PEARSON IT

CYBERSECURITY CURRICULUM

SIXTH EDITION

NETWORKING ESSENTIALS

A CompTIA® Network+ N10-008 Textbook

JEFFREY S. BEASLEY
PIYASAT NILKAEW

NETWORKING ESSENTIALS: SIXTH EDITION
A COMPTIA NETWORK+ N10-008 TEXTBOOK

INSTRUCTOR EDITION

JEFFREY S. BEASLEY AND PIYASAT NILKAEW

Pearson

Networking Essentials: Sixth Edition

Instructor Edition

ISBN-13: 978-0-13-745582-9
ISBN-10: 0-13-745582-8

Library of Congress Control Number: 2021913557

ScoutAutomatedPrintCode

EDITOR-IN-CHIEF
Mark Taber

DIRECTOR, ITP PRODUCT MANAGEMENT
Brett Bartow

DEVELOPMENT EDITOR
Marianne Bartow

MANAGING EDITOR
Sandra Schroeder

PROJECT EDITOR
Mandie Frank

COPY EDITOR
Kitty Wilson

INDEXER
Ken Johnson

PROOFREADER
Abigail Manheim

TECHNICAL EDITOR
Chris Crayton

PEER REVIEWERS
DeAnnia Clements
Osman Guzide
Gene Carwile
Dr. Theodor Richardson

PUBLISHING COORDINATOR
Cindy Teeters

DESIGNER
Chuti Prasertsith

COMPOSITOR
codeMantra

CREDITS

Figure 1-8 Screenshot of The command prompt in Windows 10 © Microsoft 2020
Figure 1-9 Screenshot of A typical text screen result when entering the ipconfig /all command in the command window. © Microsoft 2020
Figure 1-15 courtesy for Linksys
Figure 1-18 courtesy Zoom Telephonics, Inc.
Figure 1-19 courtesy for Linksys
Figure 1-27 Screenshot of (a) An example of displaying the IP address for computer 1 using the ipconfig command in Windows and (b) an example of the displayed IP address in macOS for the built-in Ethernet connection © Microsoft 2020
Figure 2-34 Screenshot of DTX-1800 certification report: Failure due to a termination problem. ©Fluke Corporation
Figure 2-35 Screenshot of DTX-1800 certification report: Failure due to excessive insertion loss. ©Fluke Corporation
Figure 2-36 Screenshot of The certification report for Test 1, showing that a short jumper cable passes the CAT5e link test. ©Fluke Corporation
Figure 2-37 Screenshot of The results for Test 2, showing that the cable failed the CAT5e link test. ©Fluke Corporation
Figure 2-38 Screenshot of The Test 3 CAT5e link test, showing failures with attenuation. ©Fluke Corporation
Figure 2-39 Screenshot of A CAT5e link test, showing failures with delay skew (Test 4). ©Fluke Corporation
Unnumbered Figure 2-1 Screenshot of Answer the following questions related to the certification report shown here. ©Fluke Corporation
Unnumbered Figure 2-2 Screenshot of Answer the following questions related to the certification report shown here. ©Fluke Corporation
Unnumbered Figure 2-3 Screenshot of Answer the following questions related to the certification report shown here - OMNI Scanner. ©Fluke Corporation
Figure 4-7 Screenshot of An example of the information displayed when an association is formed between a client and an access point. © Microsoft 2020
Figure 4-8 Screenshot of An example of a lost association. © Microsoft 2020
Figure 4-18 Screenshot of The window for configuring Bluetooth settings on a Mac. © 2020 Apple Inc
Figure 4-19 Screenshot of The Mac window showing the settings for a file transfer. © 2020 Apple Inc
Figure 4-20 Screenshot of The Mac window showing that a text file is coming in from another Bluetooth device. © 2020 Apple Inc
Figure 4-28 Screenshot of The excellent signal quality measured for the multipoint distribution. © Microsoft 2020
Figure 4-29 Screenshot of The poor signal quality measured at the remote site near the lake. © Microsoft 2020
Figure 5-7 Screenshot of The data traffic captured by computer 2 for the LAN using a hub. © Microsoft 2020
Figure 5-8 Screenshot of The data traffic captured by computer 2 for the LAN using a switch. © Microsoft 2020
Figure 5-9 Screenshot of The startup menu of a Cisco Catalyst switch in the CNA software. © Microsoft 2020
Figure 5-10 Screenshot of The highlighted ports showing the current connections and the location of the stacked switches icon. © Microsoft 2020
Figure 5-11 Screenshot of The window listing the MAC addresses currently connected to a switch. © Microsoft 2020
Figure 5-13 Screenshot of Configuring an IP address on an interface. © Microsoft 2020
Figure 5-19 Screenshot of Putty configuration © 1997-2020 Simon Tatham
Figure 5-20 Screenshot of The HyperTerminal Connect To dialog © 1997-2020 Simon Tatham
Figure 5-21 Screenshot of The Properties dialogs for configuring the serial port connection PuTTY © 1997-2020 Simon Tatham
Figure 5-23 Screenshot of The macOS dialog for configuring the settings for the serial interface. © 2020 Apple Inc
Figure 5-24 Screenshot of The macOS dialog for setting the serial port to PL2303-000. © 2020 Apple Inc
Figure 5-25 Screenshot of The macOS window listing the serial communication link settings. © 2020 Apple Inc
Figure 6-6 Screenshot of An example of the three packets exchanged in the initial TCP handshake. © Microsoft 2020
Figure 6-8 Screenshot of An example of the four-packet TCP connection termination. © Microsoft 2020
Figure 6-10 Screenshot of An example of a UDP packet transfer. © Microsoft 2020
Figure 6-12 Screenshot of Captured packets showing the (a) ARP request and the (b) ARP reply. © Microsoft 2020
Figure 6-13 Screenshot of The details of the ARP broadcast packet. © Microsoft 2020
Figure 6-14 Screenshot of An example of the use of hex numbers in data packets. © Microsoft 2020
Figure 7-3 Screenshot of The TCP/IP dialog for setting the default gateway address for computer A1. © Microsoft 2020
Figure 7-6 Screenshot of The Net-Challenge screen. © Microsoft 2020
Figure 7-7 Screenshot of The check box window for the Net-Challenge software User EXEC Mode challenge. © Microsoft 2020

Figure 7-8 Screenshot of The display for step 6, using the show command. © Microsoft 2020

Figure 7-11 Screenshot of The network topology for Net-Challenge. The arrows indicate where to click to display the router IP address configurations. © Microsoft 2020

Figure 7-14 Screenshot of An example of the port management options available with a Cisco switch: (a) Speed auto-negotiation option; (b) Duplex auto option. © Microsoft 2020

Figure 9-1a Screenshot of Setting the default gateway address or default static route on a host computer (PC). © Microsoft 2020

Figure 9-1b Screenshot of Setting the default gateway address or default static route on a host computer (macOS). © Microsoft 2020

FIG10-4 Screenshot of Captured DHCP packets. © Microsoft 2020

FIG10-9 Screenshot of An example of using an SNMP software management tool to obtain descriptions of a router's interfaces using the MIB ifDescr. © Microsoft 2020

FIG10-11 Screenshot of Using an SNMP software management tool to obtain interface speed settings. © Microsoft 2020

FIG10-12 Screenshot of An example of using SNMP to collect data traffic statistics. © Microsoft 2020

FIG10-23 Screenshot of Initializing Wireshark to capture data packets from a network. © Microsoft 2020

FIG10-24 Screenshot of Starting a capture. © Microsoft 2020

FIG10-25 Screenshot of The captured packets showing the ping from computer 1 to computer 2. © Microsoft 2020

FIG10-26 Screenshot of Computer 2 replying to computer 1 with its MAC address. © Microsoft 2020

FIG10-27 Screenshot of Computer 1 is sending an echo request to computer 2. © Microsoft 2020

FIG10-28 Screenshot of The echo reply received by computer 1. © Microsoft 2020

FIG10-30 Screenshot of (a) The beginning of the FTP data packet transfer and the request for an ASCII data transfer by the client. (b) The FTP data packet transfer and the closing of the FTP transfer. © Microsoft 2020

FIG10-31 Screenshot of Figure for problems 64–68. © Microsoft 2020

FIG11-9 Screenshot of Windows Firewall in Windows 10. © Microsoft 2020

FIG11-10 Screenshot of Windows 10 Firewall status. © Microsoft 2020

FIG11-11 Screenshot of Windows 10 allowed apps. © Microsoft 2020

FIG11-12 Screenshot of Windows 10 advanced firewall settings. © Microsoft 2020

FIG11-13 Screenshot of Windows 10 echo request properties. © Microsoft 2020

FIG11-14 Screenshot of Windows 10 echo request protocols and ports. © Microsoft 2020

FIG11-15 Screenshot of macOS firewall. © 2020 Apple Inc

FIG11-16 Screenshot of macOS advanced settings. © 2020 Apple Inc

FIG11-17 Screenshot of Linux iptables © The Netfilter's webmasters

FIG11-19 Screenshot of An example of setting WEP encryption on a wireless client. © Microsoft 2020

FIG11-26 Screenshot of The traceroute from the VPN server to the VPN remote client. © Microsoft 2020

FIG11-27 Screenshot of The first window, the VPN Client status window, is displayed after starting the VPN client software. © Cisco systems

FIG11-28 Screenshot of The connection screen for establishing a VPN link. © Cisco systems

FIG11-29 Screenshot of The initial handshake screen for the VPN client. © Cisco systems

FIG11-30 Screenshot of The menu showing that the VPN client has successfully connected to the virtual private network. © Cisco systems

FIG11-31 Screenshot of The Preferences window for the VPN client. © Cisco systems

FIG11-32 Screenshot of The Statistics window (a) and Route Details window (b) for the VPN client. © Cisco systems

FIG12-1 Screenshot of Enabling Hyper-V © Microsoft 2020

FIG12-2 Screenshot of Using Hyper-V Manager © Microsoft 2020

FIG12-3 Screenshot of Creating a virtual switch in Hyper-V © Microsoft 2020

FIG12-4 Screenshot of Specifying the name of a virtual switch © Microsoft 2020

FIG12-5 Screenshot of Creating a virtual machine © Microsoft 2020

FIG12-6 Screenshot of Specifying the name and location of a virtual machine. © Microsoft 2020

FIG12-7 Screenshot of Specifying the generation of the virtual machine © Microsoft 2020

FIG12-8 Screenshot of Specifying the desired memory size for a VM. © Microsoft 2020

FIG12-9 Screenshot of Selecting the connection name of the virtual switch. © Microsoft 2020

FIG12-10 Screenshot of Specifying a virtual hard disk name, location, and size. © Microsoft 2020

FIG12-11 Screenshot of The options for installing the VM's operating system. © Microsoft 2020

FIG12-12 Screenshot of Starting the new VM. © Microsoft 2020

FIG12-13 Screenshot of The final VM screen, showing that the machine is up. © Microsoft 2020

Peter Mell (NIST), Tim Grance (NIST), The NIST Definition of Cloud Computing, SP 800-145

Cover Artistdesign29/Shutterstock

CONTENTS AT A GLANCE

Online Only Elements:

CONTENTS

Online Only Elements:

ABOUT THE AUTHORS

Jeffrey S. Beasley is a professor emeritus in the Information and Communications Technology program at New Mexico State University, where he taught computer networking and many related topics. He is coauthor of *Modern Electronic Communication*, ninth edition, the author of *Networking,* second edition, and *co-author of Networking Essentials,* fifth edition, and *A Practical Guide to Advanced Networking*.

Piyasat Nilkaew is the director of Computing and Networking Infrastructure at New Mexico State University and has more than 20 years of experience in network management and consulting. He has extensive expertise in deploying and integrating multiprotocol and multivendor data, voice, and video network solutions. He is co-author of *Networking Essentials,* fifth edition, and *A Practical Guide to Advanced Networking.*

ABOUT THE TECHNICAL REVIEWER

Chris Crayton is a technical consultant, trainer, author, and industry-leading technical editor. He has worked as a computer technology and networking instructor, information security director, network administrator, network engineer, and PC specialist. Chris has authored several print and online books on PC repair, CompTIA A+, CompTIA Security+, and Microsoft Windows. He has also served as technical editor and content contributor on numerous technical titles for several of the leading publishing companies. He holds numerous industry certifications, has been recognized with many professional and teaching awards, and has served as a state-level SkillsUSA final competition judge. Chris tech edited and contributed to this book to make it better for students and those wishing to better their lives.

DEDICATIONS

This book is dedicated to my family: Kim, Damon/Heather, and Dana/Sam. —Jeff Beasley

This book is dedicated to my family: Boonsong, Pariya, June, Ariya, and Atisat. —Piyasat Nilkaew

ACKNOWLEDGMENTS

I am grateful to the many people who have helped with this text. My sincere thanks go to the following technical consultants:

- Danny Bosch and Matthew Peralta for sharing their expertise with optical networks and unshielded twisted-pair cabling
- Don Yates for his help with the initial Net-Challenge software

I would also like to thank my many past and present students for their help with this book:

- Abel Sanchez, Kathryn Sager, and Joshua Cook for their work on the Net-Challenge software; Adam Segura for his help taking pictures of the steps for CAT6 termination; Marc Montez, Carine George-Morris, Brian Morales, Michael Thomas, Jacob Ulibarri, Scott Leppelman, and Aarin Buskirk for their help with laboratory development; Josiah Jones and Raul Marquez Jr. for their help with the Wireshark material; and Ariya Nilkaew for her help with revising and editing many of the captured pictures

- Aaron Shapiro and Aaron Jackson for their help testing the many network connections presented in the text
- Paul Bueno and Anthony Bueno for reading through an early draft of the text

Your efforts are greatly appreciated.

We appreciate the excellent feedback of the following reviewers: Phillip Davis, DelMar College, Texas; Thomas D. Edwards, Carteret Community College, North Carolina; William Hessmiller, Editors & Training Associates; Bill Liu, DeVry University, California; and Timothy Staley, DeVry University, Texas.

Our thanks to the people at Pearson for making this project possible. Thanks to Brett Bartow for providing us with the opportunity to work on the sixth edition and for helping make this process enjoyable. Thanks to Marianne Bartow, to all the people at Pearson IT Certification, and also to the many technical editors for their help editing the manuscript.

Special thanks to our families for their continued support and patience.

—Jeffrey S. Beasley and Piyasat Nilkaew

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 and email address. We will carefully review your comments and share them with the authors and editors who worked on the book.

Email: community@informit.com

INTRODUCTION

This book provides a look at computer networking from the point of view of a network administrator. It guides readers from an entry-level knowledge of computer networks to advanced concepts related to Ethernet networks; router configuration; TCP/IP networks; routing protocols; local, campus, and wide area network configuration; network security; wireless networking; optical networks; voice over IP; network servers; and Linux networking. After reading the entire text, you will have gained a solid knowledge base in computer networks.

In our years of teaching, we have observed that technology students prefer to learn "how to swim" after they have gotten wet and taken in a little water. Then they are ready for more challenges. In this book, we therefore show you the technology, how it is used, and why, and you can take the applications of the technology to the next level. Allowing you to experiment with the technology helps you develop a greater understanding.

ORGANIZATION OF THE TEXT

This book has been thoroughly updated to reflect the latest version of the CompTIA Network+ exam. *Networking Essentials,* sixth edition, is a practical, up-to-date, and hands-on guide to the basics of networking. Written from the viewpoint of the network administrator, it requires absolutely no previous experience with either network concepts or day-to-day network management. Throughout the text, you will gain an appreciation of how basic computer networks and related hardware are interconnected to form a network. You will come to understand the concepts of twisted-pair cable, fiber optics, LANs interconnection, TCP/IP configuration, subnet masking, basic router configuration, switch configuration and management, wireless networking, and network security.

The textbook's companion website contains laboratory exercises, the Net-Challenge software, Wireshark captures, and the Network+ terminology quizzes.

Key Pedagogical Features

- The *Chapter Outline, Network+ Objectives, Key Terms,* and *Introduction* at the beginning of each chapter clearly outline specific goals for you, the reader. Figure I-1 shows an example of these features.

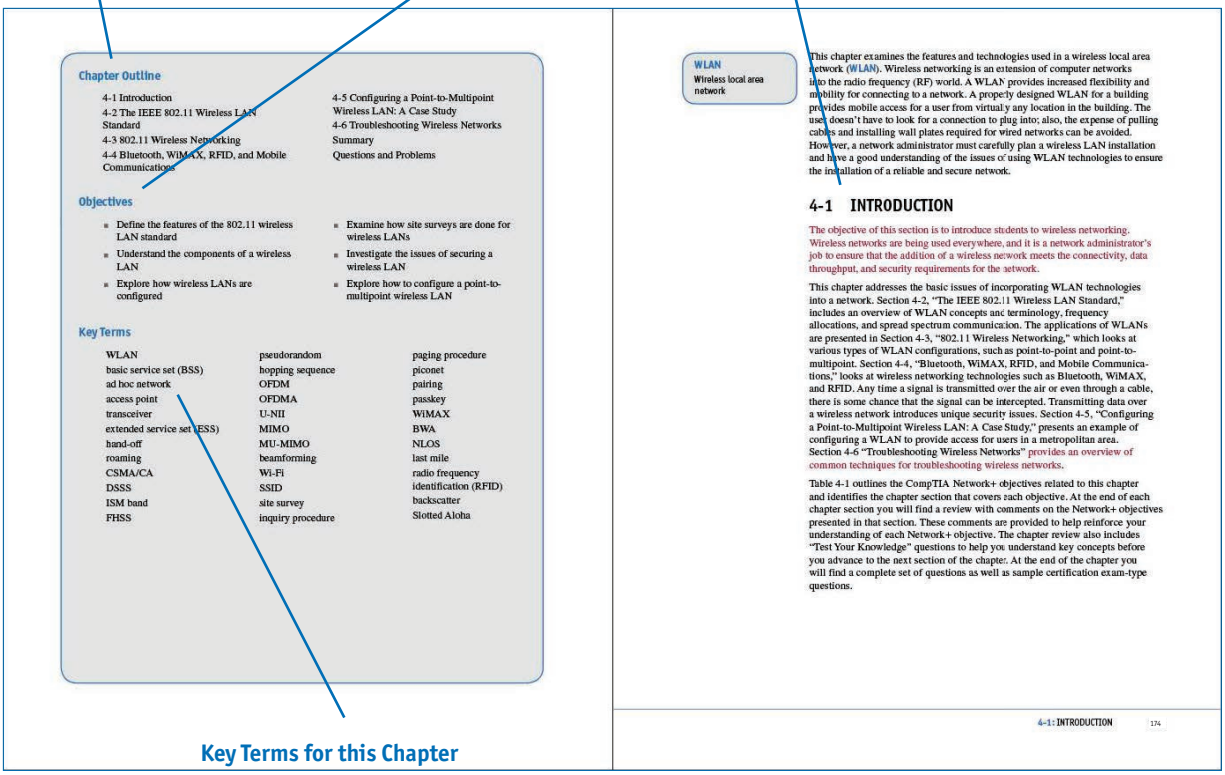


FIGURE I-1

- The *Net-Challenge software* provides simulated hands-on experience configuring routers and switches. Exercises provided in the text (see Figure I-2) and companion website challenge you to undertake certain router/network configuration tasks. These challenges help you check your ability to enter basic networking commands and to set up router functions, such as configuring the interface (Ethernet and serial) and routing protocols (for example, RIP, static). The software has the look and feel of actually being connected to a router's console port.

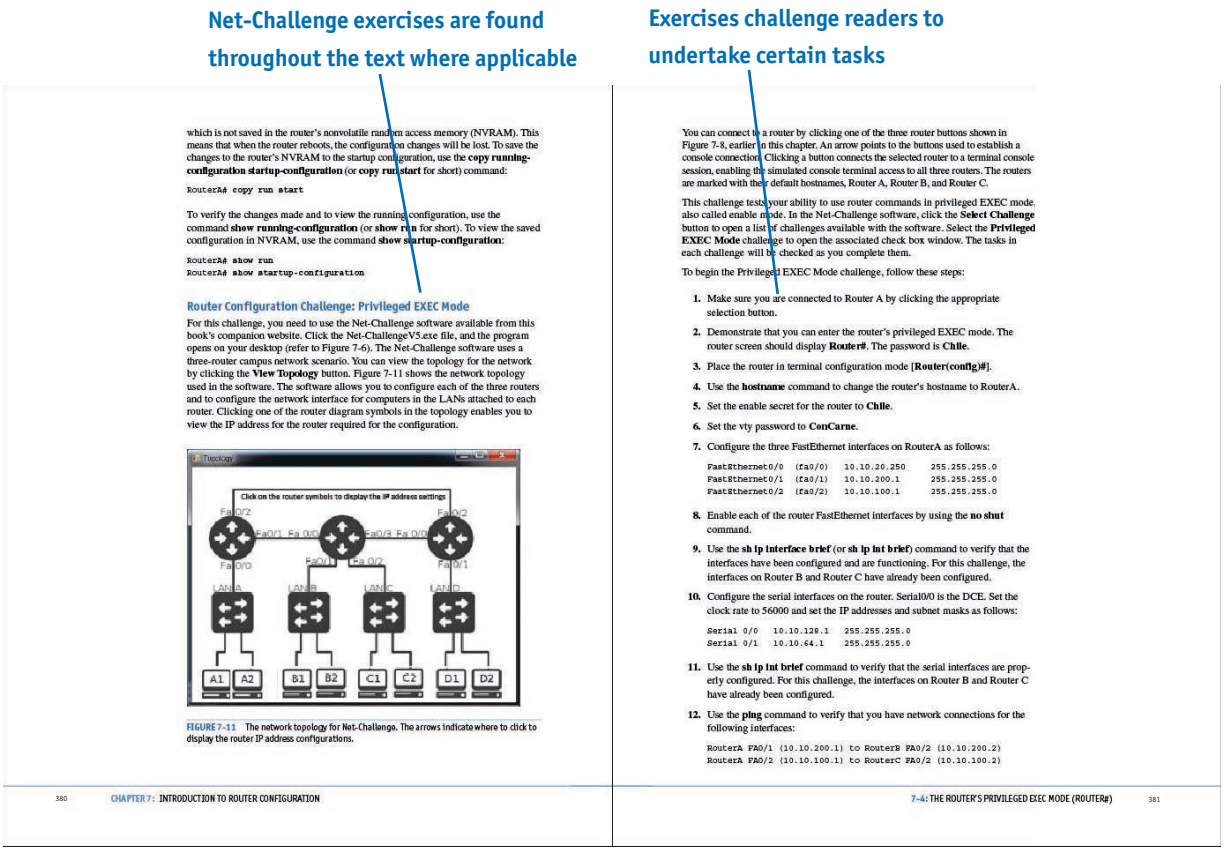
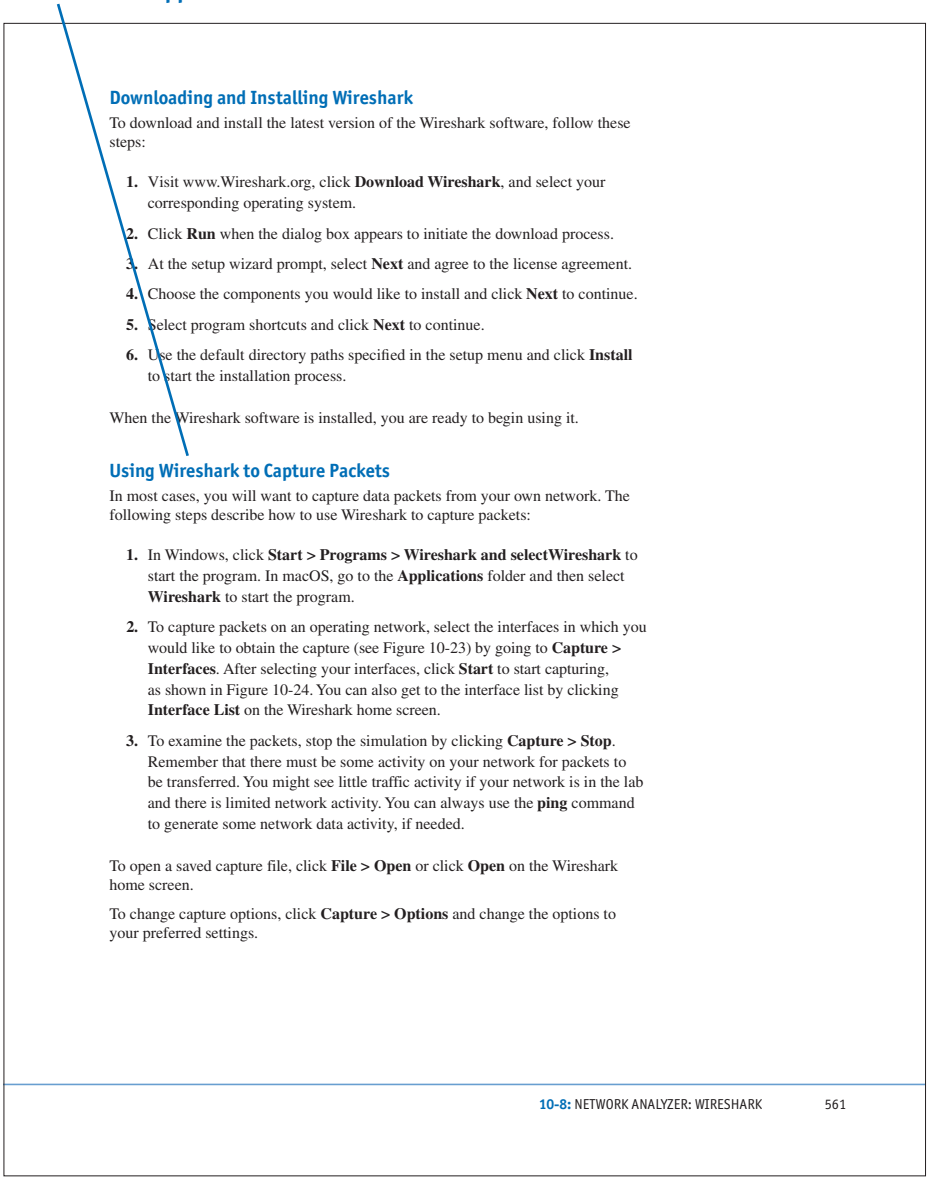


FIGURE I-2

- The textbook features and introduces how to use the *Wireshark network protocol analyzer.* Examples of using the software to analyze data traffic are included throughout the text. *Numerous worked-out examples* are included in every chapter to reinforce key concepts and aid in subject mastery, as shown in Figure I-3.

Examples using the Wireshark protocol analyzer are included throughout the text where applicable



Downloading and Installing Wireshark

To download and install the latest version of the Wireshark software, follow these steps:

1. Visit www.Wireshark.org, click **Download Wireshark**, and select your corresponding operating system.
2. Click **Run** when the dialog box appears to initiate the download process.
3. At the setup wizard prompt, select **Next** and agree to the license agreement.
4. Choose the components you would like to install and click **Next** to continue.
5. Select program shortcuts and click **Next** to continue.
6. Use the default directory paths specified in the setup menu and click **Install** to start the installation process.

When the Wireshark software is installed, you are ready to begin using it.

Using Wireshark to Capture Packets

In most cases, you will want to capture data packets from your own network. The following steps describe how to use Wireshark to capture packets:

1. In Windows, click **Start > Programs > Wireshark and selectWireshark** to start the program. In macOS, go to the **Applications** folder and then select **Wireshark** to start the program.
2. To capture packets on an operating network, select the interfaces in which you would like to obtain the capture (see Figure 10-23) by going to **Capture > Interfaces**. After selecting your interfaces, click **Start** to start capturing, as shown in Figure 10-24. You can also get to the interface list by clicking **Interface List** on the Wireshark home screen.
3. To examine the packets, stop the simulation by clicking **Capture > Stop**. Remember that there must be some activity on your network for packets to be transferred. You might see little traffic activity if your network is in the lab and there is limited network activity. You can always use the **ping** command to generate some network data activity, if needed.

To open a saved capture file, click **File > Open** or click **Open** on the Wireshark home screen.

To change capture options, click **Capture > Options** and change the options to your preferred settings.

FIGURE I-3

- *Key Terms* and their definitions are highlighted in the margins to foster inquisitiveness and ensure retention. Illustrations and photos are used throughout to aid in understanding the concepts discussed (see Figure I-4).

Key terms are highlighted in the text and defined in the margin

Extended Service Set (ESS)
A network with multiple access points to extend user mobility

Hand-off
The process in which a user's computer establishes an association with another access point

Roaming
The term used to describe a user's ability to maintain network connectivity while moving through the workplace

CSMA/CA
Carrier sense multiple access with collision avoidance

The users (clients) in the wireless LAN can communicate with other members of the network as long as a link is established with the access point. For example, data traffic from PC-A to PC-E first passes through the access point and then to PC-E in the wired LAN.

The problem with a basic service set is that mobile users can travel outside the radio range of a station's wireless link if there is only one access point. One solution is to add multiple access points to the network. Multiple access points extend the range of mobility of a wireless client in the LAN. This arrangement is called an **extended service set (ESS)**. In the example of an ESS in Figure 4-3, the mobile computer establishes an authorized connection with the access point that has the strongest signal level (for example, AP-1). As the user moves, the strength of the signal from AP-1 decreases. At some point, the signal strength from AP-2 exceeds that from AP-1, and the wireless bridge establishes a new connection with AP-2. This is called a **hand-off**. The hand-off is an automatic process for the wireless client adapter in 802.11, and the term used to describe this is **roaming**.

Network access in 802.11 uses a technique called carrier sense multiple access with collision avoidance (CSMA/CA). In **CSMA/CA**, the client station listens for other users of the wireless network. If the channel is quiet (that is, no data transmission is occurring), the client station can transmit. If the channel is busy, the station(s) must wait until transmission stops. Each client station uses a unique random back-off time. This technique prevents client stations from trying to gain access to the wireless channel as soon as it becomes quiet. Currently four physical layer technologies are being used in 802.11 wireless networking: direct-sequence spread spectrum (DSSS), frequency-hopping spread spectrum (FHSS), infrared, and orthogonal frequency-division multiplexing (OFDM). DSSS is used in 802.11b/g/n wireless networks, and OFDM is used in 802.11a, 802.11g, 802.11n, 802.11ac, and 802.11ax.

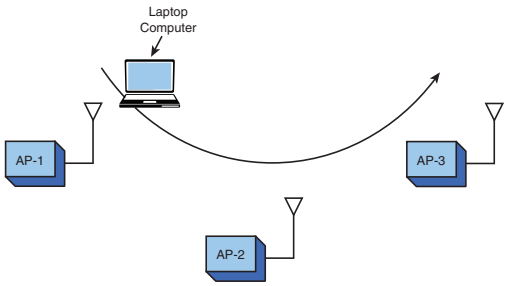


FIGURE 4-3 An example of an extended service set used for increased user mobility.

FIGURE I-4

- A *Summary, Questions and Problems, Critical Thinking*, and *Certification Questions* are provided at the end of each chapter, as shown in Figure I-5

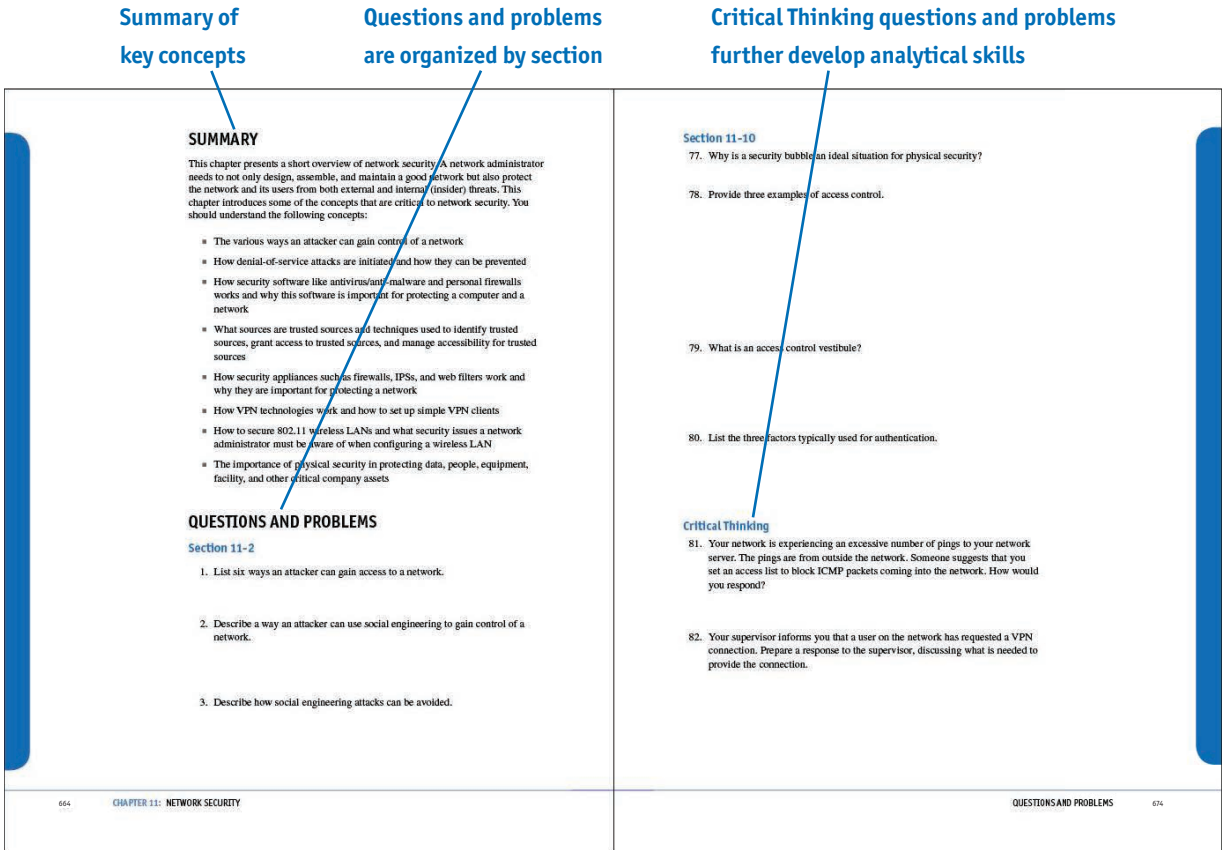


FIGURE I-5

- An extensive *Glossary* at the end of the book offers quick, accessible definitions to key terms and acronyms, and this book also includes an exhaustive *Index* (see Figure I-6).

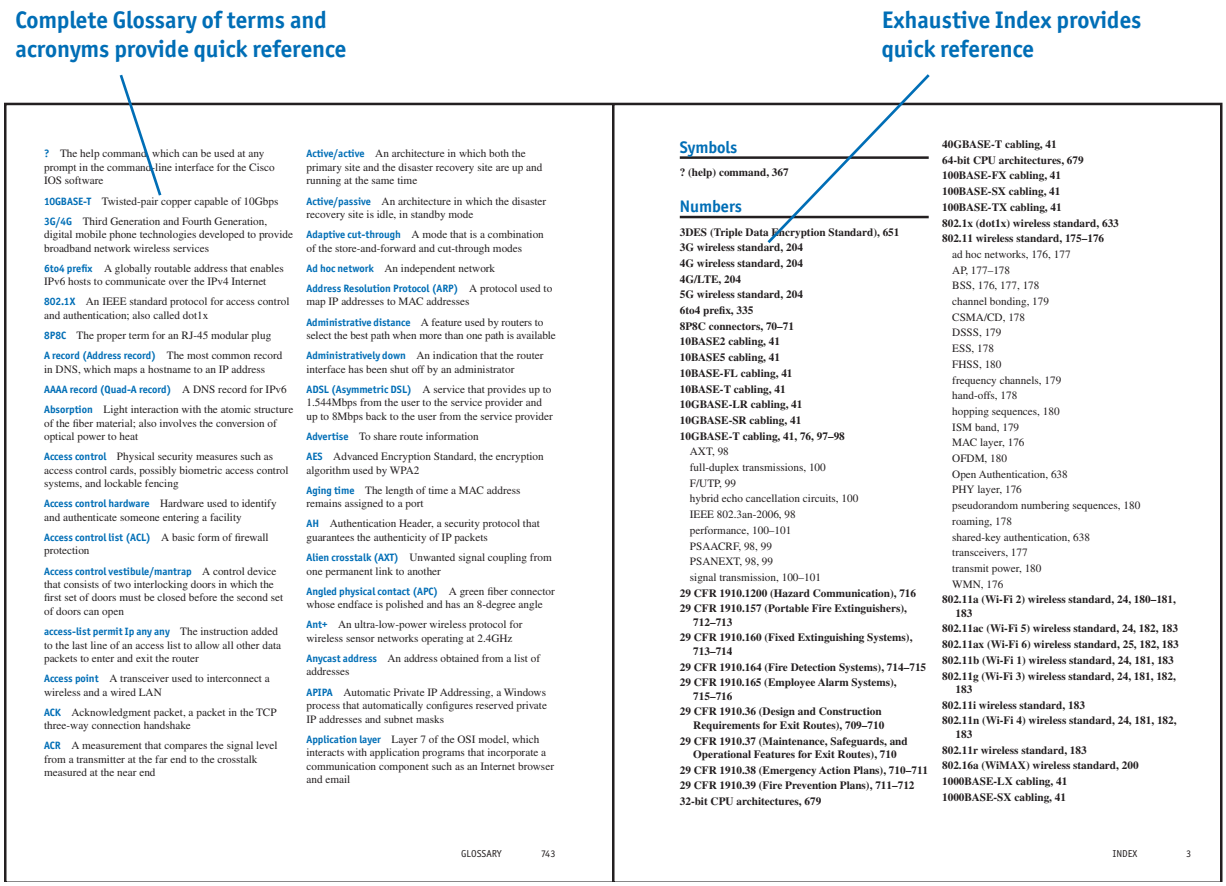


FIGURE I-6

Companion Website

The companion website includes the captured data packets used throughout the book. It also includes the NetChallenge software, which was developed specifically for this text. The companion website also includes chapter-based quiz modules for you to test your knowledge and all of the key terms in an online flash card application. Finally, you can access your 10% off Network+ exam voucher from the companion website.

4
CHAPTER

Wireless Networking

Chapter Outline

Objectives

- Define the features of the 802.11 wireless LAN standard
- Understand the components of a wireless LAN
- Explore how wireless LANs are configured
- Examine how site surveys are done for wireless LANs
- Investigate the issues of securing a wireless LAN
- Explore how to configure a point-to-multipoint wireless LAN

Key Terms

WLAN
basic service set (BSS)
ad hoc network
access point
transceiver
extended service set (ESS)
hand-off
roaming
CSMA/CA
DSSS
ISM band
FHSS
pseudorandom
hopping sequence
OFDM
OFDMA
U-NII
MIMO
MU-MIMO
beamforming
Wi-Fi
SSID
site survey
inquiry procedure
paging procedure
piconet
pairing
passkey
WiMAX
BWA
NLOS
last mile
radio frequency identification (RFID)
backscatter
Slotted Aloha

WLAN
Wireless local area network

This chapter examines the features and technologies used in a wireless local area network (**WLAN**). Wireless networking is an extension of computer networks into the radio frequency (RF) world. A WLAN provides increased flexibility and mobility for connecting to a network. A properly designed WLAN for a building provides mobile access for a user from virtually any location in the building. The user doesn't have to look for a connection to plug into; also, the expense of pulling cables and installing wall plates required for wired networks can be avoided. However, a network administrator must carefully plan a wireless LAN installation and have a good understanding of the issues of using WLAN technologies to ensure the installation of a reliable and secure network.

4-1 INTRODUCTION

The objective of this section is to introduce students to wireless networking. Wireless networks are being used everywhere, and it is a network administrator's job to ensure that the addition of a wireless network meets the connectivity, data throughput, and security requirements for the network.

This chapter addresses the basic issues of incorporating WLAN technologies into a network. Section 4-2, "The IEEE 802.11 Wireless LAN Standard," includes an overview of WLAN concepts and terminology, frequency allocations, and spread spectrum communication. The applications of WLANs are presented in Section 4-3, "802.11 Wireless Networking," which looks at various types of WLAN configurations, such as point-to-point and point-to-multipoint. Section 4-4, "Bluetooth, WiMAX, RFID, and Mobile Communications," looks at wireless networking technologies such as Bluetooth, WiMAX, and RFID. Any time a signal is transmitted over the air or even through a cable, there is some chance that the signal can be intercepted. Transmitting data over a wireless network introduces unique security issues. Section 4-5, "Configuring a Point-to-Multipoint Wireless LAN: A Case Study," presents an example of configuring a WLAN to provide access for users in a metropolitan area. Section 4-6 "Troubleshooting Wireless Networks" provides an overview of common techniques for troubleshooting wireless networks.

Table 4-1 outlines the CompTIA Network+ objectives related to this chapter and identifies the chapter section that covers each objective. At the end of each chapter section you will find a review with comments on the Network+ objectives presented in that section. These comments are provided to help reinforce your understanding of each Network+ objective. The chapter review also includes "Test Your Knowledge" questions to help you understand key concepts before you advance to the next section of the chapter. At the end of the chapter you will find a complete set of questions as well as sample certification exam-type questions.

TABLE 4-1 **Chapter 4 CompTIA Network+ Objectives**

Domain/Objective Number	Domain/Objective Description	Section Where Objective Is Covered
1.0	**Networking Fundamentals**	
1.2	Explain the characteristics of network topologies and network types.	4-2
1.3	Summarize the types of cables and connectors and explain which is the appropriate type for a solution.	4-4
1.6	Explain the use and purpose of network services.	4-2, 4-3
1.7	Explain basic corporate and datacenter network architecture.	4-4
2.0	**Network Implementations**	
2.1	Compare and contrast various devices, their features, and their appropriate placement on the network.	4-2, 4-3, 4-4, 4-5
2.3	Given a scenario, configure and deploy common Ethernet switching features.	4-2, 4-4
2.4	Given a scenario, install and configure the appropriate wireless standards and technologies.	4-2, 4-3, 4-4, 4-5
3.0	**Network Operations**	
3.1	Given a scenario, use the appropriate statistics and sensors to ensure network availability.	4-2, 4-3, 4-4
3.2	Explain the purpose of organizational documents and policies.	4-3, 4-5
3.3	Explain high availability and disaster recovery concepts and summarize which is the best solution.	4-2, 4-5
4.0	**Network Security**	
4.3	Given a scenario, apply network hardening techniques.	4-2, 4-4, 4-5
4.4	Compare and contrast remote access methods and security implications.	4-2
5.0	**Network Troubleshooting**	
5.2	Given a scenario, troubleshoot common cable connectivity issues and select the appropriate tools.	4-2, 4-3, 4-4
5.4	Given a scenario, troubleshoot common wireless connectivity issues.	4-2, 4-3, 4-5, 4-6
5.5	Given a scenario, troubleshoot general networking issues.	4-4

4-2 THE IEEE 802.11 WIRELESS LAN STANDARD

The anatomy of 802.11 wireless networking is presented in this section. This section introduces the basic service set wireless network, the extended service set, the independent basic service set (ad hoc), the frequencies used for wireless networks, the power output, and spread spectrum communications. Many topics are presented, including the 802.11 wireless (Wi-Fi) standards. Students need to be aware of these topics to fully comprehend how a wireless network functions.

A typical computer network uses twisted-pair and fiber-optic cable to interconnect LANs. Another media option competing for use in higher-data-rate LANs is

wireless, based on the IEEE 802.11 wireless standard. The advantages of wireless include the following:

- It is cost-effective for use in areas that are difficult or too costly to wire.
- It enables user mobility in the workplace.

Wireless networks have become the network of choice in environments such as homes, small offices, and public places. Being able to connect to a network without a wire is convenient for users, and the cost is relatively low. In the age of laptops and mobile devices, wireless opens the door to user mobility in the workplace, and user mobility provides flexibility. Workers can potentially access the network or wireless data services from virtually any location within the workplace. Accessing information from the network is as easy as if the information were on a USB drive.

The benefits of wireless networks in the workplace are numerous. To provide wireless connectivity, a network administrator must be sure the network services are reliable and secure. In order to provide reliable network services, an administrator must have a good understanding of WLAN configurations and technologies. This and the following sections examine the fundamentals of wireless networking, the 802.11 standard and its family (802.11a, 802.11b, 802.11g, 802.11n, 802.11ac, and 802.11ax), and how WLANs are configured.

The IEEE 802.11 WLAN standard defines the physical (PHY) layer, the media access control (MAC) layer, and the MAC management protocols and services.

The PHY layer defines the following:

- The method of transmitting the data, which can be either RF or infrared (although infrared is rarely used)
- How it interfaces with the MAC layer
- The reliability of the data service
- Access control to the shared wireless medium
- Privacy protection for transmitted data

The wireless management protocols and services are authentication, association, data delivery, and privacy.

Basic Service Set (BSS)
An independent network

Ad hoc network
An independent network

The fundamental topology of a WLAN is the **basic service set (BSS)**. This is also called the independent basic service set, or **ad hoc network**. Figure 4-1 provides an example of an ad hoc network. In this network, the wireless clients (stations) communicate directly with each other. This means the clients have recognized the other stations in the WLAN and have established a wireless data link.

A related concept is a wireless mesh network (WMN), which is a communications network made up of Wi-Fi radios connected in a mesh topology (that is, a heavily interconnected network). A WMN is basically a wireless ad hoc network.

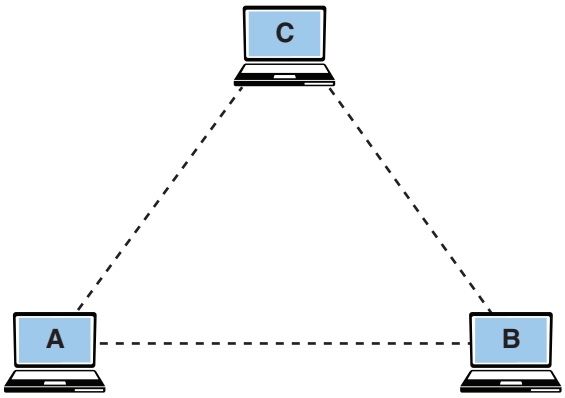


FIGURE 4-1 An example of an independent basic service set, or ad hoc, network.

The performance of the basic service set can be improved by including an **access point**, which is a transmit/receive unit (**transceiver**) that interconnects data from the wireless LAN to the wired network. In addition, the access point provides 802.11 MAC layer functions and supports bridge protocols. The access point typically uses an RJ-45 jack for connecting to the wired network. If an access point is being used, users establish a wireless communications link through it to communicate with other users in the WLAN or the wired network, as shown in Figure 4-2.

Access Point
A transceiver used to interconnect a wireless LAN and a wired LAN

Transceiver
A transmit/receive unit

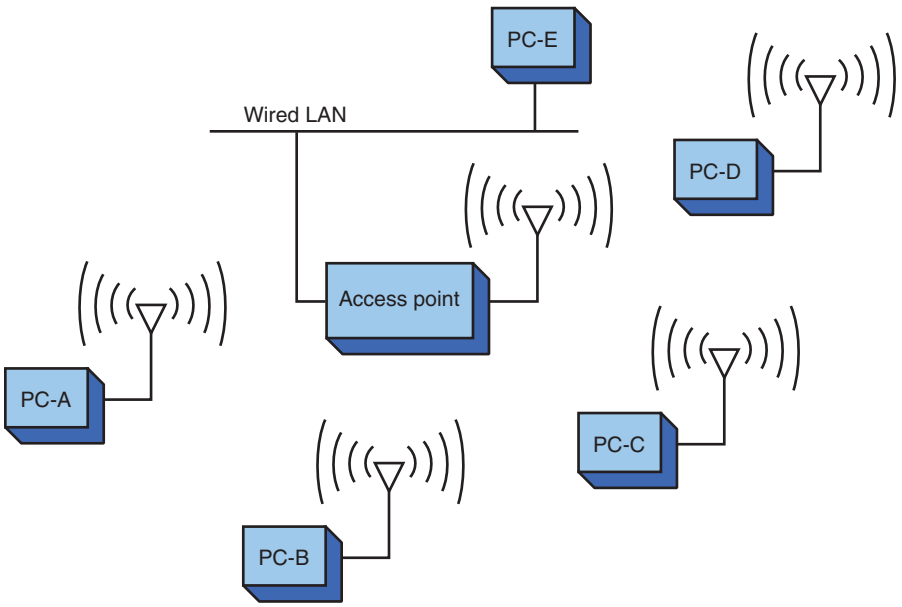


FIGURE 4-2 Adding an access point to a basic service set.

If data is being sent from PC-A to PC-D in the network shown in Figure 4-2, the data is first sent to the access point and then relayed to PC-D. Data sent from a wireless client to a client in the wired LAN also passes through the access point.

Extended Service Set (ESS)
A network with multiple access points to extend user mobility

Hand-off
The process in which a user's computer establishes an association with another access point

Roaming
The term used to describe a user's ability to maintain network connectivity while moving through the workplace

CSMA/CA
Carrier sense multiple access with collision avoidance

The users (clients) in the wireless LAN can communicate with other members of the network as long as a link is established with the access point. For example, data traffic from PC-A to PC-E first passes through the access point and then to PC-E in the wired LAN.

The problem with a basic service set is that mobile users can travel outside the radio range of a station's wireless link if there is only one access point. One solution is to add multiple access points to the network. Multiple access points extend the range of mobility of a wireless client in the LAN. This arrangement is called an **extended service set (ESS)**. In the example of an ESS in Figure 4-3, the mobile computer establishes an authorized connection with the access point that has the strongest signal level (for example, AP-1). As the user moves, the strength of the signal from AP-1 decreases. At some point, the signal strength from AP-2 exceeds that from AP-1, and the wireless bridge establishes a new connection with AP-2. This is called a **hand-off**. The hand-off is an automatic process for the wireless client adapter in 802.11, and the term used to describe this is **roaming**.

Network access in 802.11 uses a technique called carrier sense multiple access with collision avoidance (CSMA/CA). In **CSMA/CA**, the client station listens for other users of the wireless network. If the channel is quiet (that is, no data transmission is occurring), the client station can transmit. If the channel is busy, the station(s) must wait until transmission stops. Each client station uses a unique random back-off time. This technique prevents client stations from trying to gain access to the wireless channel as soon as it becomes quiet. Currently four physical layer technologies are being used in 802.11 wireless networking: direct-sequence spread spectrum (DSSS), frequency-hopping spread spectrum (FHSS), infrared, and orthogonal frequency-division multiplexing (OFDM). DSSS is used in 802.11b/g/n wireless networks, and OFDM is used in 802.11a, 802.11g, 802.11n, 802.11ac, and 802.11ax.

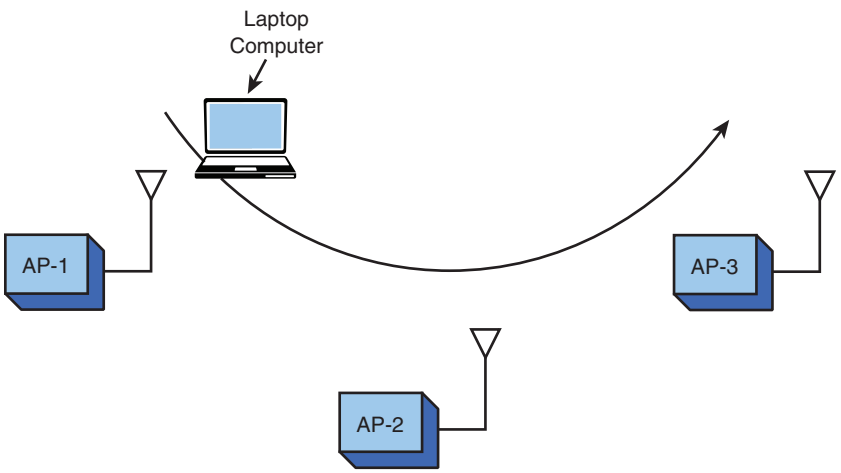


FIGURE 4-3 An example of an extended service set used for increased user mobility.

802.11 **DSSS** implements 14 channels (each consuming 22MHz) over approximately 90MHz of RF spectrum in the 2.4GHz **ISM** (industrial, scientific, and medical) **band**. DSSS is a technique used to spread the transmitted data over a wide bandwidth; in this case, it is a 22MHz bandwidth channel. A channel is a medium through which information is transmitted between transmitter and receiver. The bandwidth is a measure of the upper to lower frequencies of the channel required to transmit the information.

DSSS
Direct-sequence spread spectrum

ISM band
Industrial, scientific, and medical band

A related concept is *channel bonding*, in which two adjacent channels are combined to facilitate an increase in throughput between wireless devices. This is also called *Ethernet bonding* and is used in Wi-Fi applications.

Table 4-2 lists the frequency channels used in North America. Note that only 11 out of 14 channels are made available in North America due to regulatory requirements of the Federal Communication Commission (FCC). Figure 4-4 shows an example of the frequency spectrum for three-channel DSSS. Note that the three channels listed in Figure 4-4 (1, 6, and 11) do not overlap, while Table 4-2 shows that the other channels do have channel overlap. Remember that each channel is 22MHz in bandwidth. For example, channel 2 extends from 2.406GHz to 2.429GHz, with a center frequency of 2.417GHz, which clearly overlaps a portion of channel 1 and channel 3. Channels 1, 6, and 11 are the only channels that do not have overlap.

TABLE 4-2 **North American DSSS Channels**

Channel Number	Frequency (GHz)
1	2.412
2	2.417
3	2.422
4	2.427
5	2.432
6	2.437
7	2.442
8	2.447
9	2.452
10	2.457
11	2.462

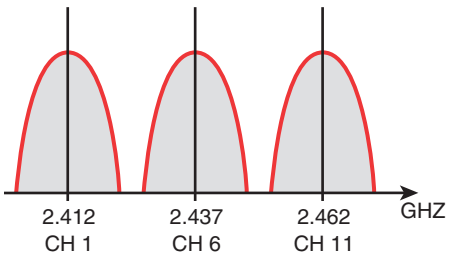


FIGURE 4-4 An example of the three channels in the DSSS spectrum.

FHSS
Frequency-hopping spread spectrum, a technique in which the transmit signal frequency changes based on a pseudorandom sequence

Pseudorandom
A number sequence that appears random but actually repeats

Hopping Sequence
The order of frequency changes

In frequency-hopping spread spectrum (**FHSS**), the transmit signal frequency changes based on a pseudorandom sequence. **Pseudorandom** means the sequence appears to be random but in fact does repeat, typically after some lengthy period of time. FHSS uses 79 channels (each 1MHz wide) in the ISM 2.4GHz band. FHSS requires that the transmitting and receiving units know the **hopping sequence** (the order of frequency changes) so that a communication link can be established and synchronized. FHSS data rates are typically 1Mbps and 2Mbps. FHSS is not commonly used anymore for wireless LANs. It's still part of the standard, but very few (if any) FHSS wireless LAN products are sold.

The maximum transmit power of 802.11b wireless devices is 1000 mW; however, the nominal transmit power level is 100 mW. The 2.4GHz frequency range used by 802.11b/g is shared by many technologies, including Bluetooth, cordless telephones, and microwave ovens.

LANs emit significant RF noise in the 2.4GHz range that can affect wireless data. A significant improvement in wireless performance is available with the IEEE 802.11a standards. The 802.11a equipment operates in the 5GHz range and provides significant improvement over 802.11b with respect to RF interference. An important concept related to noise is signal-to-noise ratio, which is a measure of the signal level relative to the noise level. The value is usually expressed in decibels (dB), and a high dB value is desirable.

OFDM
Orthogonal frequency-division multiplexing, a technique that involves dividing the signal bandwidth into smaller subchannels and transmitting the data over these subchannels in parallel

Another technique used in the 802.11 standard is **orthogonal frequency-division multiplexing (OFDM)**. The basic idea with this technique is to divide the signal bandwidth into smaller subchannels and to transmit the data over these subchannels in parallel. These subchannels can be overlapping, but they do not interfere with each other. The subchannels are mathematically orthogonal, and this setup yields uncorrelated or independent signals.

U-NII
Unlicensed National Information Infrastructure

The 802.11a standard transports data over 12 possible channels in the Unlicensed National Information Infrastructure (**U-NII**). The FCC set aside U-NII to support short-range, high-speed wireless data communications. The 802.11 channels and frequencies are governed by FCC regulations, which are periodically revised. A wireless manufacturer must keep its products up to date due to the regulatory impacts. Table 4-3 lists the operating frequencies for 802.11a, and Table 4-4 lists the transmit power levels for 802.11a.

TABLE 4-3 **IEEE 802.11a Channels and Operating Frequencies**

Channel	Center Frequency (GHz)	
36	5.180	
40	5.20	Lower band
44	5.22	
48	5.24	
52	5.26	
56	5.28	Middle band
60	5.30	
64	5.32	

Channel	Center Frequency (GHz)	
149	5.745	
153	5.765	Upper band
157	5.785	
161	5.805	

TABLE 4-4 **Maximum Transmit Power Levels for 802.11a with a 6 dBi Antenna Gain**

Band	Power Level
Lower	40 mW
Middle	200 mW
Upper	800 mW

IEEE 802.11a equipment is not compatible with 802.11b or 802.11g. The upside of this is that 802.11a equipment does not interfere with 802.11b or g; therefore, 802.11a and 802.11b/g links can run next to each other without causing interference. 802.11n can operate either in the 2.4GHz range or the 5GHz range. Cheaper 802.11n wireless cards tend to be manufactured with only 2.4GHz antennas, so users have to check the frequency specifications as not all 802.11n equipment has both 2.4GHz and 5GHz frequencies. Figure 4-5 shows an example of the two links operating together. Along the same lines, frequency mismatch is an issue if the two ends of the communications link are operating on different channels or if you are trying to make 802.11a communicate with 802.11b, as the frequencies are not compatible.

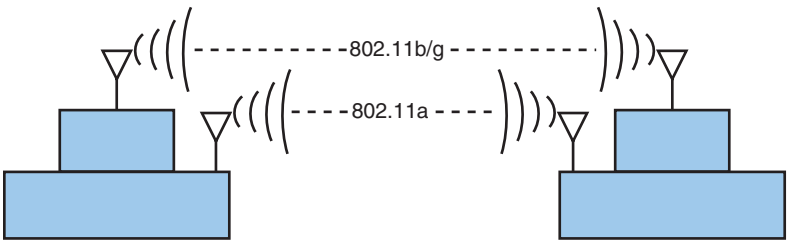


FIGURE 4-5 An example of an 802.11a installation and an 802.11b link running alongside each other.

The downsides of 802.11a are the increased cost of the equipment and increased power consumption because of the OFDM technology. This is of particular concern with mobile users because of the effect it can have on battery life. However, the maximum usable distance (RF range) for 802.11a is about the same as or even greater than that of 802.11b/g/n/ac/ax. It is important to note that any RF signal has distance limitations either due to limited output transmitted power, antenna pattern, or terrain issues.

Another IEEE 802.11 wireless standard is IEEE 802.11g. The 802.11g standard supports the higher data transmission rates of 54Mbps but operates in the same 2.4GHz range as 802.11b. The 802.11g equipment is also backward compatible with 802.11b equipment. This means that 802.11b wireless clients can communicate with the 802.11g access points, and the 802.11g wireless client equipment can communicate with the 802.11b access points. The obvious advantage of this is that a company with an existing 802.11b wireless network can migrate to the higher data rates provided by 802.11g without having to sacrifice network compatibility. In fact, new wireless equipment supports both the 2.4GHz and 5GHz standards, and it therefore has the flexibility of high speed, compatibility, and noninterference.

Another entry into wireless networks is 802.11n. This wireless technology operates in the same ISM frequency as 802.11b/g (2.4GHz) and can also operate in the 5GHz band. A significant improvement with 802.11n is multiple-input multiple-output (**MIMO**). MIMO uses a technique called space-division multiplexing, in which the data stream is split into multiple parts called spatial streams. The different spatial streams are transmitted using separate antennas. With MIMO, doubling the spatial streams doubles the effective data rate. The downside of this is the possibility of increased power consumption. The 802.11n specification includes a MIMO power-save mode. With this mode, 802.11n uses multiple data paths only when faster data transmission is required—thus saving power.

MIMO
Multiple-input multiple-output

The 802.11ac technology operates in the 5GHz band. It uses a newer version of MIMO technology with eight spatial streams and has channels up to 80MHz wide. It also introduces multiuser MIMO (**MU-MIMO**), which can send MIMO spatial streams to multiple clients at the same time. 802.11ac incorporates standardized **beamforming**, a technique that is used to direct transmission of the radio signal to a specific device. Beamforming increases data throughput and reduces power consumption. 802.11n used beamforming, but it was not standardized. The transmit range for 802.11ac is similar to or better than that of 802.11n.

MU-MIMO
Multiuser Multiple-input Multiple-output

Beamforming
A technique used to direct transmission of a radio signal to a specific device

The latest addition to the 802.11 family is 802.11ax, also known as Wi-Fi 6. Whereas 802.11ac operates in the 5GHz band only, 802.11ax operates in both 2.4GHz and 5GHz bands. 802.11ax uses OFDMA (orthogonal frequency-division multiple access) rather than OFDM. OFDMA allows multiple users or clients to share the same channel simultaneously. Wireless devices can optionally support WPA3 (Wi-Fi Protected Access 3), but 802.11ax increases security requirements by mandating the use of WPA3 as its encryption and authentication standard. WPA3 is discussed in more detail in Chapter 11, "Network Security."

Table 4-5 provides a comparison of 802.11n, 802.11ac, and 802.11ax in terms of their compatibility with other Wi-Fi technologies and the frequencies supported.

TABLE 4-5 **A Comparison of 802.11ac, 802.11n, and 802.11ax**

	802.11n	802.11ac	802.11ax
Backward-compatible with	802.11g, 802.11b, and 802.11a	802.11n	802.11a, 802.11b, 802.11g, 802.11n, and 802.11ac
Frequencies supported	2.4GHz and 5GHz	5GHz	2.4GHz and 5GHz

Wireless networks also go by the name **Wi-Fi**, which is not an acronym, but a term created and is a trademark of Wi-Fi Alliance to represent the standards for wireless communication. Wi-Fi is sometimes referred to as *wireless fidelity*. The Wi-Fi Alliance is an organization whose function is to test and certify wireless equipment for compliance with the 802.11*x* standards, the group of wireless standards developed under the IEEE 802.11 standard. The following list provides a summary of the most common wireless standards:

Wi-Fi
A term created and is a trademark of the Wi-Fi Alliance to represent the standards for wireless communication.

- **802.11b (Wi-Fi 1):** This standard can provide data transfer rates up to 11Mbps with ranges of 100–150 feet. It operates at 2.4GHz and uses DSSS.
- **802.11a (Wi-Fi 2):** This standard can provide data transfer rates up to 54Mbps and an operating range up to 75 feet. It operates at 5GHz and uses OFDM.
- **802.11g (Wi-Fi 3):** This standard can provide data transfer rates up to 54Mbps and an operating range up to 150 feet. It operates at 2.4GHz and uses DSSS or OFDM.
- **802.11n (Wi-Fi 4):** This high-speed wireless connectivity promises data transfer rates over 200Mbps. It operates at 2.4GHz and 5GHz and uses DSSS or OFDM.
- **802.11i:** This standard for WLANs provides improved data encryption for networks that use the 802.11a, 802.11b, and 802.11g standards.
- **802.11r:** This standard is designed to speed hand-offs between access points or cells in a WLAN. This standard is a critical addition to 802.11 WLANs if voice traffic is to become widely deployed.
- **802.11ac (Wi-Fi 5):** This is currently the most deployed wireless standard. It provides single-station data transfer rates of 500Mbps up to 1.3Gbps and operates in the 5GHz frequency band.
- **802.11ax (Wi-Fi 6):** This is the latest wireless standard, and manufacturers are starting to ship more equipment with this wireless technology. Theoretically, it could deliver close to 10Gbps data rates.

Another wireless technology is Z-Wave. This wireless communications protocol was developed for home automation. Typical applications include sensors for home lighting, security systems, and HVAC systems. The operating frequencies for Z-Wave in the United States are 908.4MHz and 916MHz.

Another entry into the ultra-low-power wireless protocol space is ANT+, which is used for wireless sensor networks (WSNs). This technology operates at 2.4GHz.

Section 4-2 Review

This section covers the following Network+ exam objectives.

1.2 Explain the characteristics of network topologies and network types.
This section introduces the new wireless technologies Z-Wave and ANT+.

1.6 Explain the use and purpose of network services.
This section provides an example of a network in which the wireless clients (stations) communicate directly with each other.

2.1 Compare and contrast various devices, their features, and their appropriate placement on the network.
An access point is a transmit/receive unit (transceiver) that interconnects data from the wireless LAN to the wired network. In addition, an access point provides 802.11 MAC layer functions and supports bridge protocols.

2.4 Given a scenario, install and configure the appropriate wireless standards and technologies.
This section introduces the terms basic service set, extended service set, and ad hoc set and the concept of roaming.

3.1 Given a scenario, use the appropriate statistics and sensors to ensure network availability.
This section examines the 802.11a/b/g/n/i/r/ac/ax standards as well as issues such as transmit distance, data speed, and frequencies. This section also introduces the concept of MIMO, which is used to increase the effective transmit data rate.

3.3 Explain high availability and disaster recovery concepts and summarize which is the best solution.
To provide reliable network services, an administrator must have a good understanding of WLAN configurations and technologies.

4.3 Given a scenario, apply network hardening techniques.
Table 4-3 lists the operating frequencies for 802.11a, and Table 4-4 lists the transmit power levels for 802.11a.

4.4 Compare and contrast remote access methods and security implications.
This section introduces wireless management protocols and indicates that the services are authentication, association, data delivery, and privacy.

5.2 Given a scenario, troubleshoot common cable connectivity issues and select the appropriate tools.
Technical issues related to throughput, speed, and distance are examined in this section.

Test Your Knowledge

1. True or false: 802.11ac networking equipment is compatible with 802.11b.

   True

2. True or false: 802.11g networking equipment is compatible with 802.11b.

   True

3. True or false: 802.11a and 802.11b wireless networks can run side-by-side.

   True

4. True or false: 802.11ac networking equipment is compatible with 802.11n.

   True

4-3 802.11 WIRELESS NETWORKING

This section introduces techniques for assembling a wireless network and helps students understand the purpose of the access point and the SSID (service set identifier). The techniques for implementing point-to-point and point-to-multipoint wireless networks are presented, and so is the very important concept of a site survey. Make sure students understand the importance of performing a good site survey to ensure user mobility and connectivity.

A wireless LAN can be configured in many ways to meet the needs of an organization. Figure 4-6 provides an example of a basic 802.11b/g/n/ac/ax WLAN configuration. In this configuration, each PC is outfitted with a wireless LAN adapter card. Today, most computer desktops and especially computer laptops are equipped with wireless adapters. For devices that lack these cards, an external USB wireless adapter can be used. A wireless adapter (or wireless LAN adapter) is a device that connects a client to the wireless medium, which is typically a radio wave channel in the 2.4GHz or 5GHz ISM band. The wireless medium can also be infrared, although that is not used very often. The following services are provided by a wireless LAN adapter:

- Delivery of the data
- Authentication
- Privacy

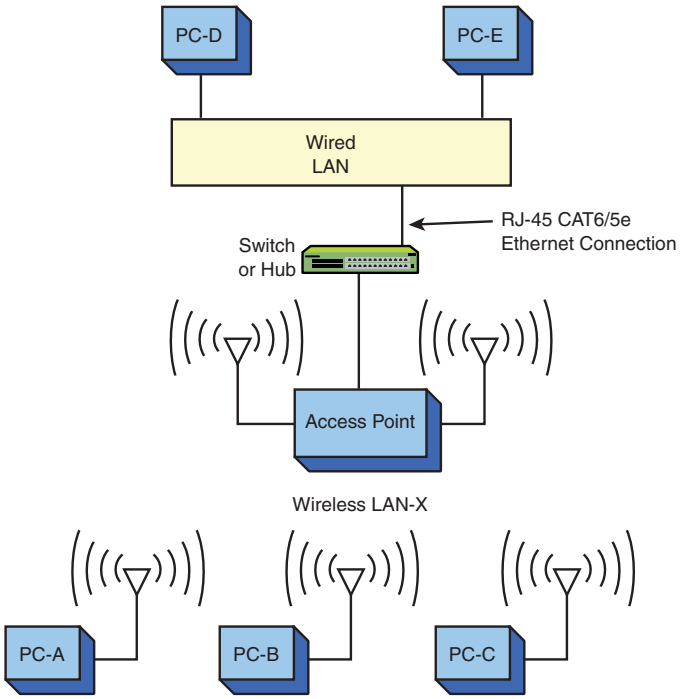


FIGURE 4-6 The setup for a basic WLAN.

One of the biggest misconceptions about wireless is that it does not require a wired connection. This is not quite correct. The connection to a wired LAN is provided by a wireless access point (WAP), which provides a bridge between the wireless LAN and the wired network. A physical cable connection (typically CAT6 or higher) ties the access point to the wired network's switch or hub (typically Ethernet).

For example, computer PC-A in Figure 4-6 sends a data packet to PC-D, a destination in the wired LAN. PC-A first sends a data packet over the wireless link. The access point recognizes the sender of the data packet as a host in wireless LAN-X and allows the wireless data to enter the access point. At this time, the data is sent out the physical Ethernet connection to the wired LAN. The data packet is then delivered to PC-D in the wired LAN.

SSID
Service set identifier, a password that enables the client to join the wireless network

How does the access point know that the wireless data packet is being sent from a client in the wireless LAN? The 802.11 wireless LAN devices use an **SSID** to identify what wireless data traffic is allowed to connect to the network. The SSID is the wireless *service set identifier*, which enables the client to join the wireless network.

The access point uses the SSID to determine whether the client is to become a member of the wireless network. The term *association* is used to describe a wireless connection that is made. The wrong SSID prevents an association, keeping the client from being able to become a member of the wireless network.

People are commonly surprised by the fact that an access point has two antennas. The two antennas implement *spatial diversity*, improving received signal gain and performance.

Figure 4-7 provides an example of the information displayed on the wireless adapter's console port when an association is made. The text indicates that a connection has been made to a parent (access point) whose MAC address is 00-40-96-25-9d-14. The text indicates that this MAC address has been added to the list of associations. This type of information is typically available via the wireless management software that comes with the wireless PC or PCMCIA adapter.

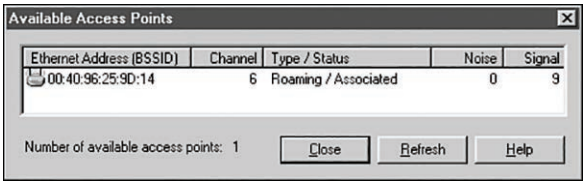


FIGURE 4-7 An example of the information displayed when an association is formed between a client and an access point.

An access point uses an association to build a table of users (clients) on the wireless network; this association table lists the MAC addresses for each networking device connected to the wireless network. Figure 4-8 provides an example of an association table. The access point uses the association table to forward data packets between the access point and the wireless network. As shown in Figure 4-8, the wireless client adapter also notifies the user if the client has lost an association with the access point.

A wireless bridge is a popular choice for connecting LANs that are running similar network protocols, even if the LANs are miles apart. Figure 4-9 provides examples. Figure 4-9(a) shows a point-to-point wireless bridge. Each building shown in Figure 4-9(a) has a connection from the wireless bridge to the building's LAN, as shown in Figure 4-10. The wireless bridge then connects to an antenna placed on the roof. A clear (line-of-sight) transmission path must exist between the two buildings; otherwise, signal *attenuation* (loss) or signal disruption can result. Antenna selection is also critical when configuring the connection. (This issue is addressed in Section 4-5.) The antenna must be selected so that the signal strength at the receiving site is sufficient to meet the required received signal level.

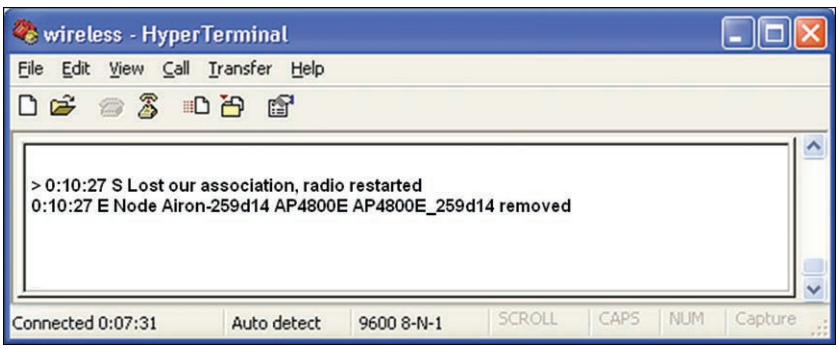


FIGURE 4-8 An example of a lost association.

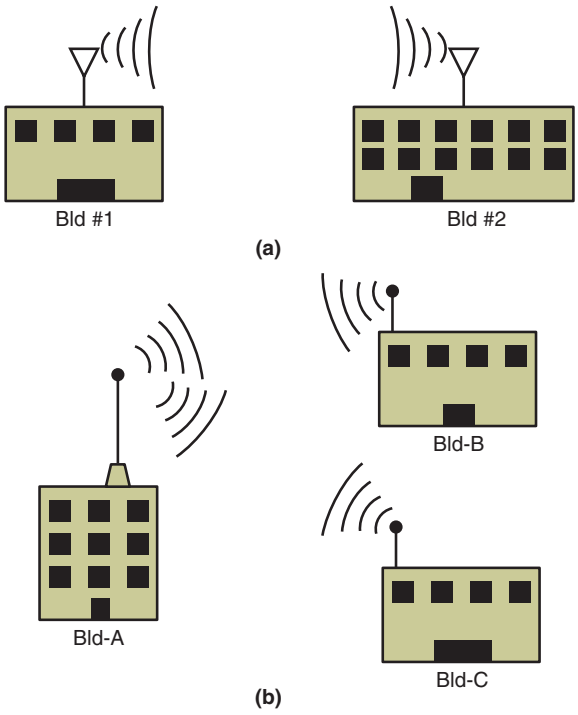


FIGURE 4-9 Examples of (a) point-to-point and (b) point-to-multipoint wireless bridge configurations.

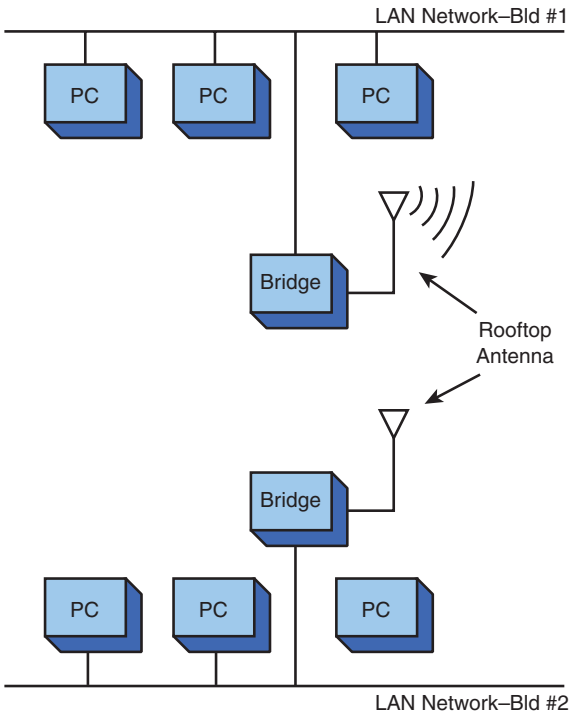


FIGURE 4-10 The wireless bridge connection to the wired network inside the building.

Figure 4-9(b) shows how a wireless bridge can be used to connect multiple remote sites to the main transmitting facility. Each building uses a bridge setup similar to that shown in Figure 4-10. The bridge connects to its respective LAN. In this case, Bld-A uses an antenna that has a wide coverage area (radiation pattern). The key objective with antenna selection is that the antenna must provide coverage for all receiving sites (in this case, Bld-B and Bld-C).

Wireless controllers are commonly used in enterprise wireless environments when managing hundreds of APs or more. In a traditional stand-alone wireless environment, each AP is managed individually. In an enterprise wireless controller environment, an AP communicates with its controller when booting up to download its necessary firmware and software, to register and authenticate itself, to receive its network information settings, and to receive its wireless LAN (WLAN) configuration. The wireless controller becomes the brain and manager of the whole operation. When wireless changes need to be made, they can be made at the controller, which pushes the changes out to all of the APs. CAPWAP (Configuration and Provisioning of Wireless Access Points) is the underlying wireless control protocol that APs use to communicate with wireless controllers. It supersedes LWAPP (Lightweight Access Point Protocol), which is a Cisco-proprietary protocol.

Wireless capacity is an issue today with the ever-increasing number of wireless users. Device density is the number of connecting wireless clients, and it has to be considered. Every wireless access point has a maximum device density that it can handle at one time. From a system design perspective, you have to plan for potential overcapacity with high-density Wi-Fi hotspots that can accommodate video streaming, image downloads, and multiple clients. Make sure you select access points than can handle the bandwidth demand; you don't want your clients to have to sacrifice bandwidth, especially when a cell phone can be set up as a hotspot that a wireless device can use to connect to the Internet via the data plan.

With wireless LANs, there is a maximum distance the signal can be transmitted. The distance limitation is a critical issue inside buildings when user mobility is required. Many obstacles can reflect and attenuate signals, causing reception to suffer. Also, the signal level for mobile users is hampered by increased distance from the access point. Distance is also a critical issue in outdoor point-to-multipoint wireless networks.

A solution is to place multiple wireless access points within the facility, as shown in Figure 4-11. Mobile clients can maintain a connection as they travel through the workplace because the wireless client automatically selects the access point that provides the strongest signal level. The access points can be arranged so that overlapping coverage of the workplace is provided, thus enabling seamless roaming for the client. The signal coverage is shown as circles in Figure 4-11. In actual practice, the radiation patterns are highly irregular due to reflections of the transmitted signal.

To have good wireless coverage in a large environment, it is not unusual to see the number of wireless access points in the range of hundreds or thousands. When dealing with so many wireless access points, it is very difficult and inefficient to program and manage each WAP individually and manually. Typically, a wireless LAN controller (WLC) is used as a central point or controller to deploy and manage all WAPs on a wireless network. When connecting to the network, each WAP connects to its WLC to get its configuration, radio channel, transmission power, and other settings. The WAPs communicate with the WLC and send their operational

wireless information to the WLC. The WLC can then use the collective information from all its WAPs to automatically adjust settings such as user load, radio channels, and radio power to improve the performance of the wireless network.

Site Survey
A process used to determine the best location(s) for placing the access point(s) to provide maximum RF coverage for wireless clients

It is important to verify that sufficient RF signal level is available for the users in a WLAN. This is best accomplished by performing a **site survey**. Inside a building, a site survey is performed to determine the best location(s) for placing the access point(s) for providing maximum RF coverage for wireless clients. Site surveys are also conducted for outside installations to determine the coverage area.

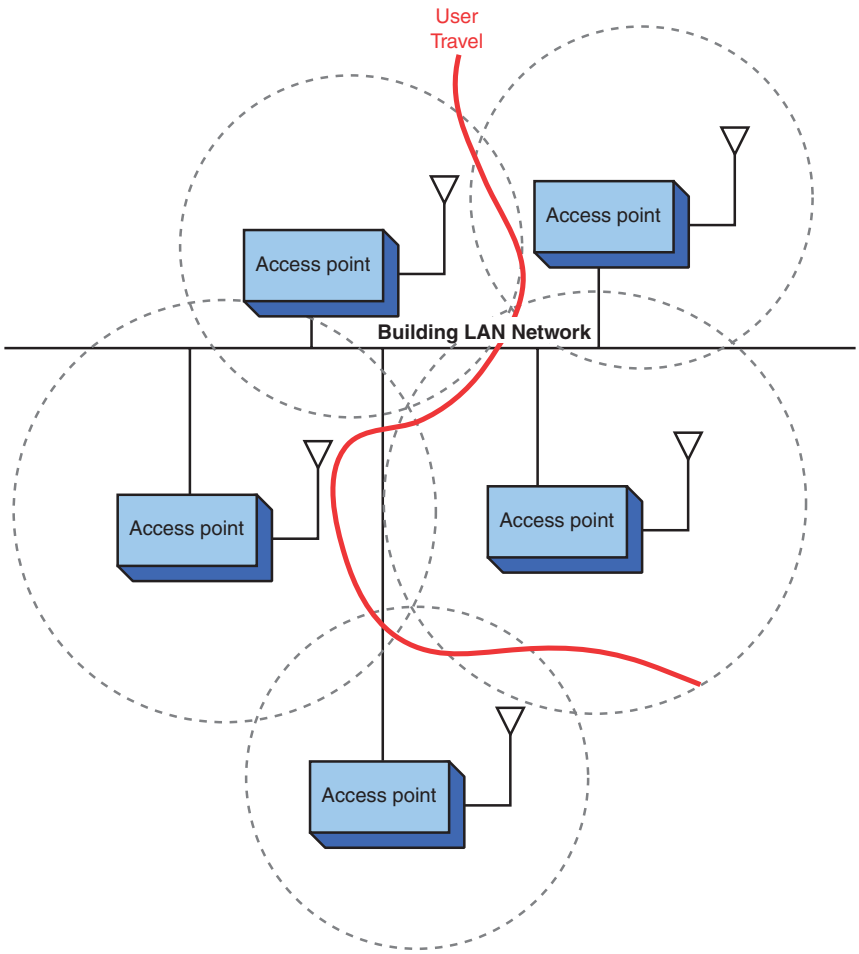


FIGURE 4-11 An example of configuring multiple access points to extend the range for wireless connectivity.

A site survey for indoor and outdoor installations should obtain the following key information:

- Indoor:
  - Electrical power
  - Wired network connection point(s)

- Access point placement
- RF coverage—user mobility
- Bandwidth supported
- Identify any significant RF interference

- Outdoor:
  - Electrical power (base access point)
  - Connection back to the home network
  - Antenna selection
  - Bandwidth supported
  - RF coverage
  - Any significant RF interference

Say that a site survey is conducted to determine access point placement to provide wireless network connectivity for the building whose floor plan is shown in Figure 4-12. The objective is to provide mobile client access throughout the building. The building already has two wired connections available for placing an access point.

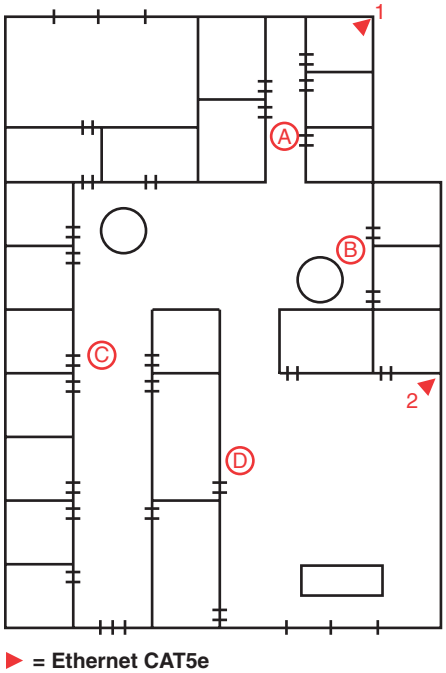


FIGURE 4-12 The floor plan for a building being surveyed for a wireless LAN.

The available wired network connections are indicated in the drawing in Figure 4-12. The site survey begins with placing an access point at position 1. A wireless mobile client is used to check the signal throughout the building. This checking used to be performed by a laptop with a purpose-built WLAN adapter as a Wi-Fi analyzer, but today, many more options are available. Handheld devices, such as tablets and smartphones, can be conveniently used for wireless site surveys. Their form factor and mobility are perfect for this purpose. Most of these devices are already equipped with built-in wireless chips. All they need is one of the many available wireless apps. This example shows test results gathered from an Android tablet with a free Wi-Fi analyzer app installed.

Figure 4-13 shows a snapshot of the wireless environment in the area. The graph shows the signal strength for each wireless SSID found. The signal strength is the wireless signal power level, and it is represented in –dBm format, from 0 to –100. This is the power ratio, in dB, of the measured power referenced to 1 mW. The closer the value is to 0, the stronger the signal, and the stronger the signal, the more reliable the wireless connection. Wireless is everywhere today, so when you conduct a site survey, you should not be too surprised to see more SSIDs than just yours. For this example, the site survey is intended for the wireless SSID ET377. As the graph shows, ET377 has the strongest signal of all the SSIDs. However, the signal strength may not represent the goodput. *Goodput* refers to the actual wireless data throughput, as measured by an application on the end device. It represents the actual transmission rate of a wireless connection, which is not the maximum theoretical transmission rate.

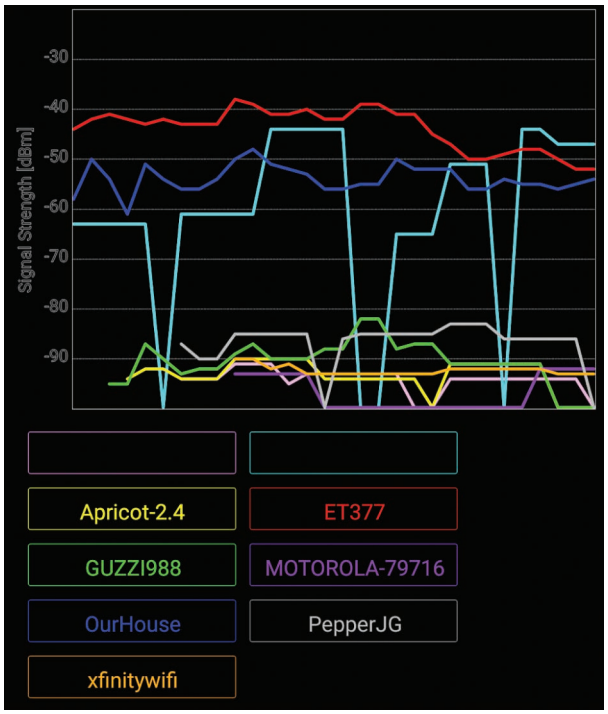


FIGURE 4-13 A snapshot of the RF signal environment.

The first measurement, shown in Figure 4-14, is taken at point A. Notice that the signal strength is at –43 dBm, which is an excellent connection. This will change if the signal level decreases significantly.

The next observation is made at point B, and the signal strength is measured at –52 dBm (see Figure 4-15). The signal has decreased somewhat, but it is still acceptable, which indicates that a connection is still good. The signal level drops to –67 dBm at point C, as shown in Figure 4-16. This connection is fair.

A floor plan showing the locations of wireless access points and wireless signal strength and coverage is a wireless or Wi-Fi heat map. Typically, a wireless/Wi-Fi heat map shows a real map of a room, floor, or even a city overlaid by a graphical representation of a wireless signal.

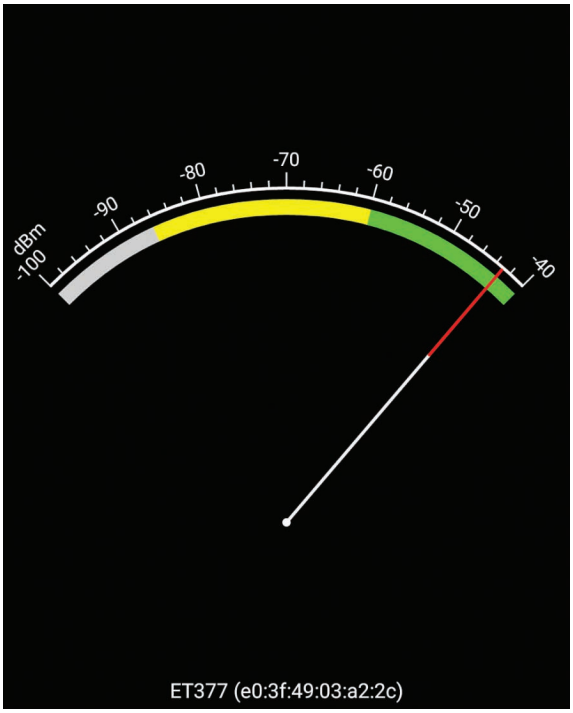


FIGURE 4-14 The RF signal strength observed at point A.

The mobile client is moved to point D in the building, and signal quality "Out of range" is observed (see Figure 4-17). This is also called a *loss of association* with the access point.

The site survey indicates that one access point placed at point 1 in the building is not sufficient to cover the building's floor plan. The survey shows that the additional cost of another access point is easily justified for providing full building wireless LAN coverage. The building has two wired network connections available for placing an access point (points 1 and 2). It is decided to place another access point at point 2. The site survey is repeated, and it shows excellent signal strength obtained throughout the building.

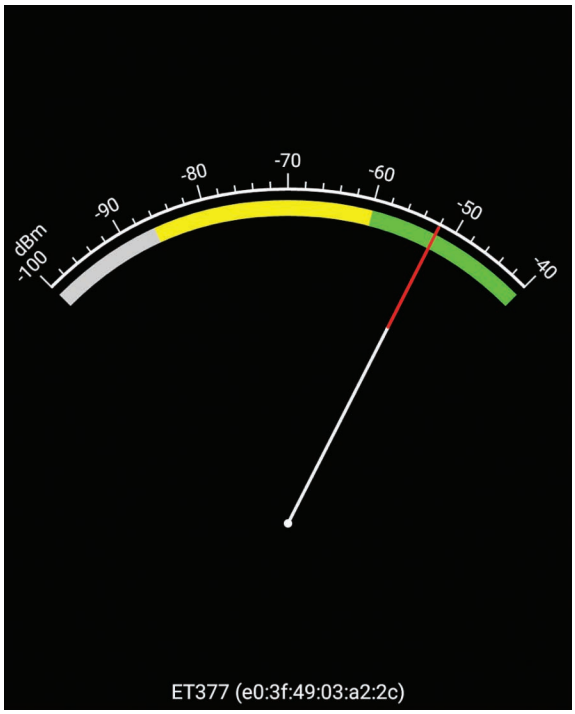


FIGURE 4-15 The RF signal strength at point B.

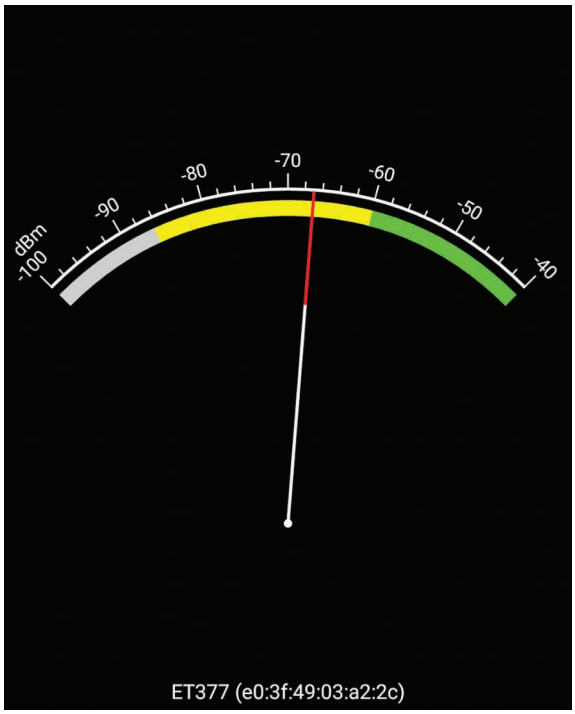


FIGURE 4-16 The drop in the signal quality to fair at point C.

In some cases, a *range extender* can be used to provide additional wireless coverage. This device basically extends the reach of the wireless network.

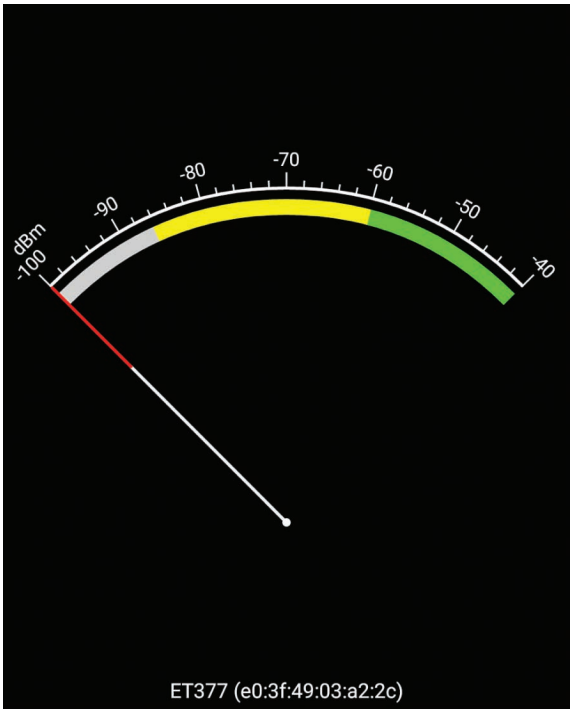


FIGURE 4-17 The "Out of range" measurement for point D.

Section 4-3 Review

This section covers the following Network+ exam objectives.

1.6 Explain the use and purpose of network services.

This section introduces the services provided by a wireless LAN adapter: delivery of the data, authentication, and privacy.

2.1 Compare and contrast various devices, their features, and their appropriate placement on the network.

A physical cable connection (typically CAT6 or greater) ties an access point to a wired network's switch or hub (typically Ethernet).

2.4 Given a scenario, install and configure the appropriate wireless standards and technologies.

This section introduces the SSID. An 802.11 wireless LAN device uses an SSID to identify what wireless data traffic is allowed to connect to the network. The SSID is the wireless service set identifier, basically a password that enables the client to join the wireless network.

3.1 Given a scenario, use the appropriate statistics and sensors to ensure network availability.

This section talks about preparing a site to support access point placement and the changes in signal strength that result from environmental factors.

3.2 Explain the purpose of organizational documents and policies.

The available wired network connections are indicated in a floor plan for a building being surveyed for a wireless LAN.

5.2 Given a scenario, troubleshoot common cable connectivity issues and select the appropriate tools.

A site survey for indoor and outdoor installations should obtain the following key information:

- Electrical power
- Wired network connection point(s)
- Access point placement
- RF coverage—user mobility
- Bandwidth supported
- Identify any significant RF interference

5.4 Given a scenario, troubleshoot common wireless connectivity issues.

The wrong SSID prevents an association, keeping a client from being able to become a member of the wireless network.

Test Your Knowledge

1. What happens when an *association* is made?

   a. A wireless connection is obtained.
   b. The MAC address of the client is obtained.
   c. Unauthorized network access is prevented.
   d. Excessive routing is prevented.

2. True or false: Site surveys help determine the following:

   - The best location for placing access points
   - Power connection
   - RF coverage
   - Antenna selection
   - IP address selection

   True

4-4 BLUETOOTH, WIMAX, RFID, AND MOBILE COMMUNICATIONS

This section looks at four wireless technologies: Bluetooth, WiMAX, RFID, and mobile communications. These technologies all play important roles in wireless networks, and this section looks at each of them. This section also looks at configurations and examples of the hardware being used. A fun exercise is to have students connect their laptops to each other using Bluetooth, as described in the example presented in this section.

This section looks at four wireless technologies: Bluetooth, WiMAX, RFID, and mobile communications. Each of these technologies plays an important role in wireless networks. The sections that follow examine each of these wireless technologies, including a look at configuration and examples of the hardware being used.

Bluetooth

The wireless technology Bluetooth is based on the 802.15 standard. Bluetooth was developed to replace the cable connecting computers, mobile phones, handheld devices, portable computers, and fixed electronic devices. The information normally carried by a cable is transmitted over the 2.4GHz ISM frequency band, which is the same frequency band used by 802.11b/g/n/ax. There are four output power classes for Bluetooth. Table 4-6 lists the maximum output power and the operating distance for each class.

Bluetooth Low Energy (BLE) technology has been developed to provide operation on a small battery for up to five years. This technology is ideal for applications that require the exchange of small amounts of data periodically. BLE operates in the 2.4GHz ISM band and remains in sleep mode except when a connection is initiated. BLE devices have significantly lower power requirements than do traditional Wi-Fi devices. For example, whereas a Wi-Fi device consumes about 500 µW for 10 messages, a BLE device consumes only 50 µW.

TABLE 4-6 **Bluetooth Output Power Classes**

Power Class	Average Output Power	Operating Distance
1	100 mW	~100 meters
2	2.5 mW	~10 meters
3	1 mW	~1 meter
4	0.5 mW	~0.5 meter

When a Bluetooth device is enabled, it uses an **inquiry procedure** to determine whether any other Bluetooth devices are available. The device also uses this procedure to allow itself to be discovered.

If a Bluetooth device is discovered, it sends an inquiry reply back to the Bluetooth device initiating the inquiry. Next, the Bluetooth devices enter the **paging procedure**, which is used to establish and synchronize a connection between

Inquiry Procedure
A process used to determine whether other Bluetooth devices are available

Paging Procedure
A process used to establish and synchronize a connection between two Bluetooth devices

Piconet
An ad hoc network of up to eight Bluetooth devices

two Bluetooth devices. When the procedure for establishing the connection has been completed, the Bluetooth devices will have established a **piconet**, an ad hoc network of up to eight Bluetooth devices, such as a computer, mouse, headset, earpiece, and so on. In a piconet, one Bluetooth device (the primary) is responsible for providing the synchronization clock reference. All other Bluetooth devices are called *secondaries*.

Let's look at an example of setting up a Bluetooth network linking a macOS computer to another Bluetooth-enabled device. To enable Bluetooth on macOS, click **Apple icon > System Preferences > Bluetooth** and then click **Turn Bluetooth On** (see Figure 4-18). The Mac automatically discovers other Bluetooth devices nearby.

Pairing
Setting up a Bluetooth device to connect to another Bluetooth device

Passkey
A passphrase used in Bluetooth security to limit outsider access to pairing

Next, you need to select the device with which you will be establishing a Bluetooth connection. When Bluetooth is turned on, the Mac searches for another Bluetooth device. When a Bluetooth device is found, it appears in the Devices window. To connect the desired Bluetooth device, select the **Pair** button next to the device. (The process of setting up a Bluetooth device to connect to another Bluetooth device is called **pairing**.) You are asked for a passkey or passphrase. The **passkey** is used in Bluetooth security to limit outsider access to the pairing. Only people with the passkey can pair with the Bluetooth device. Anyone who tries to pair units with the wrong passphrase will not be able to pair.

At this point, you can transfer files between the paired devices if the Bluetooth Sharing settings for the device have been set to allow files to come in. Find these settings by clicking **Apple icon > System Preferences > Sharing** and selecting **Bluetooth Sharing**. Figure 4-19 shows an example of the setup for the file transfer.

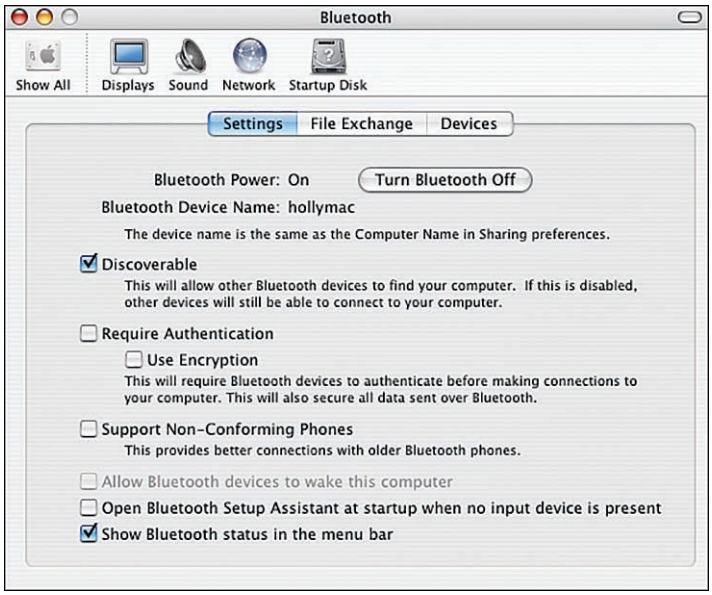


FIGURE 4-18 The window for configuring Bluetooth settings on a Mac.

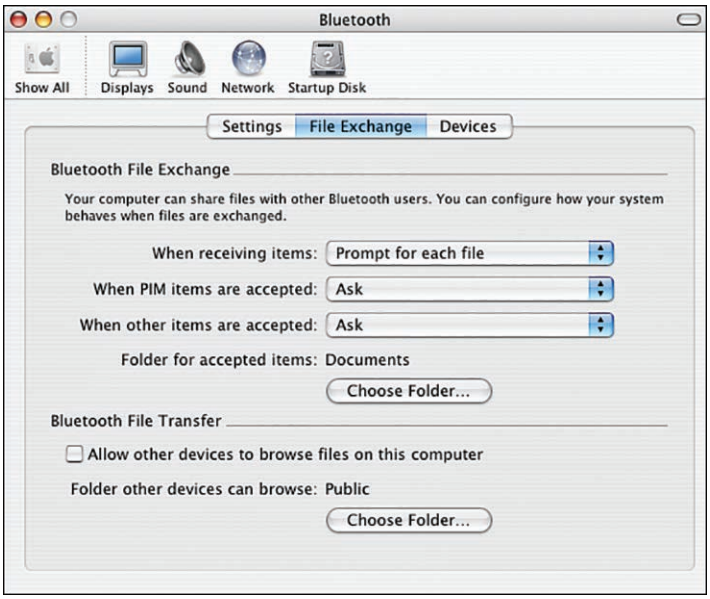


FIGURE 4-19 The Mac window showing the settings for a file transfer.

Figure 4-20 shows an incoming text file. The File Transfer menu enables you to select where received files are saved. In this case, the incoming files are being saved to the desktop.

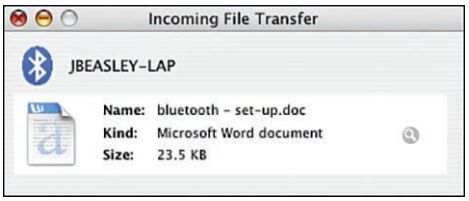


FIGURE 4-20 The Mac window showing that a text file is coming in from another Bluetooth device.

The details for setting up Bluetooth on Windows 10 differ slightly from those for macOS, but the basic steps are the same:

1. Enable the Bluetooth radio.
2. Enable discoverability (to allow other Bluetooth devices to find the device).
3. Select the device for pairing.

WiMAX
Worldwide Interoperability for Microwave Access, a broadband wireless system based on the IEEE 802.16e standard

BWA
Broadband wireless access

WiMAX

WiMAX (Worldwide Interoperability for Microwave Access) is a broadband wireless system that has been developed for broadband wireless access (**BWA**) for fixed

and mobile stations and can provide a wireless alternative for last-mile broadband access in the 2GHz–66GHz frequency range. BWA access for fixed stations can be up to 30 miles, whereas mobile BWA access is 3–10 miles. Internationally, the WiMAX frequency standard is 3.5GHz, while the United States uses both the unlicensed 5.8GHz and the licensed 2.5GHz spectra. In addition, WiMAX has been investigationally adapted for use in the 700MHz frequency range. Information transmitted at this frequency is less susceptible to signal blockage due to trees. The disadvantage of the lower frequency range is the reduction in bandwidth.

NLOS
Non-line-of-sight

WiMAX uses OFDM as its signaling format. This signaling format was selected for the WiMAX IEEE 802.16a standard because of its improved **NLOS** (non-line-of-sight) characteristics in the 2GHz–11GHz frequency range. An OFDM system uses multiple frequencies for transporting the data, which helps minimize multipath interference problems. Some frequencies may experience interference problems, but the system can select the best frequencies for transporting the data.

WiMAX also provides flexible channel sizes (for example, 3.5MHz, 5MHz, and 10MHz), which provides adaptability to standards for WiMAX worldwide. This also helps ensure that the maximum data transfer rate is supported. For example, the allocated channel bandwidth could be 6MHz, and the adaptability of the WiMAX channel size enables it to adjust to use the entire allocated bandwidth.

In addition, the WiMAX (IEEE 802.16e) media access control (MAC) layer differs from the IEEE 802.11 Wi-Fi MAC layer in that the WiMAX system has to compete only once to gain entry into the network. When a WiMAX unit has gained access, the base station allocates a time slot to it, thereby providing the WiMAX system scheduled access to the network. The WiMAX system uses time-division multiplexing (TDM) data streams on the downlink and time-division multiple access (TDMA) on the uplink and centralized channel management to ensure that time-sensitive data is delivered on time. In addition, WiMAX operates in a collision-free environment, which improves channel throughput.

Last Mile
The last part of the connection from a telecommunications provider to a customer

WiMAX has a range of up to 30 miles, and it operates in both point-to-point and point-to-multipoint configurations. This can be useful in situations where DSL or cable network connectivity is not available. WiMAX is also useful for providing the last-mile connection. The **last mile** is basically the last part of the connection from a telecommunications provider to a customer. The cost of the last mile connection can be high, which makes a wireless alternative attractive to customers.

The 802.16e WiMAX standard holds a lot of promise for use as a mobile air interface.

Radio Frequency Identification (RFID)
A technique that uses radio waves to track and identify people, animals, objects, and shipments

Backscatter
The reflection of radio waves striking an RFID tag and reflecting back to the transmitter source

Radio Frequency Identification

Radio frequency identification (RFID) uses radio waves to track and identify people, animals, objects, and shipments. It is based on the principle of modulated **backscatter**—the reflection of the radio waves striking an RFID tag back to the transmitter source, with its stored unique identification information.

Figure 4-21 illustrates a basic RFID system, which consists of two elements:

- **RFID tag:** An RFID tag (also called an RF transponder) includes an integrated antenna and radio electronics.

- **Reader:** A reader (also called a transceiver) consists of a transceiver and an antenna. A transceiver is a combination of a transmitter and receiver.

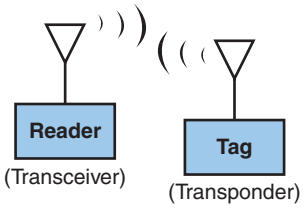


FIGURE 4-21 Basic block diagram of an RFID system.

The reader transmits radio waves, which activates (turns on) an RFID tag. The tag then transmits modulated data, containing its unique identification information stored in the tag, back to the reader. The reader then extracts the data stored on the RFID tag.

The RFID idea dates back to 1948, when the concept of using reflected power as a means of communication was first proposed. The 1970s saw further development in RFID technology—in particular, a UHF scheme that incorporates rectification of the RF signal for providing power to the tag. Development of RFID technology significantly increased in the 1990s. Applications included toll collection that allowed vehicles to pass through tollbooths at highway speeds while still being able to record data from the tag.

Today, RFID technology is being used to track inventory shipments for major commercial retailers, by the transportation industry, and by the Department of Defense. In addition, RFID applications are being used in Homeland Security for tracking container shipments at border crossings. In addition, RFID is being incorporated into WLAN computer networks to keep better track of inventory. RFID technology is being used as a wireless means of asset tracking and is therefore becoming more important in networks. The tracking technology is even being extended to tracking Wi-Fi devices within the WLAN infrastructure.

Three parameters define an RFID system:

- Means of powering the tag
- Frequency of operation
- Communications protocol (also called the air interface protocol)

Powering the Tag RFID tags are classified in three ways, based on how they obtain their operating power:

- **Passive:** Power is provided to a passive tag by rectifying the RF energy, transmitted from the reader, that strikes the RF tag antenna. The rectified power level is sufficient to power the ICs on the tags and also provides

sufficient power for the tag to transmit a signal back to the reader. Figure 4-22 shows an example of a passive RFID tag (also called an inlay). A tag inlay includes both an RFID chip and an antenna mounted on a substrate.

- **Semi-active:** With semi-active tags, a battery powers the electronics on a tag, but the tag uses backscatter to transmit information back to the reader.
- **Active:** With active tags, a battery powers the tag and transmits a signal back to the reader. Basically, this is a radio transmitter. New active RFID tags are incorporating wireless Ethernet (that is, 802.11 Wi-Fi connectivity). An example is the G2C501 active RFID tag from G2 Microsystems, shown in Figure 4-23. The power consumption of the G2C501 is 10 µA in sleep mode, and the device uses two AA batteries with an expected lifetime of five years. The G2C501 also works in the standard 915MHz range. In addition, the G2C501 has location capability. This is accomplished by making receive signal strength indicator (RSSI) measurements from three separate access points. The three measurements provide sufficient information to make a triangulation measurement for use in locating the object.

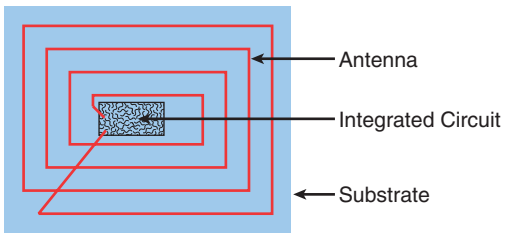


FIGURE 4-22 An example of an RFID inlay.

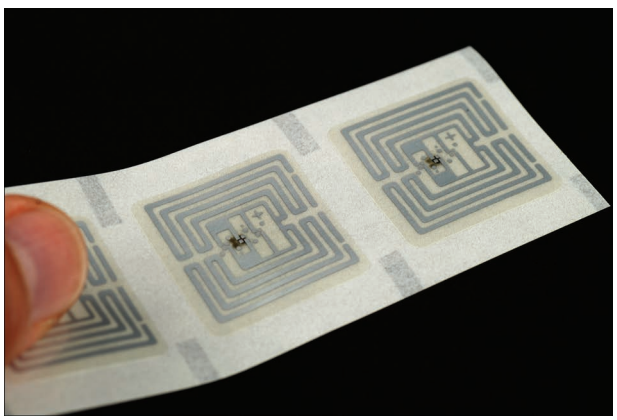


FIGURE 4-23 The G2C501 active RFID tag from G2 Microsystems (Albert Lozano/Shutterstock).

Frequency of Operation RFID tags must be tuned to the reader's transmit frequency in order to turn on. RFID systems typically use three frequency bands for operation (see Figure 4-24):

- **Low frequency (LF):** LF tags typically use frequency-shift keying (FSK) between the 125KHz and 134KHz frequencies. These tags can handle only low data rates (~12Kbps), and they are not appropriate for any applications requiring fast data transfers. However, LF tags are suitable for animal identification, such as with dairy cattle and other livestock. The RFID tag information is typically obtained when the livestock are being fed. The read range for low-frequency tags is approximately 0.33 meter.
- **High frequency (HF):** HF tags operate in the 13.56MHz industrial band. High-frequency tags have been available commercially since 1995. The longer wavelengths of the HF radio signal are less susceptible to absorption by water or other liquids. Therefore, these tags are suitable for tagging liquids. The read range for HF tags is approximately 1 meter. The short read range provides for better-defined read ranges. The applications for tags in this frequency range include access control, smart cards, and shelf inventory. The data rate for HF tags is 26Kbps.
- **Ultra-high frequency (UHF):** UHF tags work at 860–960MHz and at 2.4GHz. The data rates for these tags can be 50–150Kbps and greater. These tags are popular for tracking inventory. The read range for passive UHF tags is 3–6 meters, which makes them a good choice for reading pallet tags. However, if an active tag is used, a read range up to 100 meters is possible.

FIGURE 4-24 The frequency bands used by RFID tags.

Communications (Air Interface) Protocol The air interface protocol adopted for RFID tags is **Slotted Aloha**, a network communications protocol similar to the Ethernet protocol. With Slotted Aloha, the tags are only allowed to transmit at predetermined times after being energized. This technique reduces the likelihood of data collisions between RFID tag transmissions and allows for the reading of up to 1000 tags per second (for high-frequency tags). The operating range for RFID tags can be up to 30 meters. This means that multiple tags can be energized at the same time, and RF data collisions can possibly occur. If a collision occurs, the tag will transmit again after a random back-off time. The readers transmit continuously until there is no tag collision.

Slotted Aloha
A wireless network communications protocol similar to the Ethernet protocol

Mobile (Cellular) Communications

Today, many types of mobile devices, also called cellular devices, can be used to access computer networks. Examples include smartphones, laptops, tablets, and gaming devices. All of these devices are extremely powerful and use wireless technology to connect to the network. This chapter has provided an overview of many of the wireless technologies being used today, including the 802.11 family of Wi-Fi technologies, Bluetooth, WiMAX, and RFID. This section provides a brief summary of some of the other wireless technologies currently available.

CDMA CDMA (code-division multiple access) is a communications technology in which spread-spectrum techniques are used to multiplex more than one signal within a single channel. In this case, each device uses a different binary sequence to modulate the carrier, spreading the spectrum of the waveform (spread spectrum). The signals are separated at the receiver by a correlator that accepts only the signal from the selected binary sequence.

LTE/4G LTE (Long Term Evolution) is a 4G wireless communications standard. It is designed to provide speeds up to 10 times those of 3G networks.

HSPA+ HSPA+ (Evolved High-Speed Packet Access) provides network speeds comparable to those of LTE networks. Theoretical speeds are 168Mbps for download and 22Mbps uplink.

3G/4G/5G 3G (Third Generation) was developed to provide broadband network wireless services. The standard defining 3G wireless is International Mobile Communications, or IMT 2000. 4G (Fourth Generation), which is the successor to 3G technology, provides download speeds of 100Mbps. 5G (Fifth Generation) is the latest wireless network technology provided by the cellular network, with speeds ranging from 40Mbps to 1.5Gbps.

EDGE EDGE (Enhanced Data GSM Evolution) provides download speeds of 384Kbps.

NFC A concept related to mobile communications and smartphones is NFC, which stands for Near Field Communication. NFC is a set of communication protocols that are used to enable two electronic devices to communicate. A typical NFC device is a smartphone. By using NFC, smartphones can establish communication if they are within 4 cm of each other. Applications of NFC include reading electronic tags and making payments.

Geofencing With many type of wireless devices using different type of wireless technologies, it has become more and more difficult for network administrators to keep track of the devices entering and leaving the premises. *Geofencing* is used to create a virtual electronic boundary for mobile and wireless devices to detect their whereabouts as well as control certain functionalities, such as camera or microphone, of the devices through the use of mobile device management (MDM). For example, geofencing may be used in a highly classified area or a restricted area in a corporate building.

Section 4-4 Review

This section covers the following Network+ exam objectives.

1.3 Summarize the types of cables and connectors and explain which is the appropriate type for a solution.

This section introduces the RFID reader, which consists of a transceiver and an antenna. A transceiver is a combination of a transmitter and receiver.

1.7 Explain basic corporate and datacenter network architecture.

This section introduces Bluetooth, RFID, WiMAX, and mobile can support links up to 30 miles and is a possible alternative for providing last-mile connections.

2.1 Compare and contrast various devices, their features, and their appropriate placement on the network.

This section introduces geofencing, which is used to create a virtual electronic boundary for mobile and wireless devices to detect their whereabouts as well as control certain functionalities, such as camera or microphone, of the devices through the use of mobile device management (MDM).

2.3 Given a scenario, configure and deploy common Ethernet switching features.

This section introduces 5G (Fifth Generation), which is the latest wireless network technology provided by the cellular network, with speeds ranging from 40Mbps to 1.5Gbps.

2.4 Given a scenario, install and configure the appropriate wireless standards and technologies.

This section introduces Bluetooth, RFID, WiMAX, and mobile technologies.

3.1 Given a scenario, use the appropriate statistics and sensors to ensure network availability.

This section examines the download speeds for many different technologies.

4.3 Given a scenario, apply network hardening techniques.

This section introduces the concept of geofencing.

5.2 Given a scenario, troubleshoot common cable connectivity issues and select the appropriate tools.

This section mentions that WiMAX operates in a collision-free environment, which improves channel throughput.

5.5 Given a scenario, troubleshoot general networking issues.

The air interface protocol adopted for RFID tags is Slotted Aloha, a network communications protocol similar to the Ethernet protocol. With Slotted Aloha, tags are only allowed to transmit at predetermined times after being energized. This technique reduces the likelihood of data collisions between RFID tag transmissions and allows for the reading of up to 1000 tags per second (for high-frequency tags).

Test Your Knowledge

1. WiMAX operates at which frequencies in the United States?
    a. Both the unlicensed 5.2GHz and the licensed 2.4GHz spectra
    b. Both the unlicensed 5.3GHz and the licensed 2.6GHz spectra
    c. Both the unlicensed 13.2GHz and the licensed 5.6GHz spectra
    d. Both the unlicensed 5.8GHz and the licensed 2.5GHz spectra
2. What is the maximum range of WiMAX?
    a. 30 kilometers
    b. 30 miles
    c. 30 meters
    d. None of these answers are correct.
3. At what frequency does Bluetooth operate?
    a. 5GHz
    b. 100MHz
    c. 2.4GHz
    d. None of these answers are correct.

4-5 CONFIGURING A POINT-TO-MULTIPOINT WIRELESS LAN: A CASE STUDY

This section presents an example of preparing a proposal for providing a point-to-multipoint wireless network for a company. It walks through the multiple steps involved in implementing a point-to-multipoint wireless network, including performing an antenna site survey, establishing a link to the home network, configuring the multipoint distribution, and configuring the remote site.

This section presents an example of preparing a proposal for providing a point-to-multipoint wireless network for a company. The administrators for the company have decided that it would be beneficial to provide a wireless network connection for their employees back to the company's network (the home network). This example walks through the following steps:

1. Conducting an initial antenna site survey
2. Establishing a link from the home network to the distribution point
3. Configuring the multipoint distribution
4. Conducting an RF site survey for establishing a baseline signal level for the remote wireless user
5. Configuring the remote user's installation

The objective of this example is to establish a point-to-multipoint wireless network that provides remote users with a wireless network connection. The remote users are to be at fixed locations within the proposed coverage area. Figure 4-25 shows a simple terrain profile of the proposed area. The data rate for the wireless connection to remote users needs to be at least 2Mbps.

Note

Antenna placement is critical when setting up a point-to-multipoint wireless LAN. Incorrect antenna placement can severely affect reception quality.

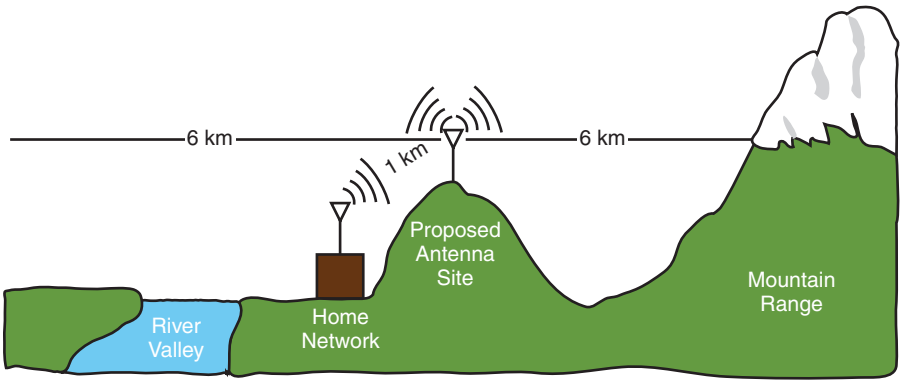


FIGURE 4-25 The terrain profile of the area to be supported by the proposed point-to-multipoint wireless network.

Step 1: Conducting an Antenna Site Survey

The proposed antenna site (refer to Figure 4-25) is on top of a hill approximately 1 kilometer from the home network. A site survey provides the following information:

- The site has a tower that can be used to mount the wireless antenna.
- The site has a small building and available rack space for setting up the wireless networking equipment.
- There is a clear view of the surrounding area for 6 kilometers in every direction.
- There is not an available wired network connection back to the home network. The decision is made to use the proposed antenna site and set up an 11Mbps wireless link back to the home network.

Step 2: Establishing a Point-to-Point Wireless Link to the Home Network

The cost of installing a wired connection back to the home network would be too high, so it is decided to use a point-to-point 802.11 wireless link for the interconnection. This requires that antennas be placed at both the home network and the antenna site. A wireless bridge is used at each end of the point-to-point wireless link to interconnect the networks. The bridge will connect to the wired home network and to the multipoint distribution on the antenna site. Also, each antenna will be outfitted with lightning arrestors to protect the electronics from any possible lightning strikes. Figure 4-26 shows the proposed wireless connection.

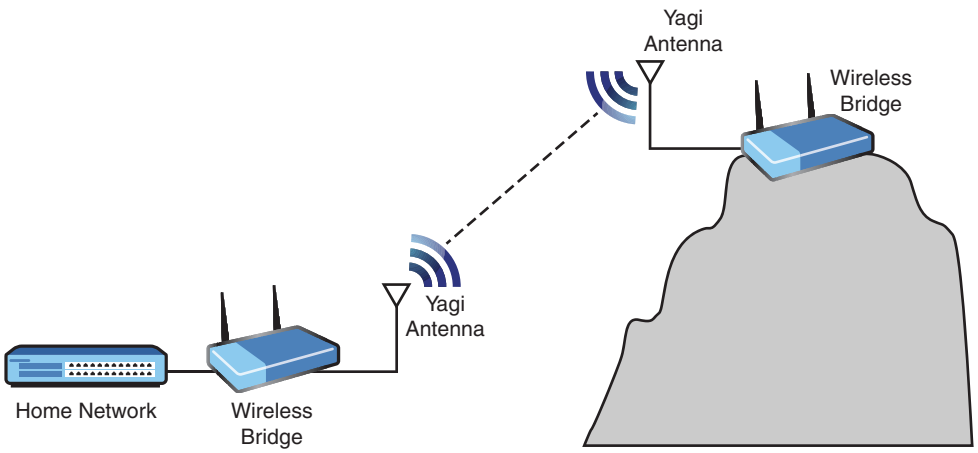


FIGURE 4-26 The proposed point-to-point wireless link between the home network and the antenna site.

Many manufacturers of antennas support wireless networking, and many types of antenna can be used. Antenna types from many manufacturers were investigated for possible use in the interconnection. Three possible antennas were selected for the wireless network, as outlined in Table 4-7.

Note

The selection of the incorrect antenna type can lead to a poorly designed radio link and poor reliability.

TABLE 4-7 **Sample of 802.11 Wireless Antennas**

Antenna	Type	Radiation Pattern	Costs
A	Omni	Omnidirectional	Moderate
B	Yagi	Directional	Moderate
C	Dish	Highly directional	High

Antenna A has an omnidirectional radiation pattern. This means the antenna can receive and transmit signals in a 360-degree pattern. Figure 4-27(a) shows the radiation pattern for an omnidirectional antenna. Antenna A supports all 802.11 types. Table 4-7 also indicates that this antenna has a moderate cost.

Antenna B is a Yagi antenna with a directional or unidirectional radiation pattern, as shown in Figure 4-27(b). The Yagi antenna supports all 802.11 antenna types.

Antenna C is a dish antenna, or parabolic reflector. These antennas provide extremely high directional gain, as illustrated in Figure 4-27(c). The dish antenna supports 802.11 systems. The cost of a dish antenna can be quite high relative to the cost of a Yagi or an omnidirectional antenna.

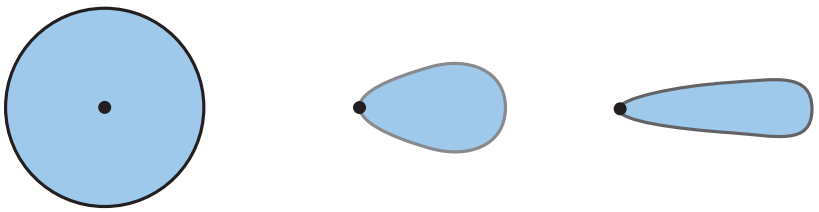


FIGURE 4-27 Antenna radiation patterns for (a) omnidirectional, (b) Yagi, and (c) dish [parabolic reflector] antennas. The cost of the Yagi antenna is comparable to that of the omnidirectional antenna.

Antenna B, the directional Yagi, is selected for the point-to-point link. The antenna meets the distance requirement and also meets the 11Mbps data rate requirement. Antennas A and C were not selected for the following reasons:

- **Antenna A:** The omnidirectional radiation pattern is not appropriate.
- **Antenna C:** The cost of a high-gain dish antenna is not justified for the short distance.

Steps 3 and 4: Configuring the Multipoint Distribution and Conducting an RF Site Survey

At this point, a wireless data link has been established with the home network. The next task is to configure the antenna site for multipoint distribution. It was previously decided that a 300Mbps link would be adequate for the remote users, based on the data rate to be supported for the planned coverage area.

The site survey in step 1 showed that there is a clear view of the surrounding area for 6 kilometers in each direction. Antenna A (see Table 4-7) provides an omnidirectional radiation pattern for 7 kilometers. This satisfies the coverage area. Antenna A is mounted on the antenna site tower, connected to a lightning arrestor,

and then connected to the output of a wireless bridge. Next, an RF site survey of the planned coverage area is conducted to verify the signal quality provided by the antenna selected. Measurements are made from multiple locations in the planned coverage area. All remote sites within 4 kilometers of the distribution show excellent signal strength (see Figure 4-28).

The signal quality drops to good at 6 kilometers at all surveyed remote locations except for one area, which shows a poor quality (see Figure 4-29). The signal is apparently being affected by multipath distortion from a small lake area. A fix to this might be to move the antenna to a different height to minimize reflection problems. An antenna at a different height will receive different reflections and possibly less interference. In some cases, antenna alignment can be changed to decrease the interference. A more costly solution would be to add antenna diversity, which basically means placing multiple antennas on the receiving tower and using the best signal for the connection.

Note

When dealing with antennas, it is important to consider effective isotropic radiated power (EIRP), which is the power that comes off an antenna and is the value the FCC uses to determine and measure power limits in wireless equipment.

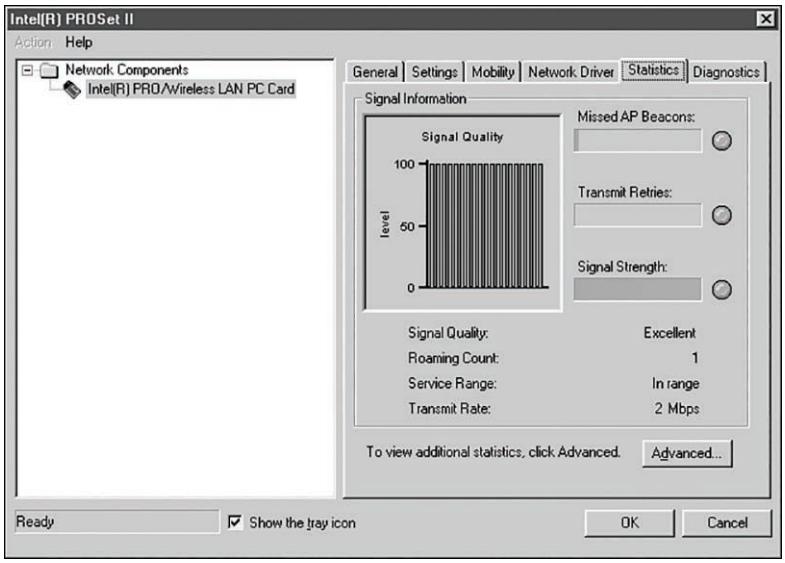


FIGURE 4-28 The excellent signal quality measured for the multipoint distribution.

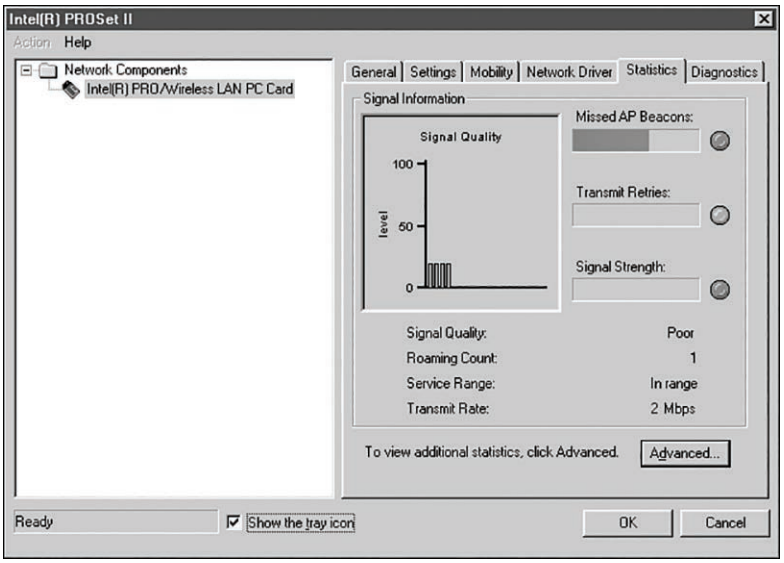


FIGURE 4-29 The poor signal quality measured at the remote site near the lake.

Step 5: Configuring the Remote Installations

The last task is to develop a configuration for the remote users. The antenna for each remote user needs to be able to see only the multipoint distribution antenna site. The requirements for the remote client are as follows:

- 300Mbps data rate connection
- Directional antenna (Yagi) plus mount, lightning arrestor, and wireless bridge

Antenna B (refer to Table 4-7) is selected for the directional antenna. This antenna will provide a sufficient RF signal level for the remote users. Each remote user will need a wireless bridge and a switch to connect multiple users. (Note that the bridge is set for a 2.4Mbps data rate.) Figure 4-30 shows the setup for the remote users.

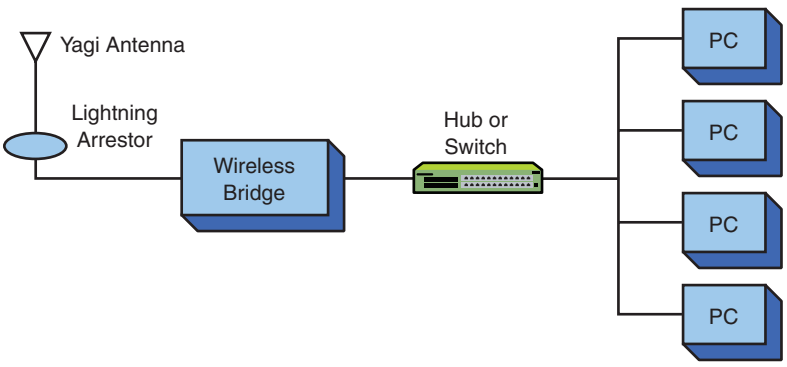


FIGURE 4-30 The setup for the remote users in the proposed point-to-multipoint wireless network.

Section 4-5 Review

This section covers the following Network+ exam objectives.

2.1 Compare and contrast various devices, their features, and their appropriate placement on the network.

This section examines various networking devices for establishing wireless networks.

2.4 Given a scenario, install and configure the appropriate wireless standards and technologies.

This section presents various types of antennas that can be used to develop a wireless network.

3.2 Explain the purpose of organizational documents and policies.

This section introduces the steps for completing a wireless antenna site survey.

3.3 Explain high availability and disaster recovery concepts and summarize which is the best solution.

This section discusses a situation in which the signal is being affected by multipath distortion from a small lake area. A fix to this might be to move the antenna to a different height to minimize reflection problems.

4.3 Given a scenario, apply network hardening techniques.

This section discusses the issues related to and planning for antenna placement.

5.4 Given a scenario, troubleshoot common wireless connectivity issues.

This section presents antenna types and placement.

Test Your Knowledge

1. Which types of antennas are typically used at receive sites from a multipoint distribution system? (Select all that apply.)

   a. Yagi
   b. Omnidirectional
   c. Parabolic
   d. Hydroxyl

2. True or false: When configuring remote installations for wireless networks, the receive site needs to be able to see the multipoint distribution antenna site.

   True

4-6 TROUBLESHOOTING WIRELESS NETWORKS

This section provides an overview of common techniques for troubleshooting wireless networks. Students should become familiar with each scenario presented.

This section examines some common techniques for troubleshooting wireless networks. Wireless networks have greatly simplified the steps for connecting to a network, but they do occasionally fail. The following sections describe some scenarios that users might encounter and steps for troubleshooting and resolving the wireless issues.

Access Point Hardware Issues

The primary hardware device in wireless networks is the access point. Some networks have multiple access points. A simple first step is to ping the IP address for an access point in order to verify network connectivity. You should expect a reply to the ping, but if you don't get a reply, you can verify the IP address and repeat the ping. If it still doesn't work, there is a good chance there is a problem with the access point. Try unplugging the access point and plugging it back in to reset the access point. Try the ping again, and if it still doesn't work, the access point might have a problem.

Wireless Router Issues

Make sure the client and wireless router support the same Wi-Fi version. For example, if a client computer's Wi-Fi card supports only 802.11b, the wireless router must also support 802.11b or must be configured to run in a mixed mode, with multiple protocols supported.

Also, in the case where multiple clients are connecting to the wireless router, it is important to understand that when an association is made between the client and the wireless router, the client with the lowest 802.11 system will set the clock speed. For example, say that a client running 802.11b and another running 802.11g connect to the same wireless router. The data transfer rate for 802.11b is 11Mbps, and the rate for 802.11g is 54Mbps. The wireless router will select 802.11b's lower clock rate for all associations. This can be of some concern to clients that have the capability to connect at a higher data transfer rate.

Wireless Compatibility

Not all wireless clients are created equal, and wireless clients depend on their hardware and software, which they must keep up to date. Also, in order to have reliable and good wireless connectivity, the wireless access point and the wireless clients must be compatible and use the same standard.

802.11n is a standard that can offer connectivity in either 2.4GHz or 5GHz or both. This means a wireless client can be 802.11n compatible just by operating in one frequency, not both. Therefore, an 802.11n wireless client with only a 2.4GHz radio will never achieve the high speed of 300Mbps offered by 5GHz. When troubleshooting the RF spectrum associated with a signal such as a Wi-Fi signal, a spectrum analyzer is typically used.

Signal Strength Problems

The purpose of measuring signal strength is to verify that you have good signal level at the receive location. Typically, the signal strength of a wireless connection can be adjusted at the access point to expand or reduce the area of coverage. Things change, and a loss in signal strength might not be a problem with the access point. It is possible that something could have been moved and is physically blocking the signal, thus causing RF attenuation. The RSSI (received signal strength indicator) value of a user should be monitored to identify signal strength issues.

Wireless Coverage

A wireless coverage area, or a cell, is very dependent on the RF transmission radiated from a wireless router or an access point. So, there is a limitation to the size of a cell for each access point. In a large geographic area, multiple wireless access points are deployed to create multiple cells in an attempt to give enough total coverage area. Good coverage depends on cells overlapping. Failure of cells to overlap introduces weak or dead wireless spots, thus creating insufficient wireless coverage. Also, bad coverage negatively affects client roaming. When a wireless client moves from one cell to another, it must establish an association with the new access point. With bad coverage, the AP association time increases, in turn causing delay or interruption.

Extending the Wireless Range

Another way to improve wireless coverage is to extend the wireless range. The following are general tips for extending the wireless range:

- Make sure the antenna is placed high and is not obstructed by any metal. It is important to remember that radio waves reflect off metal surfaces. Also, surfaces such as concrete and brick attenuate the signal.
- In some cases, you might have to use a high-gain antenna to help boost the receive signal strength.

Frequency Interference Problems

An electrical device such as a microwave oven may cause interference. Microwave ovens operate at the 2.4GHz frequency, which is the same band in which 802.11b/g/n devices operate. It is good to have a baseline measurement of the signal strength expected at each location in order to better identify interference. A good indicator of interference is the signal-to-noise RATIO (SNR).

Wireless Channel Utilization

For the 2.4GHz wireless frequency, the default channel for 802.11b, 802.11g, and 802.11n wireless routers is channel 6. If you have interference problems, there may be a wireless router nearby with an SSID using the same channel. In such a case, you can change the channel to 1 or 11 so that the RF spectra on these channels do

not overlap (refer to Figure 4-4). 802.11b, 802.11g, and 802.11n wireless routers have 11 possible channels, and you can select an alternate channel via the wireless router's settings. Changing to a different channel will reduce the SNR, which is likely to solve your problem. Even though 5GHz wireless has more channels, the same concept applies for 802.11a, 802.11n (5GHz), 802.11ac, and 802.11ax.

Load Issues

Wireless users share the same frequency channel to communicate to the same access point. If too many users connect to the same access point at the same time, they start experiencing slowness and packet drops due to overcapacity. For optimum load capacity, consult the documentation of the access point manufacturer.

SSID Issues

Once the SSID has been configured for a computer, it normally does not require reconfiguration. However, while traveling, you might reconfigure the SSID to connect to a different network. Also, when manually configuring an incorrect SSID or settings, human-error mistakes can be made. The simple fix is to reset the SSID when you return to your home network.

Securing Wi-Fi Issues

Any time you are connecting a wireless device to a public hotspot, there is a chance that someone using a packet sniffer will be able to see your data traffic. You can avoid possible problems by enabling WPA to secure your data traffic. Most wireless systems support multiple network security protocols (for example, different versions of WPA3, WPA2, WPA, or WEP). Make sure the client and access point are running the same security mode. Otherwise, an encryption protocol mismatch will occur, resulting in no wireless connection.

Cable Issues

Even when you are focusing on troubleshooting wireless issues, a problem could be due to a simple physical cable connection. A cable could be loose, may have become disconnected, or may be bad. It is always good to have a spare cable just in case. Remember that you can always verify that you have a connection by checking for the presence of a link light. Also, bad cables create attenuation and introduce loss of signal. Attenuation in any type of cable connecting to the access point—such as antenna cable attenuation, fiber cable attenuation, or Ethernet cable attenuation—could introduce signal issues into the wireless connection.

Deauthentication/Disassociation Attacks

Deauthentication and disassociation are legitimate handshakes used by a wireless client when leaving a wireless network. However, a denial of service (DOS) attack that exploits deauthentication and disassociation creates client disassociation issues. By spoofing a disassociate or deauthenticate message while pretending to be a targeted wireless client, the access point disassociates the targeted wireless client from the wireless network.

DHCP Issues

Wireless devices require valid IP addresses. Access points typically assign a 192.168.0.*x* address to the client. You can verify the IP address assigned by entering the command **ipconfig** at the command prompt (refer to Section 1-4, "The Ethernet LAN," in Chapter 1, "Introduction to Computer Networks").

Wireless Printer Issues

If you are experiencing problems with a wireless printer that was recently working, the first step is to restart the printer, your computer, and your wireless router. If this doesn't fix the problem, you can print the network configuration from the printer. Check the IP address for the printer and verify that it is assigned an IP address in your network. You can check the IP address of your computer by issuing the command **ipconfig** from the command prompt (refer to Section 1-4 in Chapter 1).

Section 4-6 Review

This section covers the following Network+ exam objective.

5.4 Given a scenario, troubleshoot common wireless connectivity issues.

This section presents the concept of an RSSI, which provides a signal strength measurement.

Test Your Knowledge

1. You are experiencing problems with a wireless printer that was recently working. How can you verify the IP address?
   a. Set the **ping** command to **auto** and look for a reply.
   b. Verify the IP address assigned by entering the command **ipconfig** at the command prompt.
   c. Remove the cover to the printer to find the MAC address.
   d. Ping the server
2. What issue is likely to happen if one wireless client is running 802.11b and another is running 802.11g, and both connect to the wireless router at the same time?
   a. There will be no issues.
   b. The wireless router will select 802.11g for setting the data transfer rate.
   c. The wireless router will select 802.11b for setting the data transfer rate.
   d. The access point will temporarily shut down until one client goes offline.

SUMMARY

This chapter presents an overview of wireless networking, including fundamental concepts and sample networks. The vendors of wireless networking equipment have made their devices easy to integrate into existing networks, but you must understand that the key objective of a network administrator is to provide a fast, reliable, and secure computer network. Carelessly integrating wireless components into a network can easily compromise this objective.

You should understand the following from reading this chapter:

- The operating characteristics of the 802.11 wireless networks
- The purposes of access points, wireless LAN adapters, and wireless bridges
- How to perform a basic site survey on a building
- How to configure a network for user mobility
- How to plan multipoint wireless distribution

Wireless networking technologies have greatly simplified planning and installation. However, they have also brought some complications. For example, any time you are working with RF, there is a chance of unexpected interference and noise. A well-planned RF installation requires a study of all known interference and a search for any possible interference. An RF study should also include signal path studies that enable the user to prepare a well-thought-out plan and allow an excellent prediction of received signal level. The bottom line is to obtain support for conducting an RF study.

QUESTIONS AND PROBLEMS

Section 4-2

1. List two advantages of wireless networking.

   User mobility and cost-effectiveness for areas where wiring would be too expensive

2. What are the three areas defined for the IEEE 802.11 standard?

   The physical layer, the MAC layer, and wireless management protocols and services

3. What is an ad hoc network?

   An ad hoc network is an independent network.

4. What is the purpose of an extended service set?

   An ESS uses multiple access points to extend user mobility.

5. What are the four physical layer technologies used in 802.11 wireless networking?

   DHSS: direct-sequence spread spectrum

   FHSS: frequency-hopping spread spectrum

   Infrared

   OFDM: orthogonal frequency-division multiplexing

6. Describe the frequency spectrum for the DSSS channels in 802.11b wireless networking.

   802.11 DSSS implements 14 channels (each consuming 22MHz) over approximately 90MHz of RF spectrum in the 2.4GHz ISM (industrial, scientific, and medical) band.

7. Define pseudorandom sequence as it applies to FHSS.

   Pseudorandom sequence means that the frequency-hopping sequence appears to be random, but it does repeat.

8. What must the FHSS transmitting and receiving units know in order to communicate?

   They must know the hopping sequence.

9. What are the frequency range and modulation technique used by 802.11a?

   5GHz, OFDM

10. What is the maximum data rate for each of the following?

    a. 802.11b

       11Mbps

    b. 802.11a

       54Mbps

    c. 802.11g

       54Mbps

    d. 802.11n

       200Mbps+

    e. 802.11ac

       1Gbps+

    f. 802.11ax

       10Gbps

11. Define MIMO as it applies to 802.11n.

    MIMO (multiple-input multiple-output) uses a technique called space-division multiplexing, in which the data stream is split into multiple parts called spatial streams. The different spatial streams are transmitted using separate antennas.

12. What is the purpose of the power save mode in 802.11n?

    With the power save mode, 802.11n uses multiple data paths only when faster data transmission is required, thus saving power.

Section 4-3

13. What is the purpose of an access point?

    An access point provides a bridge between a wireless LAN and a wired network.

14. How does an access point know if a wireless data packet is intended for its network?

    802.11 wireless LAN devices use an SSID to identify what wireless data traffic is allowed to connect to the network.

15. What is an association, and what is its purpose?

    An association is an established wireless connection. An access point uses an association to build a table of users (clients) on the wireless network.

16. Draw a picture of a point-to-point wireless connection.

    Refer to Figure 4-9(a)

17. Draw a picture of a point-to-multipoint wireless network.

    Refer to Figure 4-9(b)

18. What are the key issues to explore when conducting a site survey for each of the following?

    a. Indoor environment

       Electrical power connection points(s)

       Wired network connection point(s)

       Access point placement

       RF coverage area

       Bandwidth supported

    b. Outdoor environment

       Electrical power for the base access point

       Connection back to the home network

       Antenna selection

       Bandwidth supported

       RF coverage

Section 4-4

19. In what frequency band does Bluetooth operate?

    The 2.4GHz ISM band

20. How many output power classes does Bluetooth have? List the power level and the operating range for each class.

    Bluetooth has four operating classes.

Power Class	Average Output Power	Operating Distance
1	100 mW	~100 meters
2	2.5 mW	~10 meters
3	1 mW	~1 meter
4	0.5 mW	~0.5 meter

21. What is a piconet?

    A piconet is an ad hoc network consisting of up to eight Bluetooth devices.

22. What is the purpose of the inquiry procedure in Bluetooth?

    A Bluetooth device uses the inquiry procedure to discover other Bluetooth devices or to allow itself to be discovered.

23. What is the purpose of the paging procedure in Bluetooth?

    A Bluetooth device uses the paging procedure to establish and synchronize a connection between two networking devices.

24. Define the term backscatter.

    Backscatter refers to the reflection of the radio waves striking an RFID tag back to the transmitter source.

25. What are the three parameters that define an RFID system?

    Means of powering the tag, frequency of operation, communication protocol

26. Explain how power is provided to a passive RFID tag.

    Power is provided by rectifying the RF energy transmitted by the reader that strikes the RF tag antenna.

27. What are three advantages of using an active RFID tag?

    Can incorporate wireless Ethernet connectivity, can incorporate location capability, the unit is always turned on

28. What three frequency bands are typically used for RFID tags?

    LF: 125/134KHz

    HF: 13.56MHz

    UHF: 860–960MHZ and 2.4GHz

29. What is the WiMAX frequency standard for the United States?

    5.8GHz and 2.5GHz

30. Why was OFDM selected for WiMAX?

    OFDM was selected for WiMAX because of its improved NLOS characteristics.

31. How does WiMAX differ from Wi-Fi?

    Frequency assignments differ and data rates differ, but the main difference is that the WiMAX unit only has to compete once to gain entry to a network.

Section 4-5

32. What type of wireless connection is used to connect a home network to a multipoint distribution site?

    Point-to-point

33. Use the Internet to find a source of omnidirectional and directional antennas for each of the following standards:

    a. 802.11b
    b. 802.11a
    c. 802.11g
    d. 802.11n
    e. 802.11ac
    f. 802.11ax

34. Prepare a list of three manufacturers for each antenna type. Include cost figures.

    There are many sources for wireless network antennas. Expect the students to come up with many possible solutions.

Section 4-6

35. What command can you issue to verify network connectivity in a wireless LAN?

    ping

36. True or false: When an association is made between a client and a wireless router, the client with the lowest 802.11 system sets the clock speed.

    True

37. True or false: In order to have reliable and good throughput wireless connectivity, the wireless access point and the wireless clients must be compatible and use the same standard.

    True

38. What is the purpose of measuring signal strength at the receive location?

    The purpose of measuring signal strength at the receive location is to verify that you have good signal level.

39. What happens when wireless cell coverage isn't overlapping?

    Weak or dead wireless spots appear, thus creating insufficient wireless coverage.

40. Which of the following are general tips for extending your wireless range? (Select all that apply.)

    a. Make sure the antenna is placed high.
    b. Use a high-gain antenna to help boost the receive signal strength.
    c. Enclose the antenna with brick or concrete.
    d. Place the antenna on the ground.

41. True or false: Microwave ovens can cause interference with Wi-Fi signals.

    True

42. The default channel for 802.11b and 802.11g wireless routers is channel 6. If you have interference problems, there may be a wireless router nearby with an SSID using the same channel. You can change the channel to which of the following? (Select all that apply.)

    a. 1
    b. 3
    c. 7
    d. 8
    e. 11

43. What is meant by the term *load issues* regarding wireless access points?

    Too many users are connecting to the same access point at the same time.

44. True or false: Once the SSID (service set identifier) has been configured for a computer, it normally does not require reconfiguration. However, when you travel, you should use a PSSID (portable service set identifier) to connect to remote access points.

    False

45. What happens when an encryption protocol mismatch occurs?

    a. The SSID has to be reconfigured.
    b. The wireless authentication fails and requires reconfiguration of the client's SSID.
    c. The wireless authentication is not successful, resulting in not being able to connect to the SSID.
    d. The lowest level of encryption is applied.

46. You can avoid security problems when connecting a wireless device to a public hotspot by doing which of the following?

    a. Enabling WPA to secure your data traffic
    b. Enabling WAP to secure your data traffic
    c. Disabling WPA
    d. Disabling WAP

47. Which of the following can introduce signal loss into a wireless connection? (Select all that apply.)

    a. Antenna cable attenuation
    b. Wrong IP address
    c. An object blocking the wireless signal
    d. Radio station broadcast

48. A denial of service (DOS) attack creates client disassociation issues by doing two of the following?

    a. Setting up a continuous ping, thereby taking control of the network
    b. Replacing the SSID with a PSSID and connecting to non-authenticated access points
    c. Spoofing a disassociate or deauthenticate message and pretending to be a targeted wireless client
    d. Downgrading WPA3 to WPA2 encryption

49. An access point typically assigns a 192.168.0.*x* address to a client. How can you verify the IP address assigned?

    a. By entering the command **config-ip** at the command prompt
    b. By entering the command **ipconfig** at the command prompt
    c. By entering the command **configip** at the command prompt
    d. By pushing the reset button on the WAP

50. When you experience problems with a wireless printer that was recently working, what is the first step you should take?

    a. Restart the printer, your computer, and your wireless router.
    b. Replace the access point and router and reconfigure both of them.
    c. Remove the cable connecting the printer and replace it.
    d. Update the firmware on the wireless router.

Critical Thinking

51. A wireless network receiving site is experiencing occasional loss of signal due to interference. Discuss the steps you would take to correct this problem.

    The options for solving this problem vary depending on the location of the network receiving site. If this is an indoor site, an additional access point may be required. For an outdoor site, the antenna might need to be aligned or replaced with a more directional antenna. You also might be able to reduce impacts of RF interference by changing the access point channel. For example, most microwave ovens emit RF signals in the upper third of the 2.4GHz band. You can generally avoid microwave oven interference by tuning nearby access points to channels 1 or 6.

52. Prepare a memo to your supervisor, explaining why it is important to run encryption on your wireless network.

    The student should report that it is easy for data to be viewed over an unencrypted wireless network. The student could say something about the fact that sensitive information about personnel or the company is being broadcast to the public if encryption is not used.

53. Your company has a suite in a business complex. Another company in the suite next to you has a wireless 802.11b network with the SSID Company A. You can pick up that company's signal from your suite. Your company would like to put up its own wireless network with two access points. Discuss how you would set up these two access points so that your company can obtain optimal performance.

    It is important to determine which of the 802.11b channels the SSID Company A is using. Then you can deploy the wireless access points using different, non-overlapping channels. This will help eliminate interference. Also, it is important to do a site survey within your own suite. You want to place the two wireless access points in such a way that their radio signals provide overlapping coverage for the entire suite and their signal will be minimally reflected by the obstacles within the suite.

Certification Questions

54. True or false: If the signal quality drops from excellent to good, the antenna or access point should be replaced.

    False

55. The network administrator is setting up a wireless network. There is a chance of radio interference. How can the network administrator avoid or minimize potential interference problems?

    a. Perform an RF study prior to installation of the wireless network.
    b. Contact all owners of equipment that may cause interference and ask them to use different systems.

c. Contact the FCC to have the interfering sources shut down.

d. All of these answers are correct.

56. Define MIMO relative to 802.11n.

a. MIMO is a multiplexing technique in which the power is split into multiple parts called spatial currents.

b. MIMO is a frequency-division multiplexing technique in which the data stream is split into multiple parts called spectral streams.

c. MIMO is an OFDM multiplexing technique in which the digital data is portioned into multiple parts called filtered streams.

d. MIMO is a space-division multiplexing technique in which the data stream is split into multiple parts called spatial streams.

57. Which of the following best characterizes CSMA/CA?

a. It replaces CSMA/CD.

b. It provides carrier sense with collision avoidance.

c. It provides carrier sense with congestion avoidance.

d. It provides congestion sensing with collision avoidance.

58. Which of the following are advantages of 802.11g? (Select all that apply.)

a. Compatible with 802.11b

b. Compatible with 802.11a

c. Uses infrared instead of radio

d. High speed

59. Which of the following is used in wireless LANs to identify whether a client is to become a member of the wireless network?

a. SSID

b. MAC address

c. IP address

d. Echo

60. What does the term *last mile* mean in relation to telecommunications?

a. The distance from an RF transmitter to a receiver in WiMAX

b. A measurement of signal coverage for WiMAX and for Wi-Fi

c. A term for the last connection prior to linking to the RF transmitter

d. The last part of the connection from the telecommunications provider to the customer

61. Which of the following is the best way to extend the radio range of a station's wireless link with one access point?

    a. Add multiple access points
    b. Add additional wiring
    c. Add 87BZS encoding
    d. Add B8ZS encoding

62. Which of the following statements is true?

    a. The Wi-Fi Alliance is an organization that assembles and tests wireless equipment before it is shipped to vendors.
    b. The Wi-Fi Alliance is an organization that tests and certifies wireless equipment for compliance with the 803.1 standards.
    c. The Wi-Fi Alliance is an organization that tests and certifies wireless equipment for compliance with the 802.11*x* standards.
    d. None of these answers are correct.

63. Which of the following are current wireless networking standards? (Select all that apply.)

    a. 802.12n
    b. 802.11g
    c. 803.11g
    d. 802.11a
    e. 802.11b
    f. 802.55a
    g. 802.11n
    h. 802.1a
    i. 802.11ac
    j. 802.11ax

INDEX

Symbols

Numbers

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