KEITH BARKER CCIE No. 6783
KEVIN WALLACE CCIE No. 7945

CompTIA Approved Quality Content

Cert Guide

Learn, prepare, and practice for exam success

CompTIA Network+®

N10-006

Save 10% on Exam Voucher

See Inside

Includes labs, videos, performance-based exercises, an exam voucher, and much more!

PEARSON IT CERTIFICATION

CompTIA® Network+ N10-006 Cert Guide

Keith Barker, CCIE No. 6783
Kevin Wallace, CCIE No. 7945

PEARSON

800 East 96th Street
Indianapolis, Indiana 46240 USA

CompTIA Network+ N10-006 Cert Guide

ISBN-13: 9780789754080
ISBN-10: 0789754088

Library of Congress Control Number: 2015930209

Printed in the United States on America

First Printing: February 2015

Associate Publisher
Dave Dusthimer

Executive Editor
Brett Bartow

Senior Development Editor
Christopher Cleveland

Managing Editor
Sandra Schroeder

Project Editor
Seth Kerney

Copy Editor
Keith Cline

Indexer
Tim Wright

Proofreader
Gill Editorial Services

Technical Editors
Michelle Plumb
Anthony Sequeria

Publishing Coordinator
Vanessa Evans

Multimedia Developer
Lisa Matthews

Book Designer
Mark Shirar

Composition
Trina Wurst

Contents at a Glance

Table of Contents

About the Authors

Keith Barker, CCIE No. 6783, has been working in the information technology (IT) industry since 1985. He currently enjoys creating effective and entertaining video training for CBT Nuggets. He has certified with VMware, Cisco, Juniper, HP, Check Point, Palo Alto, (ISC)2, and many others. Keith loves to teach. You can follow Keith online through the following:

Twitter: @KeithBarkerCCIE

Facebook: Keith Barker Networking

YouTube: http://youtube.com/Keith6783

Web page: http://cbtnuggets.com

Kevin Wallace, CCIE No. 7945 (R/S and Collaboration), is a Certified Cisco Systems Instructor (CCSI No. 20061) with multiple Cisco professional and associate-level certifications in the R/S, Collaboration, Security, Design, and Data Center tracks. With networking experience dating back to 1989, Kevin has been a network design specialist for the Walt Disney World Resort, an instructor of Cisco courses for Skillsoft, and a network manager for Eastern Kentucky University.

Currently, Kevin owns and operates Kevin Wallace Training, LLC, where he primarily produces video courses and writes books for Cisco Press/Pearson IT Certification (http://kwtrain.com/books).

Kevin holds a bachelor of science degree in electrical engineering from the University of Kentucky, and he lives in central Kentucky with his wife (Vivian) and two daughters (Stacie and Sabrina).

Kevin can be followed on these social media platforms:

Blog: http://kwtrain.com

Twitter: http://twitter.com/kwallaceccie

Facebook: http://facebook.com/kwallaceccie

YouTube: http://youtube.com/kwallaceccie

LinkedIn: http://linkedin.com/in/kwallaceccie

Google+: http://google.com/+KevinWallace

Dedication

Keith: *This book is dedicated to individuals from all backgrounds and experiences who are taking deliberate steps to improve their knowledge, life, and community. May you have measureable success in your journey!*

Kevin: *My contributions to this book are dedicated to you, the reader. The CompTIA Network+ certification can be your first step in a long and rewarding career in networking. May the concepts in this book fuel your passion for continuous learning.*

Acknowledgments

Keith Barker:

All the professionals at Pearson IT Certification have been fantastic to work with, including Brett Bartow and Christopher (Chris) Cleveland. Many thanks to all of Pearson IT.

CBT Nuggets has been very supportive of me in all my endeavors. I am grateful on a daily basis for the amazing opportunity that Dan Charbonneau and the CBT Nuggets team represents for both me and the learners around the globe who enjoy CBT Nuggets videos.

Thanks to longtime friend Kevin Wallace for allowing me to work with him on this latest version of book, and for Anthony and Michelle for their sweet tech edits.

Kevin Wallace:

A huge "thank you" goes out to my good friend Keith Barker for taking the lead on this book. Your insight into these technologies is profound, and your enthusiasm is contagious.

Also, I am grateful to work with the team of professionals at Pearson IT Certification. You are all a class act.

As always, I'm thankful to God and His many blessings, not the least of which is my family (my wife, Vivian, and daughters, Sabrina and Stacie).

About the Technical Editors

Michelle Plumb is a full-time Cisco Certified Systems Instructor (CCSI). She has 26-plus years of experience in the field as an IT professional and telecommunications specialist. She maintains a high level of Cisco, Microsoft, and CompTIA certifications, including CCNP Voice, MCSE, CompTIA A+, Network+, Project+, and iNet+. Michelle has been a technical reviewer for numerous books related to the Cisco CCNP Route and Switch, CCNP Voice, and CompTIA course materials. Her main passion is helping others learn these new and exciting technologies. She lives in Phoenix, Arizona, with her husband and two dogs.

Anthony Sequeira, CCIE No. 15626, is a seasoned trainer and author on all levels and tracks of Cisco certification. Anthony formally began his career in the IT industry in 1994 with IBM in Tampa, Florida. He quickly formed his own computer consultancy, Computer Solutions, and then discovered his true passion: teaching and writing about Microsoft and Cisco technologies.

Anthony joined Mastering Computers in 1996 and lectured to massive audiences around the world about the latest in computer technologies. Mastering Computers became the revolutionary online training company KnowledgeNet, and Anthony trained there for many years.

Anthony is currently pursuing his second CCIE in the area of security and then his third Cisco Data Center. When he's not writing for Cisco Press, Anthony is a full-time instructor at CBT Nuggets.

We Want to Hear from You!

As the reader of this book, *you* are our most important critic and commentator. We value your opinion and want to know what we're doing right, what we could do better, what areas you'd like to see us publish in, and any other words of wisdom you're willing to pass our way.

We welcome your comments. You can email or write to let us know what you did or didn't like about this book—as well as what we can do to make our books better.

Please note that we cannot help you with technical problems related to the topic of this book.

When you write, please be sure to include this book's title and author as well as your name, email address, and phone number. I will carefully review your comments and share them with the author and editors who worked on the book.

Email: feedback@pearsonitcertification.com

Mail: Pearson IT Certification
ATTN: Reader Feedback
800 East 96th Street
Indianapolis, IN 46240 USA

Reader Services

Visit our website and register this book at http://www.pearsonitcertification.com/title/9780789754080 for convenient access to any updates, downloads, or errata that might be available for this book.

CompTIA

CompTIA Network+

Becoming a CompTIA Certified IT Professional is Easy

It's also the best way to reach greater professional opportunities and rewards.

Why Get CompTIA Certified?

Growing Demand

Labor estimates predict some technology fields will experience growth of over 20% by the year 2020.* CompTIA certification qualifies the skills required to join this workforce.

Higher Salaries

IT professionals with certifications on their resume command better jobs, earn higher salaries and have more doors open to new multi-industry opportunities.

Verified Strengths

91% of hiring managers indicate CompTIA certifications are valuable in validating IT expertise, making certification the best way to demonstrate your competency and knowledge to employers.**

Universal Skills

CompTIA certifications are vendor neutral—which means that certified professionals can proficiently work with an extensive variety of hardware and software found in most organizations.

Learn

Learn more about what the exam covers by reviewing the following:

- Exam objectives for key study points.
- Sample questions for a general overview of what to expect on the exam and examples of question format.
- Visit online forums, like LinkedIn, to see what other IT professionals say about CompTIA exams.

Certify

Purchase a voucher at a Pearson VUE testing center or at CompTIAstore.com.

- Register for your exam at a Pearson VUE testing center:
- Visit pearsonvue.com/CompTIA to find the closest testing center to you.
- Schedule the exam online. You will be required to enter your voucher number or provide payment information at registration.
- Take your certification exam.

Work

Congratulations on your CompTIA certification!

- Make sure to add your certification to your resume.
- Check out the CompTIA Certification Roadmap to plan your next career move.

Learn more: **Certification.CompTIA.org/networkplus**

* Source: CompTIA 9th Annual Information Security Trends study: 500 U.S. IT and Business Executives Responsible for Security
** Source: CompTIA Employer Perceptions of IT Training and Certification
*** Source: 2013 IT Skills and Salary Report by CompTIA Authorized Partner

CompTIA Network+

The CompTIA Network+ (N10-006) certification exam will test to determine that the successful candidate has the knowledge and skills required to configure, manage and troubleshoot a network that uses Internet Protocol (IP).

It Pays to Get Certified

In a digital world, digital literacy is an essential survival skill. Certification proves that you have the knowledge and skill to solve business problems in nearly any business environment. Certifications are highly valued credentials that qualify you for jobs, increased compensation, and promotion.

- **The CompTIA Network+ credential:** Proves knowledge of networking features and functions and is the leading vendor-neutral certification for networking professionals.
- **Career pathway:** CompTIA Network+ is the first step in starting a networking career. Hundreds of thousands of individuals worldwide are CompTIA Network+ certified.
- **Mandated/recommended by organizations worldwide:** Such as Cisco, HP, Ricoh, the U.S. State Department, and U.S. government contractors such as EDS, General Dynamics, and Northrop Grumman.

How Certification Helps Your Career

CompTIA Career Pathway

CompTIA offers a number of credentials that form a foundation for your career in technology and allow you to pursue specific areas of concentration. Depending on the path you choose to take, CompTIA certifications help you build upon your skills and knowledge, supporting learning throughout your entire career.

Steps to Getting Certified and Staying Certified	
Review exam objectives	Review the certification objectives to make sure that you know what is covered in the exam: http://certification.comptia.org/training/testingcenters/examobjectives.aspx.
Practice for the exam	After you have studied for the certification, take a free assessment and sample test to get an idea of what type of questions might be on the exam: http://certification.comptia.org/training/testingcenters/samplequestions.aspx.

Steps to Getting Certified and Staying Certified	
Purchase an exam voucher	Purchase your exam voucher on the CompTIA Marketplace, which is located at http://www.comptiastore.com/.
Take the test!	Select a certification exam provider and schedule a time to take your exam. You can find exam providers at http://certification.comptia.org/training/testingcenters.aspx.
Stay certified! Continuing education	CompTIA Network+ certifications are valid for three years from the date of certification. There are a number of ways the certification can be renewed. For more information, go to http://certification.comptia.org/stayCertified.aspx.

Why CompTIA?

- **Global recognition:** CompTIA is recognized globally as the leading IT nonprofit trade association and has enormous credibility. Plus, CompTIA's certifications are vendor-neutral and offer proof of foundational knowledge that translates across technologies.
- **Valued by hiring managers:** Hiring managers value CompTIA certification because it is vendor- and technology-independent validation of your technical skills.
- **Recommended or required by government and businesses:** Many government organizations and corporations either recommend or require technical staff to be CompTIA certified.

How to Obtain More Information from CompTIA

- **Visit CompTIA online:** Visit http://www.comptia.org to learn more about getting CompTIA certified.
- **Contact CompTIA:** Call 866-835-8020.

Introduction

The CompTIA Network+ certification is a popular certification for those entering the computer networking field. Although many vendor-specific networking certifications are popular in the industry, the CompTIA Network+ certification is unique in that it is vendor neutral. The CompTIA Network+ certification often acts as a stepping-stone to more specialized and vendor-specific certifications, such as those offered by Cisco Systems.

In CompTIA Network+, the topics are mostly generic in that they can apply to networking equipment regardless of vendor. Although the CompTIA Network+ is vendor neutral, network software and systems are implemented by multiple independent vendors. In that light, several of the exercises, examples, and simulations in this book include using a vendor's configuration and technology such as Microsoft Windows operating systems or Cisco Systems routers and switches. More detailed training for a specific vendor's software and hardware can be found in books and training specific to that vendor.

Goals and Methods

The goal of this book is to assist you in learning and understanding the technologies covered in the Network+ N10-006 blueprint from CompTIA. This also allows you to demonstrate that knowledge by passing the N10-006 version of the CompTIA Network+ exam.

To aid you in mastering and understanding the Network+ certification objectives, this book uses the following methods:

- **Opening topics list:** This defines the topics that are covered in the chapter.
- **Foundation topics:** At the heart of a chapter, this section explains the topics from a hands-on and a theory-based standpoint. This includes in-depth descriptions, tables, and figures that build your knowledge so that you can pass the N10-006 exam. The chapters are each broken into multiple sections.
- **Key topics:** This indicates important figures, tables, and lists of information that you need to know for the exam. They are sprinkled throughout each chapter and are summarized in table format at the end of each chapter.
- **Memory tables:** You can find these on the DVD within Appendixes D and E. Use them to help memorize important information.
- **Key terms:** Key terms without definitions are listed at the end of each chapter. Write down the definition of each term, and check your work against the complete key terms in the Glossary. On the DVD, you will find a flash card application with all the glossary terms separated by chapter, so feel free to use that to study key terms as well.

- **Exercises:** This book comes with 40 performance-based practice exercises that are designed to help you prepare for the hands-on portion of the Network+ exam. These exercises are available on the DVD. Make sure you do the exercises as you complete each chapter and again when you have completed the book and are doing your final preparation.
- **Hands-on Labs:** These include matching, drag and drop, and simulations. These hands-on exercises are an important part of this book. In addition to reading this book, you should go through all the exercises included with the book. These interactive hands-on exercises provide examples, additional information, and insight about a vendor's implementation of the technologies. To perform the labs, simply install the CompTIA Network+ N10-006 Hands-on Lab Simulator Lite software from the DVD.
- **Practice Exams:** This book comes complete with several full length practice exams available to you in the Pearson IT Certification Practice Test software on the DVD. Be sure to run through the questions in Exam Bank 1 as you complete each chapter in study mode. When you have completed the book, take a full practice test using Exam Bank 2-4 questions in practice exam mode to test your exam readiness.
- **Exam Essentials:** This book includes an Exam Essentials appendix that summaries the key points from every chapter. This review tool is available in both print and an interactive PDF on the DVD. Review these essential exam facts after each chapter and again when you have completed the book. This makes a great review summary that you can mark up as you review and master each concept.

For current information about the CompTIA Network+ certification exam, visit http://certification.comptia.org/getCertified/certifications/network.aspx.

Who Should Read This Book?

Readers will range from people who are attempting to attain a position in the IT field to people who want to keep their skills sharp or perhaps retain their job because of a company policy that mandates they take the new exams.

This book is also for the reader who wants to acquire additional certifications beyond the Network+ certification (for example, the Cisco Certified Network Associate [CCNA] certification and beyond). The book is designed in such a way to offer easy transition to future certification studies.

Strategies for Exam Preparation

This book comes with a study planner tool on the DVD. This spreadsheet helps you keep track of the activities you need to perform in each chapter and helps you organize your exam preparation tasks. As you read the chapters in this book, jot down notes with key concepts or configurations in the study planner. Each chapter ends with a summary and series of exam preparation tasks to help you reinforce what you learned. These tasks include review exercises like reviewing key topics, completing memory tables, defining key terms, answering review questions, performing hands-on labs and exercises, and so on. Make sure you perform these tasks as you complete each chapter to improve your retention of the material and record your progress in the study planner.

The book concludes with a Final Preparation chapter that offers you guidance on your final exam preparation and provides you with some helpful exam advice. Make sure you read over that chapter to help you assess your exam readiness and identify areas where you need to focus your review.

Make sure you complete all the performance-based question exercises and hands-on labs associated with this book. The exercises and labs are organized by chapter, making it easy to perform them after you complete each section. These exercises will reinforce what you have learned, offer examples of some popular vendors methods for implementing networking technologies, and provide additional information to assist you in building real-world skills and preparing you for the certification exam.

Download the current exam objectives by submitting a form on the following web page: http://certification.comptia.org/training/testingcenters/examobjectives.aspx.

Use the practice exam, which is included on this book's DVD. As you work through the practice exam, use the practice test software reporting features to note the areas where you lack confidence and review those concepts. After you review these areas, work through the practice exam a second time and rate your skills. Keep in mind that the more you work through the practice exam, the more familiar the questions become, and the practice exam becomes a less-accurate judge of your skills.

After you work through the practice exam a second time and feel confident with your skills, schedule the real CompTIA Network+ exam (N10-006). The following website provides information about registering for the exam: http://certification.comptia.org/training/testingcenters.aspx.

CompTIA Network+ Exam Topics

Table I-1 lists general exam topics (objectives) and specific topics under each general topic (subobjectives) for the CompTIA Network+ N10-006 exam. This table lists the primary chapter in which each exam topic is covered. Note that many objectives and subobjectives are interrelated and are addressed in multiple chapters within the book itself.

Table I-1 CompTIA Network+ Exam Topics

Chapter	N10-006 Exam Objective	N10-006 Exam Subobjective
1 Computer Network Fundamentals	1.0 Network architecture	1.1 Explain the functions and applications of various network devices 1.6 Differentiate between common network topologies 1.7 Differentiate between network infrastructure implementations
2 The OSI Reference Model	5.0 Industry standards, practices, and network theory	5.1 Analyze a scenario and determine the corresponding OSI layer 5.2 Explain the basics of network theory and concepts 5.9 Compare and contrast ports and protocols 5.10 Given a scenario, configure and apply the appropriate ports and protocols
3 Network Components	1.0 Network architecture 5.0 Industry standards, practices, and network theory	1.3 Install and configure networking services/applications 1.5 Install and properly terminate various cable types and connectors using appropriate tools 1.10 Identify the basic elements of unified communication technologies 1.11 Compare and contrast technologies that support the cloud and virtualization 1.12 Given a set of requirements, implement a basic network 5.7 Given a scenario, install and configure equipment in the appropriate location using best practices
4 Ethernet Technology	2.0 Network operations 5.0 Industry standards, practices, and network theory	2.6 Given a scenario, configure a switch using proper features 5.4 Given a scenario, deploy the appropriate wired connectivity standard
5 IPv4 and IPv6 Addresses	1.0 Network architecture	1.8 Given a scenario, implement and configure the appropriate addressing schema
6 Routing IP Packets	1.0 Network architecture	1.9 Explain the basics of routing concepts and protocols

7 Wide-Area Networks	1.0 Network architecture 4.0 Troubleshooting	1.4 Explain the characteristics and benefits of various WAN technologies 4.8 Given a scenario, troubleshoot and resolve common WAN issues
8 Wireless LANs	2.0 Network operations 5.0 Industry standards, practices, and network theory	2.7 Install and configure wireless LAN infrastructure and implement the appropriate technologies in support of wireless capable devices 4.3 Given a scenario, troubleshoot and resolve common wireless issues 5.3 Given a scenario, deploy the appropriate wireless standard
9 Network Optimization	1.0 Network architecture	1.10 Identify the basic elements of unified communication technologies
10 Command-Line Tools	4.0 Troubleshooting	4.6 Given a scenario, troubleshoot and resolve common network issues
11 Network Management	2.0 Network operations 5.0 Industry standards, practices, and network theory	2.1 Given a scenario, use appropriate monitoring tools 2.2 Given a scenario, analyze metrics and reports from monitoring and tracking performance tools 2.3 Given a scenario, use appropriate resources to support configuration management 5.5 Given a scenario, implement the appropriate policies or procedures 5.6 Summarize safety practices 5.8 Explain the basics of change management procedures

12 Network Security	1.0 Network architecture 2.0 Network operations 3.0 Network security 4.0 Troubleshooting	1.2 Compare and contrast the use of networking services and applications 2.4 Explain the importance of implementing network segmentation 2.5 Given a scenario, install and apply patches and updates 3.1 Compare and contrast risk-related concepts 3.2 Compare and contrast common network vulnerabilities and threats 3.3 Given a scenario, implement network hardening techniques 3.4 Compare and contrast physical security controls 3.5 Given a scenario, install and configure a basic firewall 3.6 Explain the purpose of various network access control models 3.7 Summarize basic forensic concepts 4.7 Given a scenario, troubleshoot and resolve common security issues
13 Network Troubleshooting	4.0 Troubleshooting	4.1 Given a scenario, implement a network troubleshooting methodology 4.2 Given a scenario, analyze and interpret the output of troubleshooting tools 4.4 Given a scenario, troubleshoot and resolve common copper cable issues 4.5 Given a scenario, troubleshoot and resolve common fiber cable issues

How This Book Is Organized

Although this book could be read cover to cover, it is designed to be flexible and allow you to easily move between chapters and sections of chapters to cover just the material that you need more work with. However, if you do intend to read all the chapters, the order in the book is an excellent sequence to use:

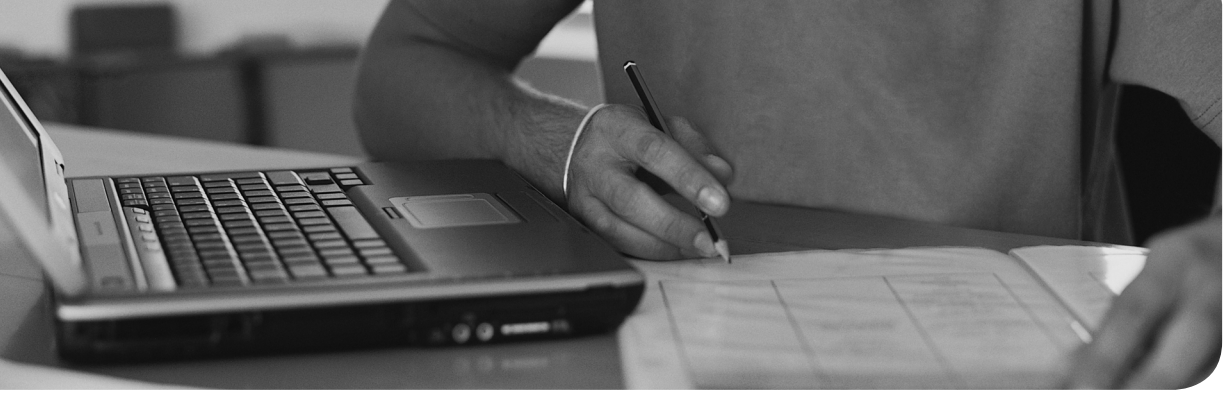
- **Chapter 1, "Computer Network Fundamentals,"** introduces the purpose of computer networks and their constituent components. In addition, networks are categorized by their geography, topology, and resource location.
- **Chapter 2, "The OSI Reference Model,"** presents the two network models: the OSI model and the TCP/IP stack. These models categorize various network components from a network cable up to and including an application,

such as e-mail. These models are contrasted, and you are given a listing of well-known TCP and UDP port numbers used for specific applications.

- **Chapter 3, "Network Components."** A variety of network components are introduced in this chapter. You are given an explanation of various media types, the roles of specific infrastructure components, and the features provided by specialized network devices (for example, a firewall or content switch).
- **Chapter 4, "Ethernet Technology."** The most widely deployed LAN technology is Ethernet, and this chapter describes the characteristics of Ethernet networks. Topics include media access, collision domains, broadcast domains, and distance/speed limitations for popular Ethernet standards. Additionally, you are introduced to some of the features available on Ethernet switches, such as VLANs, trunks, STP, link aggregation, PoE, port monitoring, and user authentication.
- **Chapter 5, "IPv4 and IPv6 Addresses."** One of the most challenging concepts for many CompTIA Network+ students is IP subnetting. This chapter demystifies IP subnetting by reviewing the basics of binary numbering before delving into basic subnetting and then advanced subnetting. Although most of the focus of this chapter is on IPv4 addressing, the chapter concludes with an introduction to IPv6.
- **Chapter 6, "Routing IP Packets."** A primary job of a computer network is to route traffic between subnets. This chapter reviews the operation of routing IP traffic and discusses how a router obtains routing information. One way a router can populate its routing table is through the use of dynamic routing protocols, several of which are discussed in this chapter. Many environments (such as a home network connecting to the Internet via a cable modem) use NAT to convert between private IP addresses inside a network and public IP addresses outside a network. This chapter discusses Dynamic NAT (DNAT), Static NAT (SNAT), and Port Address Translation (PAT). Although the primary focus on this chapter is on unicast routing, the chapter concludes with a discussion of multicast routing.
- **Chapter 7, "Wide-Area Networks."** Many corporate networks need to interconnect multiple sites separated by large distances. Connections between such geographically dispersed sites make up a WAN. This chapter discusses three categories of WAN connections and contrasts various WAN connection types, based on supported data rates and media types. Finally, this chapter lists characteristics for multiple WAN technologies.
- **Chapter 8, "Wireless LANs."** In this increasingly mobile world, wireless technologies are exploding in popularity. This chapter discusses the basic operation of WLANs. In addition, WLAN design and security considerations are addressed.

- **Chapter 9, "Network Optimization."** This chapter explains the importance of high availability for a network and what mechanisms help provide a high level of availability. Network performance optimization strategies are addressed, including a section on quality of service (QoS). This chapter allows you to use what you have learned in this and preceding chapters to design a small office/home office (SOHO) network.
- **Chapter 10, "Command-Line Tools."** In your daily administration and troubleshooting of computer networks, you need familiarity with various command-line utilities available on the operating systems present in your network. This chapter presents a collection of popular command-line utilities for both Microsoft Windows and UNIX platforms.
- **Chapter 11, "Network Management,"** reviews some of the more common tools used to physically maintain a network. The components of configuration management are also presented. This chapter discusses some of the network monitoring tools available to network administrators and what types of information are included in various logs.
- **Chapter 12, "Network Security."** Network security is an issue for most any network, and this chapter covers a variety of network security technologies. You begin by learning the goals of network security and the types of attacks you must defend against. Then you review a collection of security best practices. Next, the chapter discusses specific security technologies, including firewalls, virtual private networks (VPNs), intrusion detection systems (IDSs), and intrusion prevention systems (IPSs).
- **Chapter 13, "Network Troubleshooting."** Troubleshooting network issues is an inherent part of network administration, and this chapter presents a structured approach to troubleshooting various network technologies. Specifically, you learn how to troubleshoot common Layer 2, Layer 3, and wireless network issues.
- **Chapter 14, "Final Preparation,"** reviews the exam-preparation tools available in this book and the enclosed DVD. For example, the enclosed DVD contains exercises including drag and drop, matching, and simulations as well as a practice exam engine and a collection of a few training videos. Finally, a suggested study plan is presented to assist you in preparing for the CompTIA Network+ exam (N10-006).

In addition to the 13 main chapters, this book includes tools to help you verify that you are prepared to take the exam. The DVD includes drag-and-drop, matching, and simulation exercises that are an important part of your preparation for certification. The DVD also includes a practice test and memory tables that you can work through to verify your knowledge of the subject matter. Finally, the DVD contains a few videos that can assist you in mastering the content.



After completion of this chapter, you will be able to answer the following questions:

- How do various wireless LAN technologies function, and what wireless standards are in common use?
- What are some of the most important WLAN design considerations?
- What WLAN security risks exist, and how can those risks be mitigated?

CHAPTER 8

Wireless LANs

The popularity of wireless LANs (WLANs) has exploded over the past decade, allowing users to roam within a WLAN coverage area, take their laptops with them, and maintain network connectivity as they move throughout a building or campus environment. Many other devices, however, can take advantage of wireless networks, such as gaming consoles, smartphones, and printers.

This chapter introduces WLAN technology, along with various wireless concepts, components, and standards. WLAN design considerations are then presented, followed by a discussion of WLAN security.

Foundation Topics

Introducing Wireless LANs

This section introduces the basic building blocks of WLANs and discusses how WLANs connect into a wired local-area network (LAN). Various design options, including antenna design, frequencies, and communications channels, are discussed, along with a comparison of today's major wireless standards, which are all some variant of IEEE 802.11.

WLAN Concepts and Components

Wireless devices, such as laptops and smartphones, often have a built-in wireless card that allows those devices to communicate on a WLAN. But what is the device to which they communicate? It could be another laptop with a wireless card. This would be an example of an *ad hoc* WLAN. However, enterprise-class WLANs, and even most WLANs in homes, are configured in such a way that a wireless client connects to some sort of a wireless base station, such as a wireless access point (AP) or a wireless router. Many companies offer WiFi as a service, and when in range of an AP, it is also referred to as a *hotspot*, indicating that WiFi is available through the AP.

This communication might be done using a variety of antenna types, frequencies, and communication channels. The following sections consider some of these elements in more detail.

Wireless Routers

Consider the basic WLAN topology shown in Figure 8-1. Such a WLAN might be found in a residence whose Internet access is provided by digital subscriber line (DSL) modem. In this topology, a wireless router and switch are shown as separate components. However, in many residential networks, a wireless router integrates switch ports and wireless routing functionality into a single device.

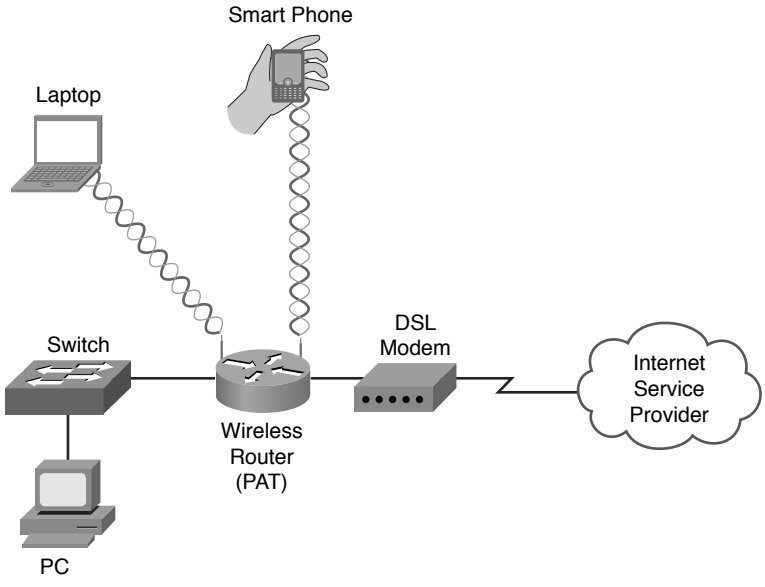


Figure 8-1 Basic WLAN Topology with a Wireless Router

In Figure 8-1, the wireless router obtains an IP address via DHCP from the Internet service provider (ISP). Then the router uses Port Address Translation (PAT), as described in Chapter 6, "Routing IP Packets," to provide IP addresses to devices attaching to it wirelessly or through a wired connection. The process through which a wireless client (for example, a laptop or a smartphone) attaches with a wireless router (or wireless AP) is called *association*. All wireless devices associating with a single AP share a collision domain. Therefore, for scalability and performance reasons, WLANs might include multiple APs.

Wireless Access Point

Although a wireless access point (AP) interconnects a wired LAN with a WLAN, it does not interconnect two networks (for example, the service provider's network with an internal network). Figure 8-2 shows a typical deployment of an AP.

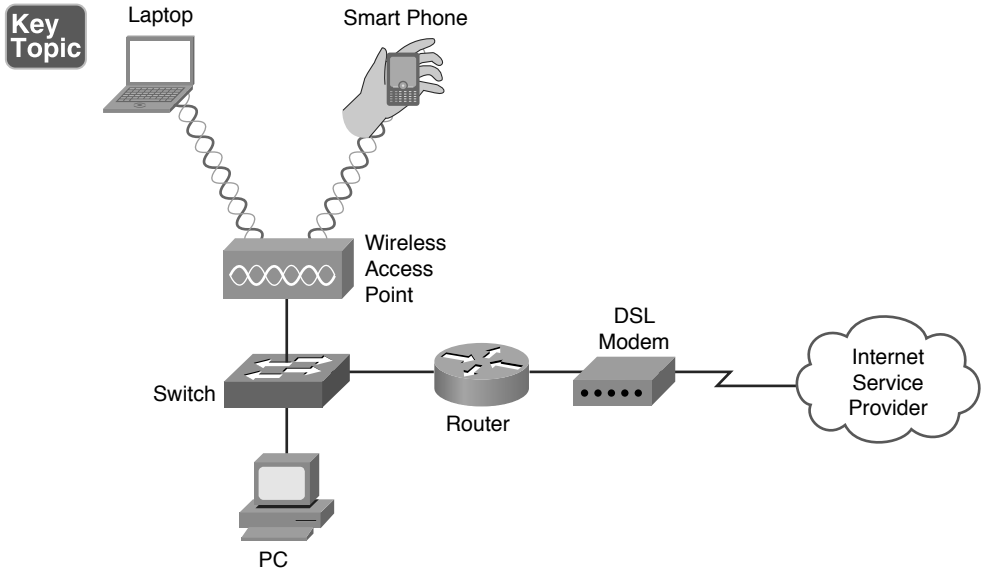


Figure 8-2 Basic WLAN Topology with a Wireless AP

The AP connects to the wired LAN, and the wireless devices that connect to the wired LAN via the AP are on the same subnet as the AP. (No Network Address Translation [NAT] or PAT is being performed.) This is acting as a wireless bridge between the wireless clients connected to the AP and the wired devices connected to the switch in the same Layer 2 domain.

To manage multiple APs, a company will use a Wireless LAN Controller (WLC) for centralized management and control of the APs. A Cisco model 5760 WLC would be an example of a network controller for multiple APs. The protocols used to communicate between an AP and a WLC could be the older Lightweight Access Point Protocol (LWAPP) or the more current Control And Provisioning of Wireless Access Points (CAPWAP). Using a WLC, VLAN pooling can be used to assign IP addresses to wireless clients from a pool of IP subnets and their associated VLANs.

Antennas

The coverage area of a WLAN is largely determined by the type of antenna used on a wireless AP or a wireless router. Although some lower-end, consumer-grade wireless APs have fixed antennas, higher-end, enterprise-class wireless APs often support various antenna types.

Design goals to keep in mind when selecting an antenna include the following:

Key Topic

- Required distance between an AP and a wireless client.
- Pattern of coverage area. (For example, the coverage area might radiate out in all directions, forming a spherical coverage area around an antenna, or an antenna might provide increased coverage in only one or two directions.)
- Indoor or outdoor environment.
- Avoiding interference with other APs.

The strength of the electromagnetic waves being radiated from an antenna is referred to as *gain*, which involves a measurement of both direction and efficiency of a transmission. For example, the gain measurement for a wireless AP's antenna transmitting a signal is a measurement of how efficiently the power being applied to the antenna is converted into electromagnetic waves being broadcast in a specific direction. Conversely, the gain measurement for a wireless AP's antenna receiving a signal is a measurement of how efficiently the received electromagnetic waves arriving from a specific direction are converted back into electricity leaving the antenna.

Gain is commonly measured using the dBi unit of measure. In this unit of measure, the *dB* stands for *decibels* and the *i* stands for *isotropic*. A decibel, in this context, is a ratio of radiated power to a reference value. In the case of dBi, the reference value is the signal strength (power) radiated from an isotropic antenna, which represents a theoretical antenna that radiates an equal amount of power in all directions (in a spherical pattern). An isotropic antenna is considered to have gain of 0 dBi.

The most common formula used for antenna gain is the following:

$$GdBi = 10 * \log^{10} (G)$$

Based on this formula, an antenna with a peak power gain of 4 (*G*) would have a gain of 6.02 dBi. Antenna theory can become mathematical (heavily relying on the use of Maxwell's equations). However, to put this discussion in perspective, generally speaking, if one antenna has 3 dB more gain than another antenna, it has approximately twice the effective power.

Antennas are classified not just by their gain but also by their coverage area. Two broad categories of antennas, which are based on coverage area, are as follows:

- **Omnidirectional:** An omnidirectional antenna radiates power at relatively equal power levels in all directions (somewhat similar to the theoretical isotropic antenna). Omnidirectional antennas, an example of which is depicted in Figure 8-3, are popular in residential WLANs and small office/home office (SOHO) locations.

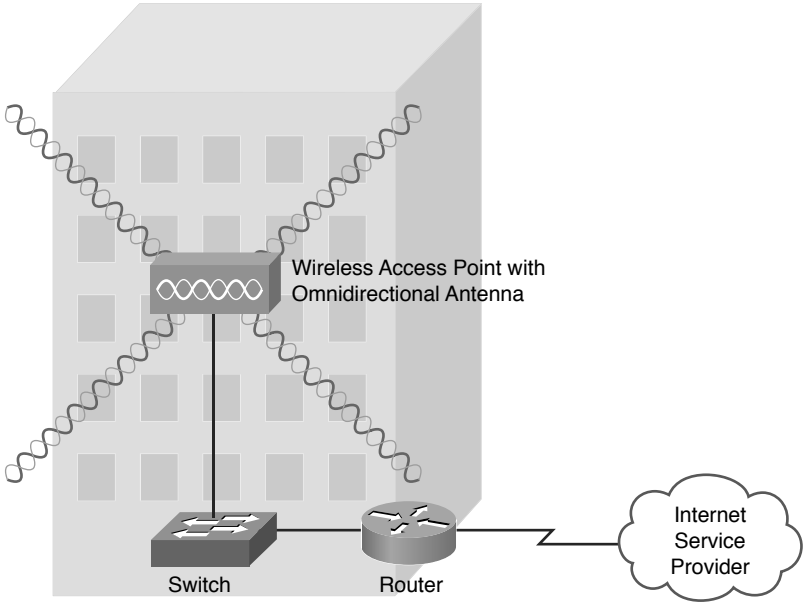


Figure 8-3 Omnidirectional Antenna Coverage

- **Unidirectional:** Unidirectional antennas can focus their power in a specific direction, thus avoiding potential interference with other wireless devices and perhaps reaching greater distances than those possible with omnidirectional antennas. One application for unidirectional antennas is interconnecting two nearby buildings, as shown in Figure 8-4.

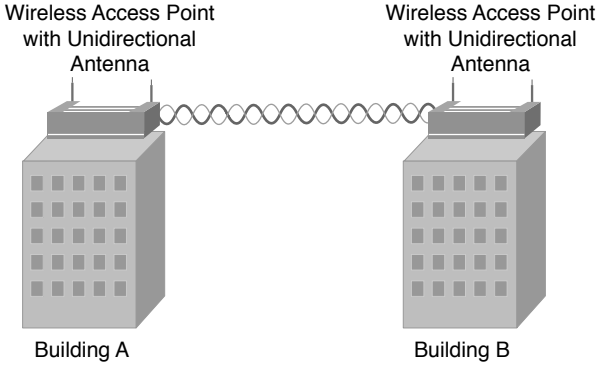


Figure 8-4 Unidirectional Antenna Coverage

Another consideration for antenna installation is the horizontal or vertical orientation of the antenna. For best performance, if two wireless APs communicate with one another, they should have matching antenna orientations, which is referred to as the *polarity* of the antenna.

Frequencies and Channels

Later in this chapter, you are introduced to a variety of wireless standards, which are all variants of the IEEE 802.11 standard. As you contrast one standard versus another, a characteristic to watch out for is the frequencies at which these standards operate. Although there are some country-specific variations, certain frequency ranges (or *frequency bands*) have been reserved internationally for industrial, scientific, and medical purposes. These frequency bands are called the *ISM bands*, where ISM derives from *i*ndustrial, *s*cientific, and *m*edical.

Two of these bands are commonly used for WLANs. Specifically, WLANs can use the range of frequencies in the 2.4-GHz to 2.5-GHz range (commonly referred to as the *2.4-GHz band*) or in the 5.725-GHz to 5.875-GHz range (commonly referred to as the *5-GHz band*). In fact, some WLANs support a mixed environment, where 2.4-GHz devices run alongside 5-GHz devices.

Within each band are specific frequencies (or *channels*) at which wireless devices operate. To avoid interference, nearby wireless APs should use frequencies that do not overlap with one another. Using wireless survey tools such as AirMagnet from Fluke Networks can provide analysis of what is currently in use, allowing you to set up a new wireless system that does not compete for the same frequencies that are already in use. Those same tools can assist in identifying wireless channel utilization as well in existing and new wireless networks. Regarding channel selection, merely selecting different channels is not sufficient, however, because transmissions on one channel spill over into nearby channels. Site survey tools can collect data to show the relative strength of signals in the areas being serviced by the APs. This output can be color-coded and overlaid on top of the floor plan and is often referred to as a *heat map* of the wireless signals.

Consider, for example, the 2.4-GHz band. Here, channel frequencies are separated by 5 MHz (with the exception of channel 14, which has 12 MHz of separation from channel 13). However, a single channel's transmission can spread over a frequency range of 22 MHz. As a result, channels must have five channels of separation (5 * 5 MHz = 25 MHz, which is greater than 22 MHz). You can see from Figure 8-5 that, in the United States, you could select nonoverlapping channels of 1, 6, and 11.

Key Topic

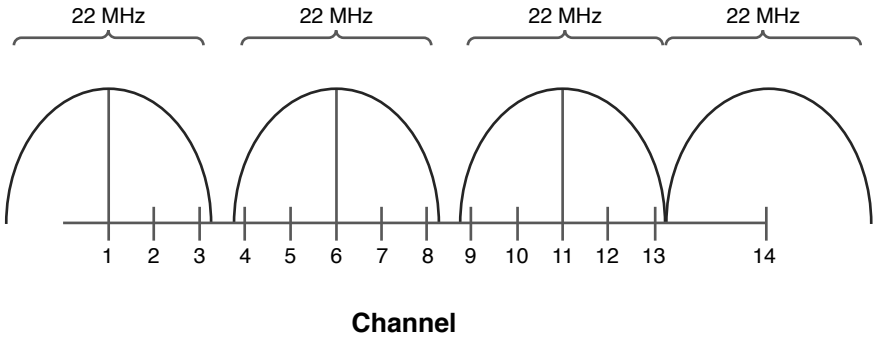


Figure 8-5 Nonoverlapping Channels in the 2.4 GHz Band

NOTE Even though some countries use channel 14 as a nonoverlapping channel, it is not supported in the United States.

As a reference, Table 8-1 shows the specific frequencies for each of the channels in the 2.4-GHz band.

Table 8-1 Channel Frequencies in the 2.4-GHz Band

Channel	Frequency (GHz)	Recommended as a Nonoverlapping Channel
1	2.412	Yes
2	2.417	No
3	2.422	No
4	2.427	No
5	2.432	No
6	2.437	Yes
7	2.442	No
8	2.447	No
9	2.452	No
10	2.457	No
11	2.462	Yes
12	2.467	No
13	2.472	No
14	2.484	Yes (not supported in the United States)

The 5-GHz band has a higher number of channels, as compared to the 2.4-GHz band. Table 8-2 lists the recommended nonoverlapping channels for the 5-GHz band in the United States. Note that additional channels are supported in some countries.

Table 8-2 Nonoverlapping Channels in the 5-GHz Band Recommended for Use in the United States

Channel	Frequency (GHz)
36	5.180
40	5.200
44	5.220
48	5.240
52	5.260*
56	5.280*
60	5.300*
64	5.320*
100	5.500**
104	5.520**
108	5.540**
112	5.560**
116	5.580**
136	5.680**
140	5.700**
149	5.745
153	5.765
157	5.785
161	5.805
165	5.825

*Must support dynamic frequency selection to prevent interference with RADAR

**Must be professionally installed

CSMA/CA

In Chapter 4, "Ethernet Technology," you learned about Ethernet's carrier sense multiple access collision detection (CSMA/CD) technology. WLANs use a similar technology called carrier sense multiple access collision avoidance (CSMA/CA). Just

as CSMA/CD is needed for half-duplex Ethernet connections, CSMA/CA is needed for WLAN connections because of their half-duplex operation. Similar to the way an Ethernet device listens to an Ethernet segment to determine whether a frame exists on the segment, a WLAN device listens for a transmission on a wireless channel to determine whether it is safe to transmit. In addition, the collision-avoidance part of the CSMA/CA algorithm causes wireless devices to wait for a random backoff time before transmitting.

Transmission Methods

In the previous discussion, you saw the frequencies used for various wireless channels. However, be aware that those frequencies are considered to be the *center frequencies* of a channel. In actual operation, a channel uses more than one frequency, which is a transmission method called *spread spectrum*. These frequencies are, however, very close to one another, which results in a *narrowband transmission*.

The three variations of spread-spectrum technology to be aware of for your study of WLANs include the following:

Key Topic

- **Direct-sequence spread spectrum (DSSS):** Modulates data over an entire range of frequencies using a series of symbols called *chips*. A chip is shorter in duration than a bit, meaning that chips are transmitted at a higher rate than the actual data. These chips encode not only the data to be transmitted, but also what appears to be random data. Although both parties involved in a DSSS communication know which chips represent actual data and which chips do not, if a third party intercepted a DSSS transmission, it would be difficult for him to eavesdrop on the data because he would not easily know which chips represented valid bits. DSSS is more subject to environmental factors, as opposed to FHSS and OFDM, because of its use of an entire frequency spectrum.
- **Frequency-hopping spread spectrum (FHSS):** Allows the participants in a communication to hop between predetermined frequencies. Security is enhanced because the participants can predict the next frequency to be used, but a third party cannot easily predict the next frequency. FHSS can also provision extra bandwidth by simultaneously using more than one frequency.
- **Orthogonal frequency-division multiplexing (OFDM):** Whereas DSSS uses a high modulation rate for the symbols it sends, OFDM uses a relatively slow modulation rate for symbols. This slower modulation rate, combined with the simultaneous transmission of data over 52 data streams, helps OFDM support high data rates while resisting interference between the various data streams.

Of these three wireless modulation techniques, only DSSS and OFDM are commonly used in today's WLANs.

WLAN Standards

Most modern WLAN standards are variations of the original IEEE 802.11 standard, which was developed in 1997. This original standard supported a DSSS and an FHSS implementation, both of which operated in the 2.4-GHz band. However, with supported speeds of 1 Mbps or 2 Mbps, the original 802.11 standard lacks sufficient bandwidth to meet the needs of today's WLANs. The most popular variants of the 802.11 standard in use today are 802.11a, 802.11b, 802.11g, 802.11n, and 802.11ac, as described in detail in the following sections.

802.11a

The 802.11a WLAN standard, which was ratified in 1999, supports speeds as high as 54 Mbps. Other supported data rates (which can be used if conditions are not suitable for the 54 Mbps rate) include 6, 9, 12, 18, 24, 36, and 48 Mbps. The 802.11a standard uses the 5-GHz band and uses the OFDM transmission method. Interestingly, 802.11a never gained widespread adoption because it was not backward compatible with 802.11b, whereas 802.11g was backward compatible.

802.11b

The 802.11b WLAN standard, which was ratified in 1999, supports speeds as high as 11 Mbps. However, 5.5 Mbps is another supported data rate. The 802.11b standard uses the 2.4-GHz band and uses the DSSS transmission method.

802.11g

The 802.11g WLAN standard, which was ratified in 2003, supports speeds as high as 54 Mbps. Like 802.11a, other supported data rates include 6, 9, 12, 18, 24, 36, and 48 Mbps. However, like 802.11b, 802.11g operates in the 2.4-GHz band, which allows it to offer backward compatibility to 802.11b devices. 802.11g can use either the OFDM or the DSSS transmission method.

802.11n

The 802.11n WLAN standard, which was ratified in 2009, supports a wide variety of speeds, depending on its implementation. Although the speed of an 802.11n network could exceed 300 Mbps (through the use of *channel bonding*, as discussed later), many 802.11n devices on the market have speed ratings in the 130–150 Mbps range. Interestingly, an 802.11n WLAN could operate in the 2.4-GHz band, the 5-GHz band, or both simultaneously. 802.11n uses the OFDM transmission method.

One way 802.11n achieves superior throughput is through the use of a technology called *multiple input*, *multiple output* (MIMO). MIMO uses multiple antennas for transmission and reception. These antennas do not interfere with one another, thanks to MIMO's use of *spatial multiplexing*, which encodes data based on the antenna from which the data will be transmitted. Both reliability and throughput can be increased with MIMO's simultaneous use of multiple antennas.

Yet another technology implemented by 802.11n is *channel bonding*. With channel bonding, two wireless bands can be logically bonded together, forming a band with twice the bandwidth of an individual band. Some literature refers to channel bonding as *40-MHz mode*, which is the bonding of two adjacent 20-MHz bands into a 40-MHz band.

The 802.11n high throughput (HT) standard defines modes for ensuring that older a/b/g devices and newer 802.11n devices can avoid collisions with each other.

802.11ac

The 802.11ac WLAN standard was published in 2013 and builds on (and is faster and more scalable than) 802.11n. 802.11ac is a 5-GHz only technology that can use wider channels in the 5-GHz band, more spatial streams, and multi-user MIMO (MU-MIMO).

802.11x Standard Summary

Table 8-3 acts as a reference to help you contrast the characteristics of the 802.11 standards.

Key Topic

Table 8-3 Characteristics of 802.11 Standards

Standard	Band	Max. Bandwidth	Transmission Method	Max. Range
802.11	2.4 GHz	1 Mbps or 2 Mbps	DSSS or FHSS	20 m indoors / 100 m outdoors
802.11a	5 GHz	54 Mbps	OFDM	35 m indoors/ 120 m outdoors
802.11b	2.4 GHz	11 Mbps	DSSS	32 m indoors/ 140 m outdoors
802.11g	2.4 GHz	54 Mbps	OFDM or DSSS	32 m indoors/ 140 m outdoors
802.11n	2.4 GHz or 5 GHz (or both)	> 300 Mbps (with channel bonding)	OFDM	70 m indoors/ 250 m outdoors
802.11ac	5 GHz	> 3 Gbps (with MU-MIMO and several antennas)	OFDM	Similar to 802.11n operating at 5 GHz

Deploying Wireless LANs

When designing and deploying WLANs, you have a variety of installation options and design considerations. This section delves into your available options and provides you with some best practice recommendations.

Types of WLANs

WLANs can be categorized based on their use of wireless APs. The three main categories are independent basic service set (IBSS), basic service set (BSS), and extended service set (ESS). An IBSS WLAN operates in an ad hoc fashion, while BSS and ESS WLANs operate in infrastructure mode. The following sections describe the three types of WLANs in detail.

IBSS

As shown in Figure 8-6, a WLAN can be created without the use of an AP. Such a configuration, called an IBSS, is said to work in an ad hoc fashion. An ad hoc WLAN is useful for temporary connections between wireless devices. For example, you might temporarily interconnect two laptop computers to transfer a few files.

Key Topic

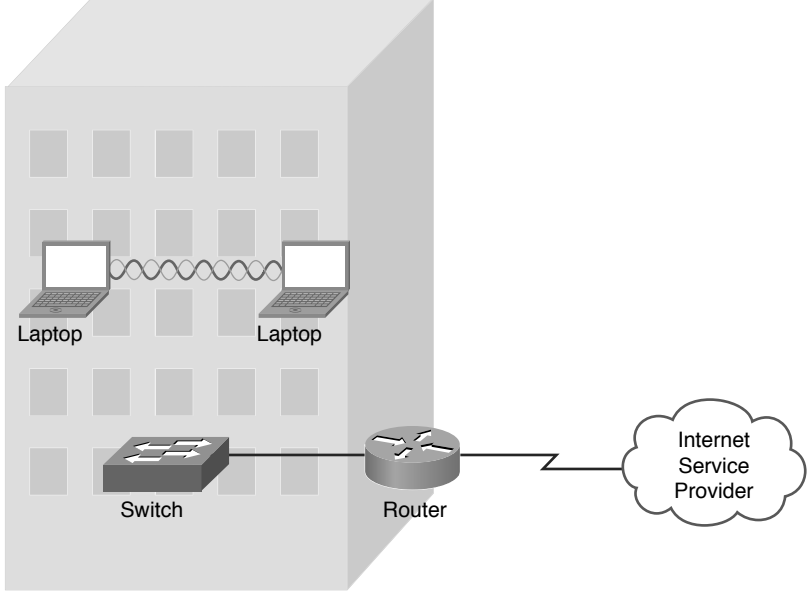


Figure 8-6 Independent Basic Service Set (IBSS) WLAN

BSS

Figure 8-7 depicts a WLAN using a single AP. WLANs that have just one AP are called BSS WLANs. BSS WLANs are said to run in infrastructure mode because wireless clients connect to an AP, which is typically connected to a wired network infrastructure. A BSS network is often used in residential and SOHO locations, where the signal strength provided by a single AP is sufficient to service all the WLAN's wireless clients.

Key Topic

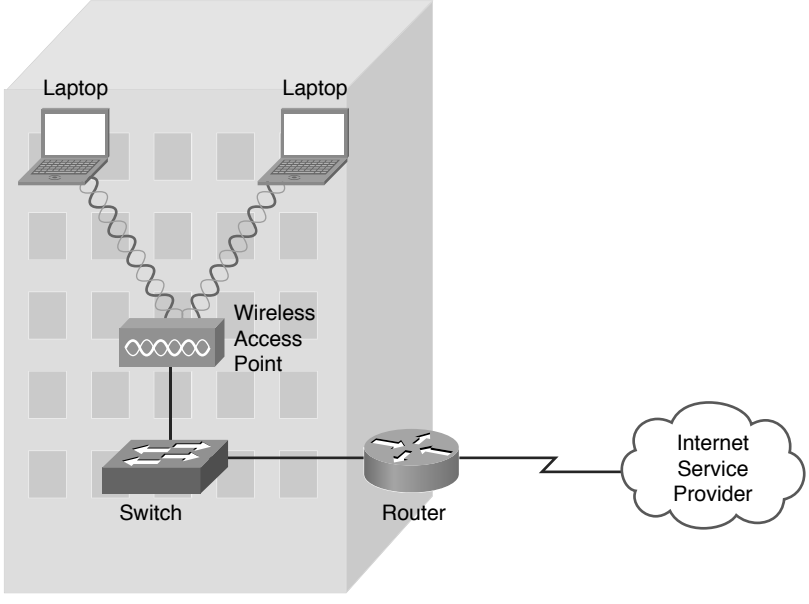


Figure 8-7 Basic Service Set (BSS) WLAN

ESS

Figure 8-8 illustrates a WLAN using two APs. WLANs containing more than one AP are called *ESS WLANs*. Like BSS WLANs, ESS WLANs operate in infrastructure mode. When you have more than one AP, take care to prevent one AP from interfering with another. Specifically, the previously discussed nonoverlapping channels (channels 1, 6, and 11 for the 2.4-GHz band) should be selected for adjacent wireless coverage areas.

Key Topic

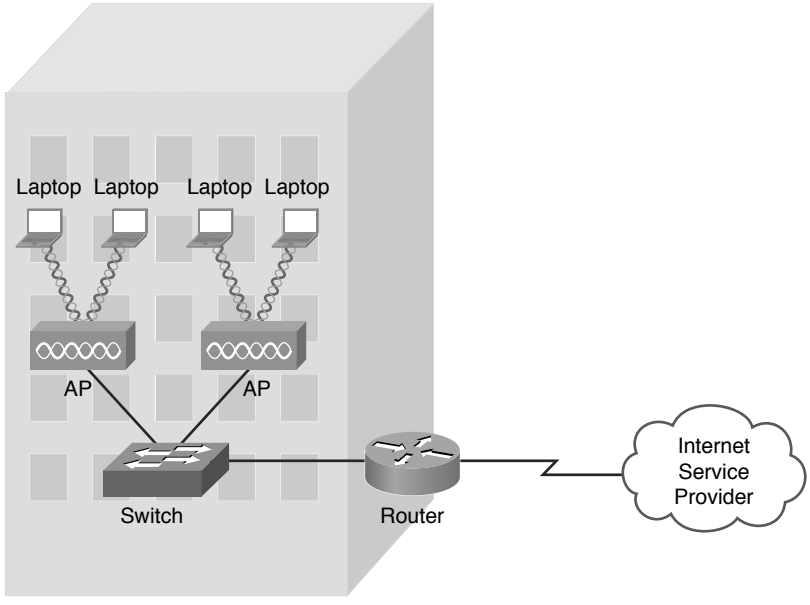


Figure 8-8 Extended Service Set (ESS) WLAN

Mesh Topology

A mesh wireless network is a collection of wireless devices that may not use centralized control (decentralized management). The combined wireless coverage range defines the range of the network. This could also be referred to as a *mesh cloud*. Additional wireless technologies (besides WiFi) could be used to build a mesh wireless topology. This type of network could be used for hosts to communicate with other devices in the mesh, or the network could provide a gateway to the Internet or other networks.

Sources of Interference

A major issue for WLANs is radio frequency interference (RFI) caused by other devices using similar frequencies to the WLAN devices. Also, physical obstacles can impede or reflect WLAN transmissions. The following are some of the most common sources of interference:

Key Topic

- **Other WLAN devices:** Earlier in this chapter, you read about nonoverlapping channels for both the 2.4-GHz and 5-GHz bands. However, if two or more WLAN devices are in close proximity and use overlapping channels, those devices could interfere with one another.

- **Cordless phones:** Several models of cordless phones operate in the 2.4-GHz band and can interfere with WLAN devices. However, if you need cordless phones to coexist in an environment with WLAN devices using the 2.4-GHz band, consider the use of digital enhanced cordless telecommunications (DECT) cordless phones. Although the exact frequencies used by DECT cordless phones vary based on country, DECT cordless phones do not use the 2.4-GHz band. For example, in the United States, DECT cordless phones use frequencies in the range 1.92 GHz to 1.93 GHz.
- **Microwave ovens:** Older microwave ovens, which might not have sufficient shielding, can emit relatively high-powered signals in the 2.4-GHz band, resulting in significant interference with WLAN devices operating in the 2.4-GHz band.
- **Wireless security system devices:** Most wireless security cameras operate in the 2.4-GHz frequency range, which can cause potential issues with WLAN devices.
- **Physical obstacles:** In electromagnetic theory, radio waves cannot propagate through a perfect conductor. So, although metal filing cabinets and large appliances are not perfect conductors, they are sufficient to cause degradation of a WLAN signal. For example, a WLAN signal might hit a large air conditioning unit, causing the radio waves to be reflected and scattered in multiple directions. Not only does this limit the range of the WLAN signal, but radio waves carrying data might travel over different paths. This *multipath issue* can cause data corruption. Concrete walls, metal studs, or even window film could reduce the quality of the wireless network signals.
- **Signal strength:** The range of a WLAN device is a function of the device's signal strength. Lower-cost consumer-grade APs do not typically allow an administrative adjustment of signal strength. However, enterprise-class APs often allow signal strength to be adjusted to ensure sufficient coverage of a specific area, while avoiding interference with other APs using the same channel.

As you can see from this list, most RFI occurs in the 2.4-GHz band as opposed to the 5-GHz band. Therefore, depending on the wireless clients you need to support, you might consider using the 5-GHz band, which is an option for 802.11a and 802.11n WLANs. With the increased use of wireless, both coverage and capacity-based planning should be done to provide acceptable goodput. *Goodput* refers to the number of useful information bits that the network can deliver (not including overhead for the protocols being used). Another factor is the density (ratio of users to APs), which if too high could harm performance of the network. Areas expecting high density would include classrooms, hotels, and hospitals. Device or bandwidth saturation could impact performance.

Wireless AP Placement

WLANs using more than one AP (an ESS WLAN) require careful planning to prevent the APs from interfering with one another, while still servicing a desired coverage area. Specifically, an overlap of coverage between APs should exist to allow uninterrupted roaming from one WLAN *cell* (which is the coverage area provided by an AP) to another. However, those overlapping coverage areas should not use overlapping frequencies.

Figure 8-9 shows how nonoverlapping channels in the 2.4-GHz band can overlap their coverage areas to provide seamless roaming between AP coverage areas. A common WLAN design recommendation is to have a 10–15 percent overlap of coverage between adjoining cells.

Key Topic

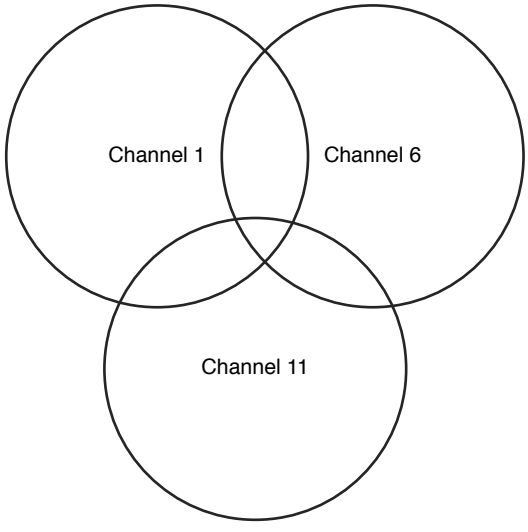


Figure 8-9 10 Percent to 15 Percent Coverage Overlap in Coverage Areas for Nonoverlapping Channels

If a WLAN has more than three APs, the APs can be deployed in a honeycomb fashion to allow an overlap of AP coverage areas while avoiding an overlap of identical channels. The example shown in Figure 8-10 shows an approach to channel selection for adjoining cells in the 2.4-GHz band. Notice that cells using the same nonoverlapping channels (channels 1, 6, and 11) are separated by another cell. For example, notice that none of the cells using channel 11 overlap another cell using channel 11.

Key Topic

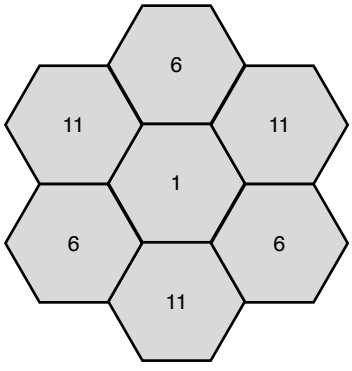


Figure 8-10 Nonoverlapping Coverage Cells for the 2.4-GHz Band

NOTE Although a honeycomb channel assignment scheme can be used for the 5-GHz band, identical channels should be separated by at least two cells, rather than the single cell shown for the 2.4-GHz band.

Securing Wireless LANs

WLANs introduce some unique concerns to your network. For example, improperly installed wireless APs are roughly equivalent to putting an Ethernet port in a building's parking lot, where someone can drive up and access your network. Fortunately, various features are available to harden the security of your WLAN, as discussed in this section.

Security Issues

In the days when dial-up modems were popular, malicious users could run a program on their computer to call all phone numbers in a certain number range. Phone numbers that answered with modem tone became targets for later attacks. This type of reconnaissance was known as *war dialing*. A modern-day variant of war dialing is *war driving*, where potentially malicious users drive around looking for unsecured WLANs. These users might be identifying unsecured WLANs for nefarious purposes or simply looking for free Internet access. Devices like cell phones, laptops, tablets, and gaming and media devices could act as wireless clients as well as be used in a wireless attack as they have potential WiFi access to the network.

Other WLAN security threats include the following:

Key Topic

- **War chalking:** Once an open WLAN (or a WLAN whose SSID and authentication credentials are known) is found in a public place, a user might write a symbol on a wall (or some other nearby structure) to let others know the characteristics of the discovered network. This practice, which is a variant of the decades-old practice of hobos leaving symbols as messages to fellow hobos, is called *war chalking*. Figure 8-11 shows common war-chalking symbols.

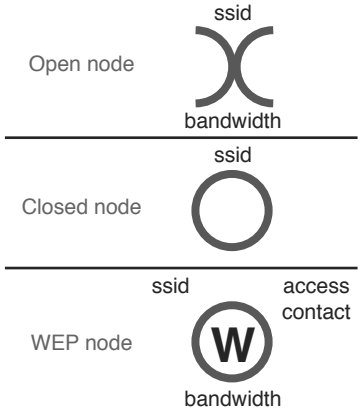


Figure 8-11 War-Chalking Symbols

- **WEP and WPA security cracking:** As discussed later in this chapter, various security standards are available for encrypting and authenticating a WLAN client with an AP. Two of the less secure standards include Wired Equivalent Privacy (WEP) and Wi-Fi Protected Access (WPA). Although WPA is considered more secure than WEP, utilities are available on the Internet for cracking each of these approaches to wireless security. By collecting enough packets transmitted by a secure AP, these cracking utilities can use mathematical algorithms to determine the preshared key (PSK) configured on a wireless AP, with which an associating wireless client must also be configured.
- **Rogue access point:** A malicious user could set up his own AP to which legitimate users would connect. Such an AP is called a *rogue access point*. That malicious user could then use a packet sniffer (which displays information about unencrypted traffic, including the traffic's data and header information) to eavesdrop on communications flowing through his AP. To cause unsuspecting users to connect to the rogue AP, the malicious user could configure the rogue AP with the same service set identifier (SSID) as used by a legitimate AP. When a rogue AP is configured with the SSID of a legitimate AP, the rogue AP is commonly referred to as an evil twin.

NOTE An SSID is a string of characters identifying a WLAN. APs participating in the same WLAN (in an ESS) can be configured with identical SSIDs. An SSID shared among multiple APs is called an *extended service set identifier* (ESSID).

Approaches to WLAN Security

A WLAN that does not require authentication or provide encryption for wireless devices (for example, a publicly available WLAN found in many airports) is said to be using *open authentication*. To protect WLAN traffic from eavesdroppers, a variety of security standards and practices have been developed, including the following:

Key Topic

- **MAC address filtering:** An AP can be configured with a listing of MAC addresses that are permitted to associate with the AP. If a malicious user attempts to connect via his laptop (whose MAC address is not on the list of trusted MAC addresses), that user is denied access. One drawback to MAC address filtering is the administrative overhead required to keep an approved list of MAC addresses up-to-date. Another issue with MAC address filtering is that a knowledgeable user could falsify the MAC address of his wireless network card, making his device appear to be approved.
- **Disabling SSID broadcast:** An SSID can be broadcast by an AP to let users know the name of the WLAN. For security purposes, an AP might be configured not to broadcast its SSID. However, knowledgeable users could still determine the SSID of an AP by examining captured packets.
- **Preshared key:** To encrypt transmission between a wireless client and an AP (in addition to authenticating a wireless client with an AP), both the wireless client and the AP could be preconfigured with a matching string of characters (a PSK, as previously described). The PSK could be used as part of a mathematical algorithm to encrypt traffic, such that if an eavesdropper intercepted the encrypted traffic, he would not be able to decrypt the traffic without knowing the PSK. Although using a PSK can be effective in providing security for a small network (for example, a SOHO network), it lacks scalability. For example, in a large corporate environment, a PSK being compromised would necessitate the reconfiguration of all devices configured with that PSK.

NOTE WLAN security based on a PSK technology is called *personal mode*.

- **IEEE 802.1X:** Rather than having all devices in a WLAN be configured with the same PSK, a more scalable approach is to require all wireless users to authenticate using their own credentials (for example, a username and password). Allowing each user to have his own set of credentials prevents the compromising of one password from impacting the configuration of all wireless devices. IEEE 802.1x is a technology that allows wireless clients to authenticate with an authentication server (typically, a Remote Authentication Dial-In User Service [RADIUS] server).

NOTE WLAN security based on IEEE 802.1x and a centralized authentication server such as RADIUS is called *enterprise mode*.

Chapter 4 discussed IEEE 802.1X in detail and described the role of a supplicant, an authenticator, and an authentication server, but Chapter 4 showed how IEEE 802.1X was used in a wired network. Figure 8-12 shows a wireless implementation of IEEE 8021X.

Key Topic

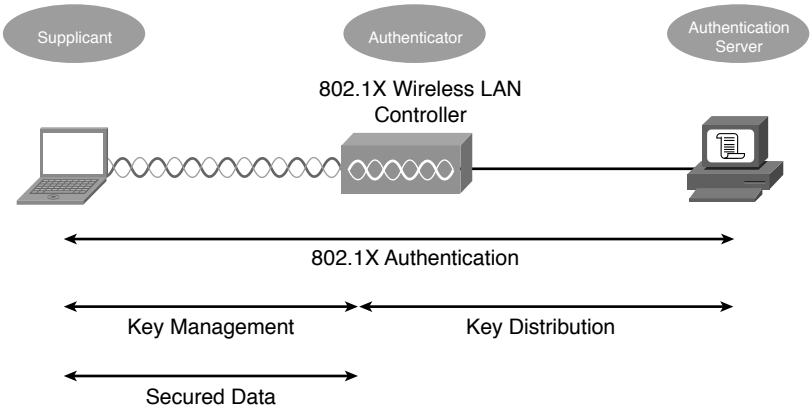


Figure 8-12 IEEE 802.1X Security for a WLAN

NOTE IEEE 802.1S works in conjunction with an Extensible Authentication Protocol (EAP) to perform its job of authentication. A variety of EAP types exist, including Lightweight Extensible Authentication Protocol (LEAP), EAP-Flexible Authentication via Secure Tunneling (EAP-FAST), EAP-Transport Layer Security (EAP-TLS), EAP-Tunneled Transport Layer Security (EAP-TTLS), Protected EAP–Generic Token Card (PEAP-GTC), and Protected EAP–Microsoft Challenge Handshake Authentication Protocol version 2 (PEAP-MSCHAPv2). Although these EAP types differ in their procedures, the overriding goal for each EAP type is to securely authenticate a supplicant and provide the supplicant and the authenticator a session key that can be used during a single session in the calculation of security algorithms (for example, encryption algorithms).

Security Standards

When configuring a wireless client for security, the most common security standards from which you can select are as follows:

- Wired Equivalent Privacy (WEP)
- Wi-Fi Protected Access (WPA)
- Wi-Fi Protected Access Version 2 (WPA2)

The following sections describe these standards in detail.

WEP

The original 802.11 standard did address security; however, the security was a WEP key. With WEP, an AP is configured with a static WEP key. Wireless clients needing to associate with an AP are configured with an identical key (making this a PSK approach to security). The 802.11 standard specifies a 40-bit WEP key, which is considered to be a relatively weak security measure.

Because a WEP key is a static string of characters, it could be compromised with a brute-force attack, where an attacker attempts all possible character combinations until a match for the WEP key is found. Another concern, however, is that WEP uses RC4 as its encryption algorithm.

NOTE RC4 (which stands for Ron's Code or Rivest Cipher because it was developed by Ron Rivest of RSA Security) is sometimes pronounced *arc 4*.

RC4 uses a 24-bit initialization vector (IV), which is a string of characters added to the transmitted data, such that the same plain-text data frame will never appear as the same WEP-encrypted data frame. However, the IV is transmitted in clear text. So, if a malicious user, using packet-capture software, captures enough packets having the same WEP key, and because the malicious user can see the IV in clear text, he can use a mathematical algorithm (which can be performed with WEP-cracking software found on the Internet) to determine the static WEP key.

Some WEP implementations support the use of a longer WEP key (for example, 128 bits instead of 40 bits), making a WEP key more difficult to crack; however, both the wireless clients and their AP must support the longer WEP key.

WPA

The Wi-Fi Alliance (a nonprofit organization formed to certify interoperability of wireless devices) developed its own security standard, WPA, to address the weaknesses of WEP. Some of the security enhancements offered by WPA include the following:

- WPA operating in enterprise mode can require a user to be authenticated before keys are exchanged.
- In enterprise mode, the keys used between a wireless client and an access point are temporary session keys.
- WPA uses Temporal Key Integrity Protocol (TKIP) for enhanced encryption. Although TKIP does rely on an initialization vector, the IV is expanded from WEP's 24-bit IV to a 48-bit IV. Also, broadcast key rotation can be used, which causes a key to change so quickly that an eavesdropper would not have time to exploit a derived key.
- TKIP leverages Message Integrity Check (MIC), which is sometimes referred to as *Message Integrity Code* (MIC). MIC can confirm that data was not modified in transit.

Although not typically written as WPA1, when you see the term *WPA*, consider it to be WPA Version 1 (WPA1). WPA Version 2, however, is written as *WPA2*.

WPA2

In 2004, the IEEE 802.11i standard was approved and required stronger algorithms for encryption and integrity checking than those seen in previous WLAN security protocols such as WEP and WPA. The requirements set forth in the IEEE 802.11i standard are implemented in the Wi-Fi Alliance's WPA Version 2 (WPA2) security

standard. WPA2 uses Counter Mode with Cipher Block Chaining Message Authentication Code Protocol (CCMP) for integrity checking and Advanced Encryption Standard (AES) for encryption. WPA2 that uses a centralized server for authenticating users is referred to as *Enterprise* mode. An implementation of WPA2 that uses a configured password or PSK instead of a centralized server is referred to as *Personal* mode.

Additional Wireless Options

Other wireless technologies, such as Bluetooth, infrared (IR), and near-field communications (NFC), which are often integrated into smartphones, can also provide connectivity for a personal-area network (PAN) or other short-range networking applications.

Real-World Case Study

Acme Inc. hired an outside contractor who specializes in WiFi. The consultants came in and did a needs assessment and performed a wireless site survey. Recommendations were then made about the need for 15 access points in the headquarters office spaces and three access points at each of the remote branch offices. Three wireless LAN controllers, one for each office, will be used to manage the respective access points. The management of the access points through the wireless LAN controllers will be done primarily through the headquarters office using the WAN that is connecting the branch offices to the headquarters office.

Because of the high number of other WiFi access points being used in the same building as the headquarters office, Acme Inc. decided to use the 5-GHz range (due to less competition in that space) and to use 802.11n.

For security, Acme will use WPA2 in conjunction with a RADIUS server. ACME will use Enterprise mode for authentication of each user before allowing them access on the wireless network(s). The RADIUS server is integrated with Microsoft Active Directory so that Acme will not have to re-create every user account; the RADIUS server can check with the Active Directory server to verify user credentials and passwords.

There are separate SSIDs set up that map to the various VLANs and departments that are currently on the wired network. There is also a separate SSID set up as a wireless guest network that has limited access but does provide Internet access for guest users.

Once in place, a site survey was done again to verify the signal strengths and to identify any interference related to the wireless implementation. A heat map was provided to visually represent the signal strengths in the coverage areas in the respective office space.

Summary

The main topics covered in this chapter are the following:

- Various components, technologies, and terms used in WLANs were identified.
- WLAN design considerations were presented, such as the selection of WLAN standards, bands, and nonoverlapping channels. Potential sources of interference were also identified.
- Some of the security risks posed by a WLAN were described and the technologies available for mitigating those risks were presented.

Exam Preparation Tasks

Review All the Key Topics

Review the most important topics from inside the chapter, noted with the Key Topic icon in the outer margin of the page. Table 8-4 lists these key topics and the page numbers where each is found.

Table 8-4 Key Topics for Chapter 8

Key Topic Element	Description	Page Number
Figure 8-1	Basic WLAN topology with a wireless router	269
Figure 8-2	Basic WLAN topology with a wireless access point	270
List	Antenna selection criteria	271
Figure 8-3	Omnidirectional antenna coverage	272
Figure 8-4	Unidirectional antenna coverage	272
Figure 8-5	Nonoverlapping channels in the 2.4-GHz band	274
List	Spread spectrum transmission methods	276
Table 8-3	Characteristics of 802.11 standards	278
Figure 8-6	Independent basic service set (IBSS) WLAN	279
Figure 8-7	Basic service set (BSS) WLAN	280
Figure 8-8	Extended service set (ESS) WLAN	281
List	Sources of interference	281
Figure 8-9	10 percent to 15 percent coverage overlap in coverage areas for nonoverlapping channels	281

Key Topic Element	Description	Page Number
Figure 8-10	Nonoverlapping coverage cells for the 2.4-GHz band	284
List	Wireless security threats	285
List	Security standards and best practices	286
Figure 8-12	IEEE 802.1X security for a WLAN	287

Complete Tables and Lists from Memory

Print a copy of Appendix D, "Memory Tables" (found on the DVD), or at least the section for this chapter, and complete the tables and lists from memory. Appendix E, "Memory Table Answer Key," also on the DVD, includes the completed tables and lists so you can check your work.

Define Key Terms

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

wireless access point (AP), wireless router, decibel (dB), omnidirectional antenna, unidirectional antenna, carrier sense multiple access collision avoidance (CSMA/CA), direct-sequence spread spectrum (DSSS), frequency-hopping spread spectrum (FHSS), orthogonal frequency-division multiplexing (OFDM), 802.11a, 802.11b, 802.11g, 802.11n, 802.11ac multiple input, multiple output (MIMO), channel bonding, independent basic service set (IBSS), basic service set (BSS), extended service set (ESS), war chalking, service set identifier (SSID), Wired Equivalent Privacy (WEP), Wi-Fi Protected Access (WPA), Wi-Fi Protected Access Version 2 (WPA2), Enterprise mode, Personal mode

Complete Chapter 8 Hands-On Lab in Network+ Simulator Lite

- Matching Wireless Standards and Terminology

Review Questions

The answers to these review questions are in Appendix A, "Answers to Review Questions."

1. What type of antenna, commonly used in wireless APs and wireless routers in SOHO locations, radiates relatively equal power in all directions?
   - **a.** Unidirectional
   - **b.** Yagi
   - **c.** Parabolic
   - **d.** Omnidirectional

2. When using the 2.4-GHz band for multiple access points in a WLAN located in the United States, which nonoverlapping channels should you select? (Choose three.)
   - **a.** 0
   - **b.** 1
   - **c.** 5
   - **d.** 6
   - **e.** 10
   - **f.** 11
   - **g.** 14

3. What technology do WLANs use to determine when they gain access to the wireless media?
   a. SPF
   b. CSMA/CA
   c. RSTP
   d. DUAL

4. What IEEE 802.11 variant supports a maximum speed of 54 Mbps and uses the 2.4-GHz band?
   a. 802.11a
   b. 802.11b
   c. 802.11g
   d. 802.11n

5. Which of the following is used by IEEE 802.11n to achieve high throughput through the use of multiple antennas for transmission and reception?
   a. MIMO
   b. DSSS
   c. FHSS
   d. LACP

6. A WLAN formed directly between wireless clients (without the use of a wireless AP) is referred to as what type of WLAN?
   a. Enterprise mode
   b. IBSS
   c. Personal mode
   d. BSS

7. When extending the range for a 2.4-GHz WLAN, you can use nonoverlapping channels for adjacent coverage cells. However, there should be some overlap in coverage between those cells (using nonoverlapping channels) to prevent a connection from dropping as a user roams from one coverage cell to another. What percentage of coverage overlap is recommended for these adjacent cells?
   a. 5 percent to 10 percent
   b. 10 percent to 15 percent
   c. 15 percent to 20 percent
   d. 20 percent to 25 percent

8. If a WLAN does not require a user to provide credentials to associate with a wireless AP and access the WLAN, what type of authentication is said to be in use?
   a. WEP
   b. SSID
   c. Open
   d. IV

9. WEP's RC4 approach to encryption uses a 24-bit string of characters added to transmitted data, such that the same plain-text data frame will never appear as the same WEP-encrypted data frame. What is this string of characters called?
   a. Initialization vector
   b. Chips
   c. Orthogonal descriptor
   d. Session key

10. What standard developed by the Wi-Fi Alliance implements the requirements of IEEE 802.11i?
   a. TKIP
   b. MIC
   c. WEP
   d. WPA2

Index

Numerics

A

B

C

D

E

F

G

H

I

J-K-L

M

N

O

P

Q

R

S

T

U

V

W

X-Y-Z