, 165-168
 - alternating pattern holes*, 166
 - channel reuse*, 167

- honeycomb pattern*, 167
- three dimensions*, 168
- clients
 - session timeouts*, 365
 - settings, verifying*, 462-463
- controller configured, displaying, 366
- converged WLCs, configuring, 252
- coverage/performance verification
 - active site surveys*, 176-178
 - AP deployment phases*, 178-179
 - AP-on-a-stick surveys*, 175
 - device/application requirements*, 169-170
 - location services*, 170
 - passive site surveys*, 174-175
 - planning surveys*, 172-173
 - site surveys*, 171-172
- defining, 355
- dynamic interface, creating, 358-360
- Express Setup, 254-256
- guest
 - dynamic interface*, 377
 - interface, assigning*, 378
 - IP address information*, 377
 - isolation*, 375
 - Layer 3 roaming*, 376
 - mobility anchors*, 376, 380-381
 - open authentication*, 379
 - scaling*, 375-376
 - SSID*, 378
 - web authentication*, 375, 379
- limiting, 356
- listing of, displaying, 360
- Local EAP, 349-350
- management access, allowing, 367
- new, creating
 - broadcasting SSIDs*, 362
 - controller interfaces*, 362
 - enabling/disabling*, 362
 - general parameters*, 361
 - names/ID numbers*, 361
 - radio selection*, 362
 - WLAN list, displaying*, 360
- open authentication, 336
- QoS, 364-365
- RADIUS server, configuring, 356-357
- security, 362-364
 - authentication*, 363
 - centralized controllers*, 364
 - client exclusion policies*, 365
 - configuring*, 344
 - converged controllers*, 364
 - Layer 2 types*, 362-363
- too many, creating, 355
- topologies
 - BSSs*, 116-118
 - distribution systems*, 118-120
 - ESSs*, 120-121
 - IBSSs*, 122
- user segregation into logical networks, 355
- WPA2, configuring
 - enterprise mode*, 346-348
 - Local EAP*, 348-350
 - personal mode*, 344-345
- WLC (wireless LAN controller), 193
 - activities, 196
 - centralized, 200
 - location*, 197
 - traffic paths*, 198-199
 - user mobility*, 198
 - client states, 455

Configuration wizard

802.11, 252

administrative users, creating, 249

clock, 253

management ports, 250

mobility, 251

RF mobility, 251

SNMP parameters, 249

starting, 248

verifying, 253

wireless management, 250

WLAN, 252

converged location, 201

discovery, 270-271

LAPs, linking, 193

LAPs to central WLC, connecting, 195

platforms/capabilities, 205-206

selecting, 271

WMAN (wireless metropolitan-area network), 114

WMM (Wi-Fi Multimedia), 149

working groups, 45

Worldwide interoperability for Microwave Access (WiMAX) interference, 434

WPA (Wi-Fi Protected Access), 342-343

WPA2 (WPA Version 2), 342-343

enterprise mode, 346-348

Local EAP, 348-350

personal mode, 344-345

WPAN (wireless personal-area network), 114

WWAN (wireless wide-area network), 114

X - Z

Xbox interference, 435

Yagi antennas, 104-105

ZigBee Alliance, 434

ZigBee interference, 433