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

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

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

Library of Congress Control Number: 2021913557

ScoutAutomatedPrintCode

Trademarks

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

Warning and Disclaimer

Every effort has been made to make this book as complete and as accurate as possible, but no warranty or fitness is implied. The information provided is on an "as is" basis. The authors and the publisher shall have neither liability nor responsibility to any person or entity with respect to any loss or damages arising from the information contained in this book.

Special Sales

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

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

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

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

CHAPTER 5 Interconnecting the LANs 228

Online Only Elements:

Net-Challenge Software
Wireshark Captures
Network+ quizzes

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

READER SERVICES

Register your copy of *Networking Essentials*, Sixth Edition at www.pearsonitcertification.com for convenient access to downloads, updates, and corrections as they become available. To start the registration process, go to www.pearsonitcertification.com/register and log in or create an account.* Enter the product ISBN 9780137455928 and click Submit. When the process is complete, you will find any available bonus content under Registered Products.

*Be sure to check the box that you would like to hear from us to receive exclusive discounts on future editions of this product.

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.

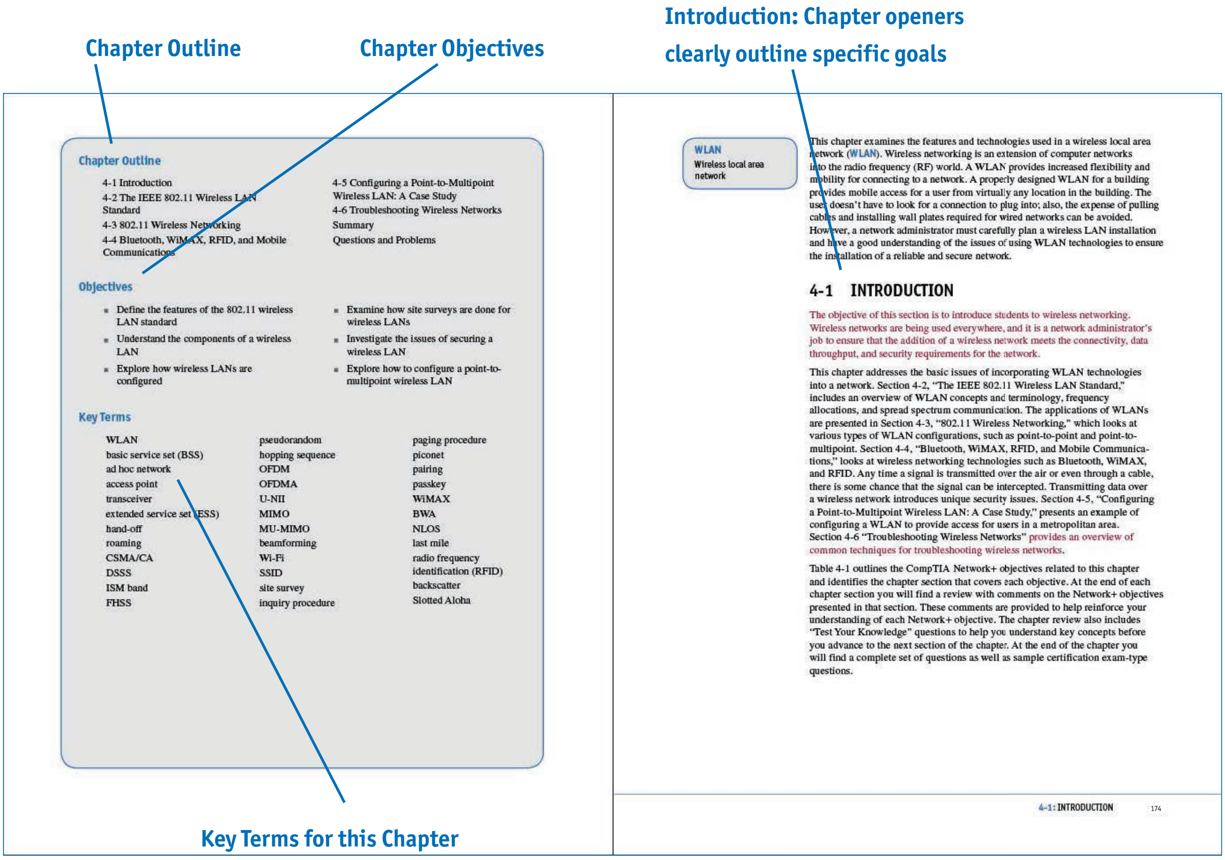
ORGANIZATION OF THE TEXT

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.


Chapter Outline
Chapter Objectives
Introduction: Chapter openers clearly outline specific goals
Key Terms for this Chapter

Chapter Outline

4-1 Introduction
4-2 The IEEE 802.11 Wireless LAN Standard
4-3 802.11 Wireless Networking
4-4 Bluetooth, WiMAX, RFID, and Mobile Communications
4-5 Configuring a Point-to-Multipoint Wireless LAN: A Case Study
4-6 Troubleshooting Wireless Networks
Summary
Questions and Problems

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.

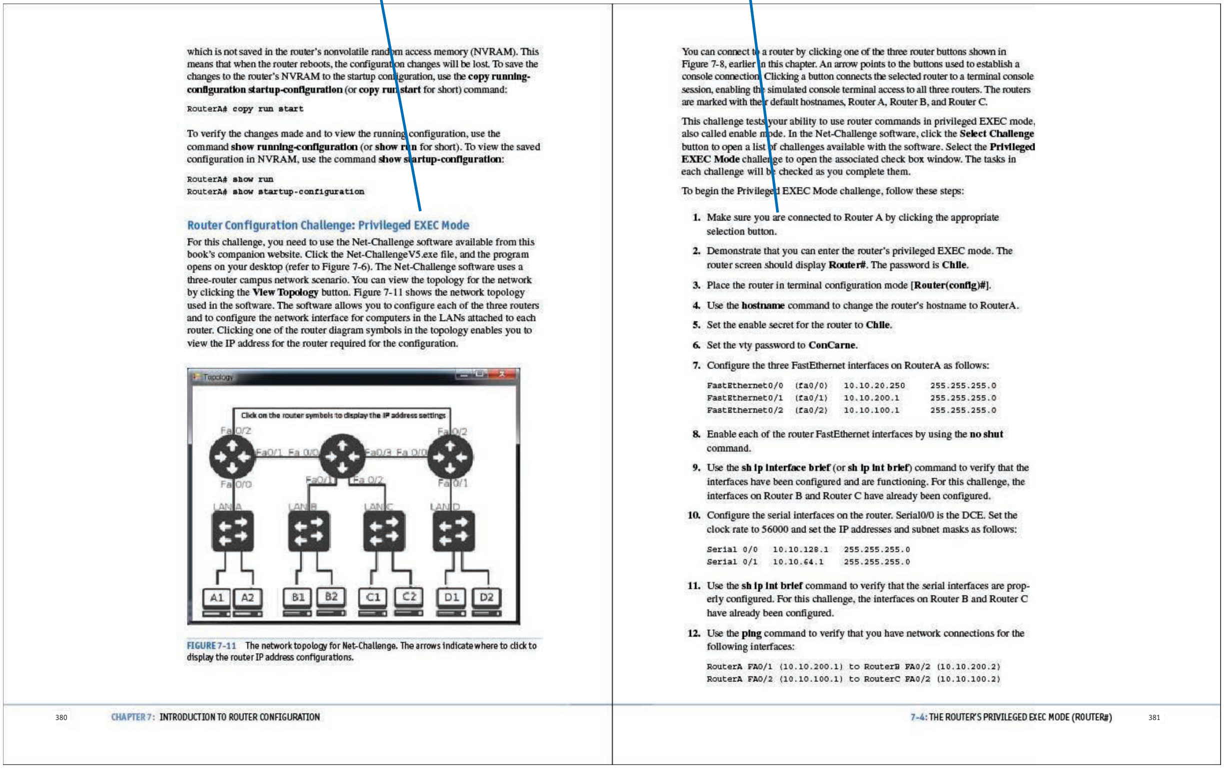
4-1: INTRODUCTION 174

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.

Net-Challenge exercises are found throughout the text where applicable

Exercises challenge readers to undertake certain tasks



which is not saved in the router's nonvolatile random access memory (NVRAM). This means that when the router reboots, the configuration changes will be lost. To save the changes to the router's NVRAM to the startup configuration, use the **copy running-configuration startup-configuration** (or **copy run start** for short) command:

```
RouterA# copy run start
```

To verify the changes made and to view the running configuration, use the command **show running-configuration** (or **show run** for short). To view the saved configuration in NVRAM, use the command **show startup-configuration**:

```
RouterA# show run
RouterA# show startup-configuration
```

Router Configuration Challenge: Privileged EXEC Mode

For this challenge, you need to use the Net-Challenge software available from this book's companion website. Click the Net-ChallengeV5.exe file, and the program opens on your desktop (refer to Figure 7-6). The Net-Challenge software uses a three-router campus network scenario. You can view the topology for the network by clicking the **View Topology** button. Figure 7-11 shows the network topology used in the software. The software allows you to configure each of the three routers and to configure the network interface for computers in the LANs attached to each router. Clicking one of the router diagram symbols in the topology enables you to view the IP address for the router required for the configuration.

FIGURE 7-11 The network topology for Net-Challenge. The arrows indicate where to click to display the router IP address configurations.

380 CHAPTER 7: INTRODUCTION TO ROUTER CONFIGURATION

You can connect to a router by clicking one of the three router buttons shown in Figure 7-8, earlier in this chapter. An arrow points to the buttons used to establish a console connection. Clicking a button connects the selected router to a terminal console session, enabling the simulated console terminal access to all three routers. The routers are marked with their default hostnames, Router A, Router B, and Router C.

This challenge tests your ability to use router commands in privileged EXEC mode, also called enable mode. In the Net-Challenge software, click the **Select Challenge** button to open a list of challenges available with the software. Select the **Privileged EXEC Mode** challenge to open the associated check box window. The tasks in each challenge will be checked as you complete them.

To begin the Privileged EXEC Mode challenge, follow these steps:

1. Make sure you are connected to Router A by clicking the appropriate selection button.
2. Demonstrate that you can enter the router's privileged EXEC mode. The router screen should display **Router#**. The password is **Chile**.
3. Place the router in terminal configuration mode [**Router(config)#**].
4. Use the **hostname** command to change the router's hostname to RouterA.
5. Set the enable secret for the router to **Chile**.
6. Set the vty password to **ConCarne**.
7. Configure the three FastEthernet interfaces on RouterA as follows:

```
FastEthernet0/0  (fa0/0)  10.10.20.250   255.255.255.0
FastEthernet0/1  (fa0/1)  10.10.200.1    255.255.255.0
FastEthernet0/2  (fa0/2)  10.10.100.1    255.255.255.0
```

8. Enable each of the router FastEthernet interfaces by using the **no shut** command.
9. Use the **sh ip interface brief** (or **sh ip int brief**) command to verify that the interfaces have been configured and are functioning. For this challenge, the interfaces on Router B and Router C have already been configured.
10. Configure the serial interfaces on the router. Serial0/0 is the DCE. Set the clock rate to 56000 and set the IP addresses and subnet masks as follows:

```
Serial 0/0  10.10.128.1  255.255.255.0
Serial 0/1  10.10.64.1   255.255.255.0
```

11. Use the **sh ip int brief** command to verify that the serial interfaces are properly configured. For this challenge, the interfaces on Router B and Router C have already been configured.
12. Use the **ping** command to verify that you have network connections for the following interfaces:

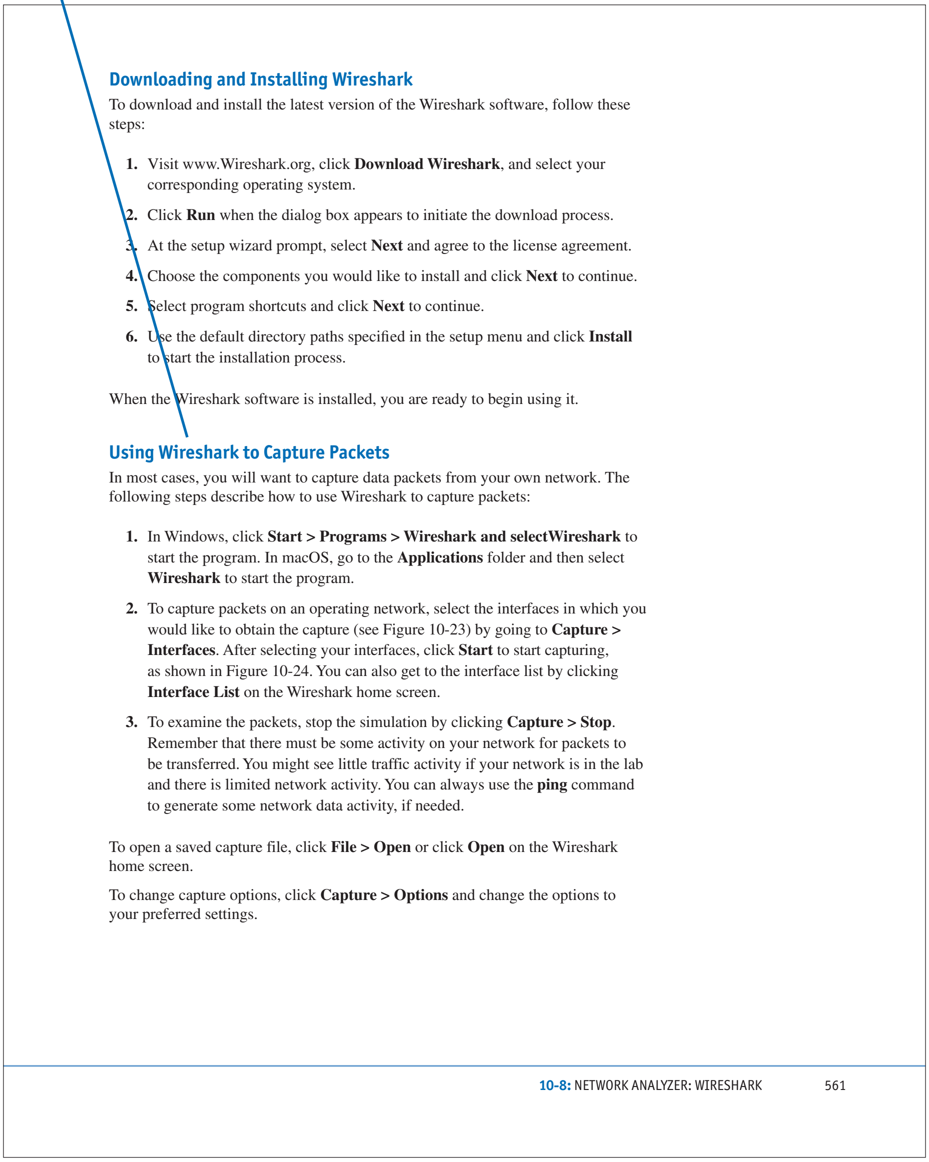
```
RouterA FA0/1 (10.10.200.1) to RouterB FA0/2 (10.10.200.2)
RouterA FA0/2 (10.10.100.1) to RouterC FA0/2 (10.10.100.2)
```

7-4: THE ROUTER'S PRIVILEGED EXEC MODE (ROUTER#) 381

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.

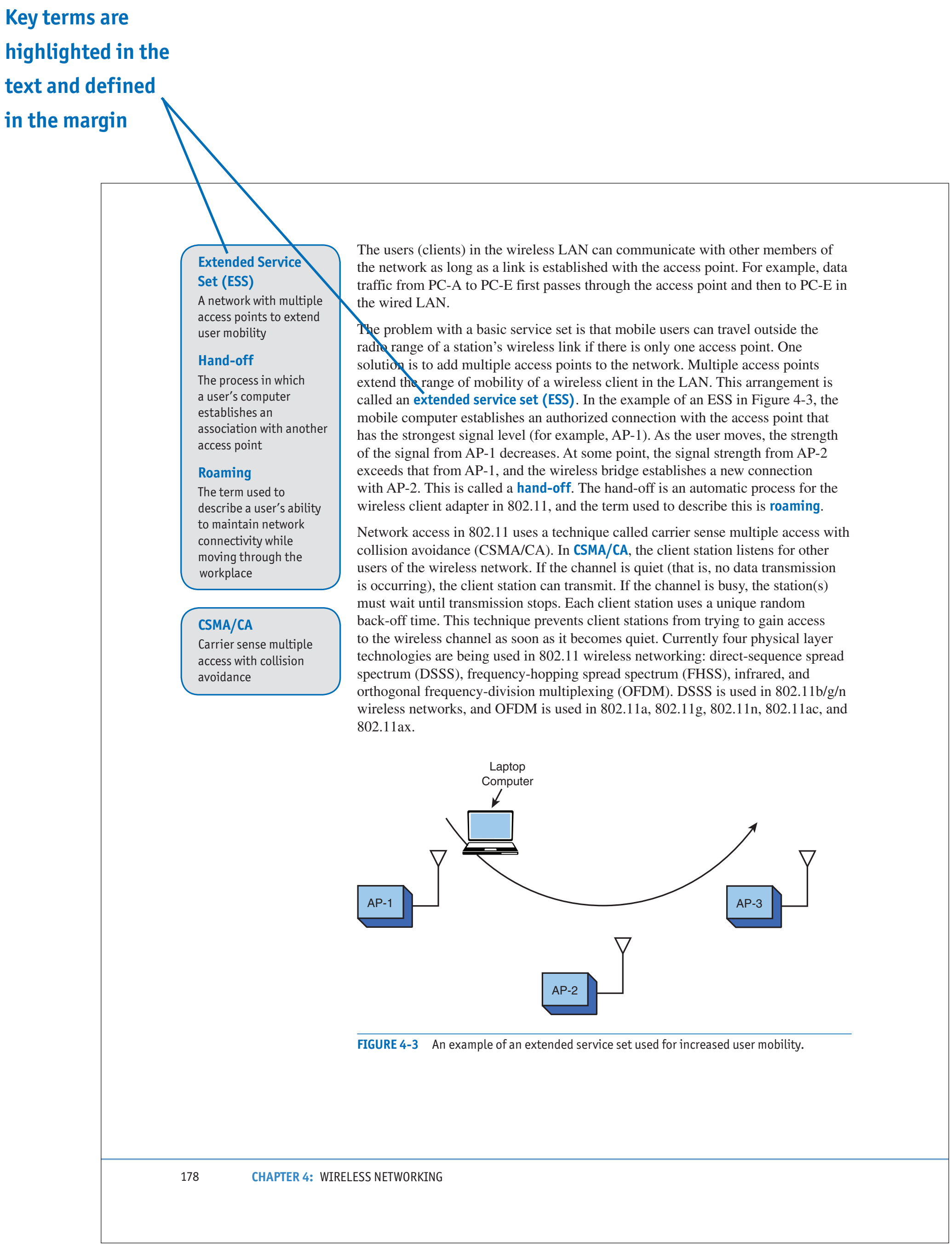
To open a saved capture file, click **File > Open** or click **Open** on the Wireshark home screen.

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

10-8: NETWORK ANALYZER: WIRESHARK 561

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**.

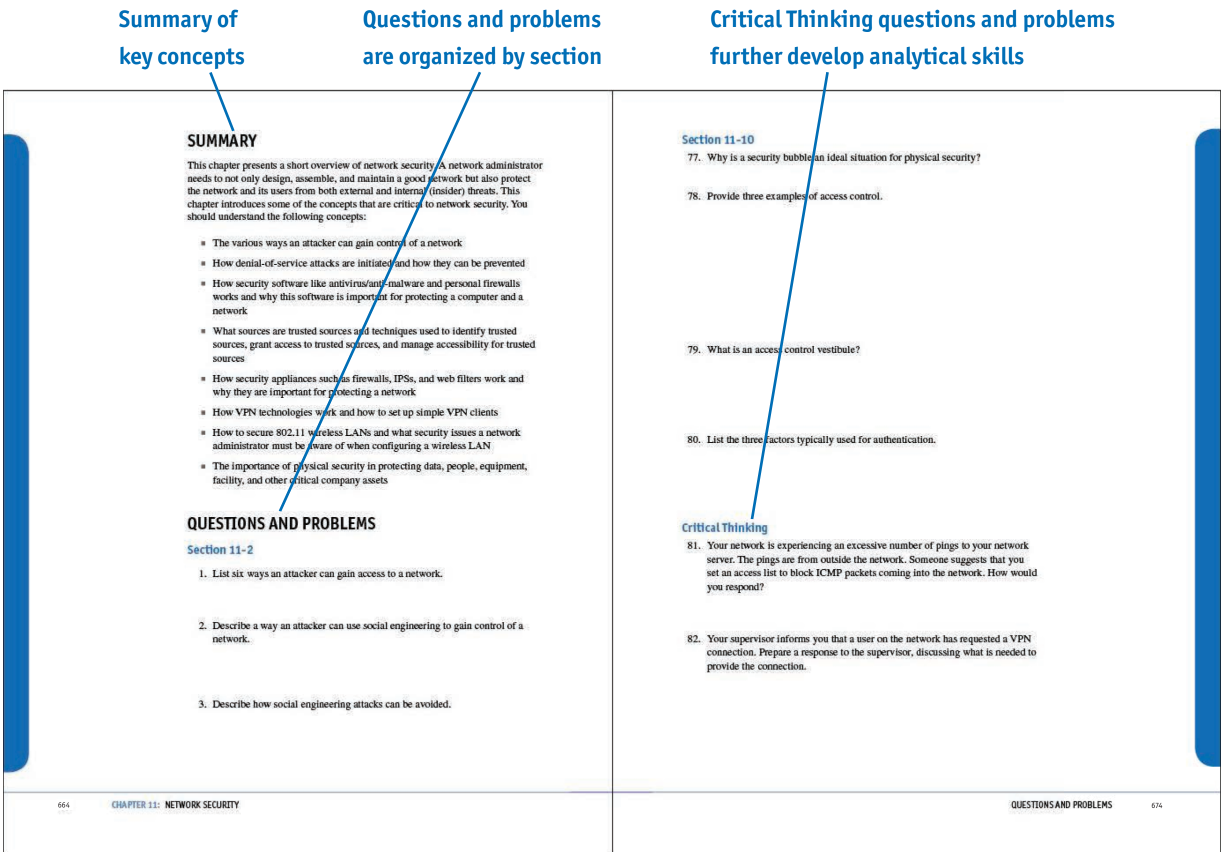
Network access in 802.11 uses a technique called carrier sense multiple access with collision avoidance (CSMA/CA). In **CSMA/CA**, the client station listens for other users of the wireless network. If the channel is quiet (that is, no data transmission is occurring), the client station can transmit. 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.

178 **CHAPTER 4:** WIRELESS NETWORKING

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



Summary of key concepts

Questions and problems are organized by section

Critical Thinking questions and problems further develop analytical skills

SUMMARY

This chapter presents a short overview of network security. A network administrator needs to not only design, assemble, and maintain a good network but also protect the network and its users from both external and internal (insider) threats. This chapter introduces some of the concepts that are critical to network security. You should understand the following concepts:

- The various ways an attacker can gain control of a network
- How denial-of-service attacks are initiated and how they can be prevented
- How security software like antivirus/anti-malware and personal firewalls works and why this software is important for protecting a computer and a network
- What sources are trusted sources and techniques used to identify trusted sources, grant access to trusted sources, and manage accessibility for trusted sources
- How security appliances such as firewalls, IPSs, and web filters work and why they are important for protecting a network
- How VPN technologies work and how to set up simple VPN clients
- How to secure 802.11 wireless LANs and what security issues a network administrator must be aware of when configuring a wireless LAN
- The importance of physical security in protecting data, people, equipment, facility, and other critical company assets

QUESTIONS AND PROBLEMS

Section 11-2

1. List six ways an attacker can gain access to a network.

2. Describe a way an attacker can use social engineering to gain control of a network.

3. Describe how social engineering attacks can be avoided.

664 CHAPTER 11: NETWORK SECURITY

Section 11-10

77. Why is a security bubble an ideal situation for physical security?

78. Provide three examples of access control.

79. What is an access control vestibule?

80. List the three factors typically used for authentication.

Critical Thinking

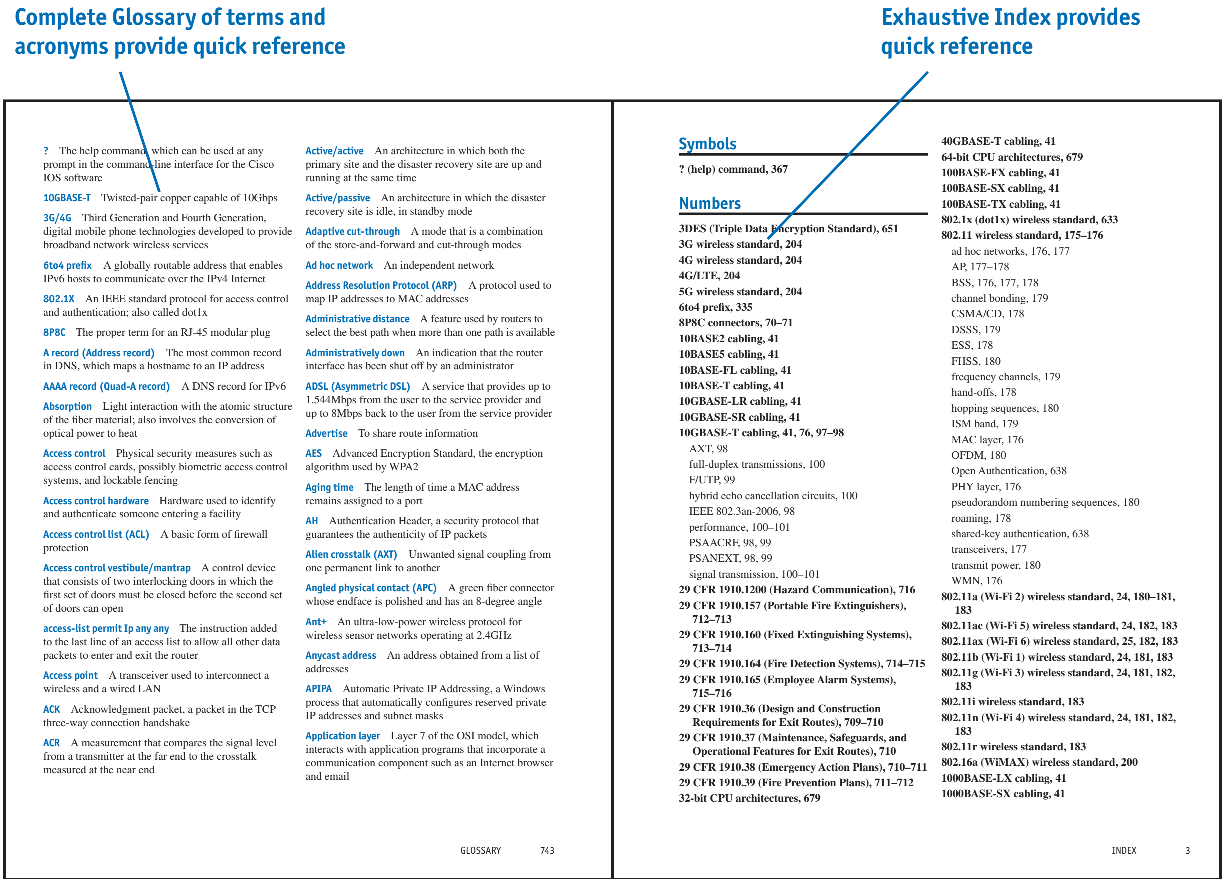
81. Your network is experiencing an excessive number of pings to your network server. The pings are from outside the network. Someone suggests that you set an access list to block ICMP packets coming into the network. How would you respond?

82. Your supervisor informs you that a user on the network has requested a VPN connection. Prepare a response to the supervisor, discussing what is needed to provide the connection.

QUESTIONS AND PROBLEMS 674

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).



Complete Glossary of terms and acronyms provide quick reference

Exhaustive Index provides quick reference

? The help command, which can be used at any prompt in the command-line interface for the Cisco IOS software

10GBASE-T Twisted-pair copper capable of 10Gbps

3G/4G Third Generation and Fourth Generation, digital mobile phone technologies developed to provide broadband network wireless services

6to4 prefix A globally routable address that enables IPv6 hosts to communicate over the IPv4 Internet

802.1X An IEEE standard protocol for access control and authentication; also called dot1x

8P8C The proper term for an RJ-45 modular plug

A record (Address record) The most common record in DNS, which maps a hostname to an IP address

AAAA record (Quad-A record) A DNS record for IPv6

Absorption Light interaction with the atomic structure of the fiber material; also involves the conversion of optical power to heat

Access control Physical security measures such as access control cards, possibly biometric access control systems, and lockable fencing

Access control hardware Hardware used to identify and authenticate someone entering a facility

Access control list (ACL) A basic form of firewall protection

Access control vestibule/mantrap A control device that consists of two interlocking doors in which the first set of doors must be closed before the second set of doors can open

access-list permit Ip any any The instruction added to the last line of an access list to allow all other data packets to enter and exit the router

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

ACK Acknowledgment packet, a packet in the TCP three-way connection handshake

ACR A measurement that compares the signal level from a transmitter at the far end to the crosstalk measured at the near end

Active/active An architecture in which both the primary site and the disaster recovery site are up and running at the same time

Active/passive An architecture in which the disaster recovery site is idle, in standby mode

Adaptive cut-through A mode that is a combination of the store-and-forward and cut-through modes

Ad hoc network An independent network

Address Resolution Protocol (ARP) A protocol used to map IP addresses to MAC addresses

Administrative distance A feature used by routers to select the best path when more than one path is available

Administratively down An indication that the router interface has been shut off by an administrator

ADSL (Asymmetric DSL) A service that provides up to 1.544Mbps from the user to the service provider and up to 8Mbps back to the user from the service provider

Advertise To share route information

AES Advanced Encryption Standard, the encryption algorithm used by WPA2

Aging time The length of time a MAC address remains assigned to a port

AH Authentication Header, a security protocol that guarantees the authenticity of IP packets

Alien crosstalk (AXT) Unwanted signal coupling from one permanent link to another

Angled physical contact (APC) A green fiber connector whose endface is polished and has an 8-degree angle

Ant+ An ultra-low-power wireless protocol for wireless sensor networks operating at 2.4GHz

Anycast address An address obtained from a list of addresses

APIPA Automatic Private IP Addressing, a Windows process that automatically configures reserved private IP addresses and subnet masks

Application layer Layer 7 of the OSI model, which interacts with application programs that incorporate a communication component such as an Internet browser and email

GLOSSARY 743

Symbols

? (help) command, 367

Numbers

3DES (Triple Data Encryption Standard), 651
3G wireless standard, 204
4G wireless standard, 204
4G/LTE, 204
5G wireless standard, 204
6to4 prefix, 335
8P8C connectors, 70–71
10BASE2 cabling, 41
10BASE5 cabling, 41
10BASE-FL cabling, 41
10BASE-T cabling, 41
10GBASE-LR cabling, 41
10GBASE-SR cabling, 41
10GBASE-T cabling, 41, 76, 97–98
AXT, 98
full-duplex transmissions, 100
F/UTP, 99
hybrid echo cancellation circuits, 100
IEEE 802.3an-2006, 98
performance, 100–101
PSAACRF, 98, 99
PSANEXT, 98, 99
signal transmission, 100–101
29 CFR 1910.1200 (Hazard Communication), 716
29 CFR 1910.157 (Portable Fire Extinguishers), 712–713
29 CFR 1910.160 (Fixed Extinguishing Systems), 713–714
29 CFR 1910.164 (Fire Detection Systems), 714–715
29 CFR 1910.165 (Employee Alarm Systems), 715–716
29 CFR 1910.36 (Design and Construction Requirements for Exit Routes), 709–710
29 CFR 1910.37 (Maintenance, Safeguards, and Operational Features for Exit Routes), 710
29 CFR 1910.38 (Emergency Action Plans), 710–711
29 CFR 1910.39 (Fire Prevention Plans), 711–712
32-bit CPU architectures, 679
40GBASE-T cabling, 41
64-bit CPU architectures, 679
100BASE-FX cabling, 41
100BASE-SX cabling, 41
100BASE-TX cabling, 41
802.1x (dot1x) wireless standard, 633
802.11 wireless standard, 175–176
ad hoc networks, 176, 177
AP, 177–178
BSS, 176, 177, 178
channel bonding, 179
CSMA/CD, 178
DSSS, 179
ESS, 178
FHSS, 180
frequency channels, 179
hand-offs, 178
hopping sequences, 180
ISM band, 179
MAC layer, 176
OFDM, 180
Open Authentication, 638
PHY layer, 176
pseudorandom numbering sequences, 180
roaming, 178
shared-key authentication, 638
transceivers, 177
transmit power, 180
WMN, 176
802.11a (Wi-Fi 2) wireless standard, 24, 180–181, 183
802.11ac (Wi-Fi 5) wireless standard, 24, 182, 183
802.11ax (Wi-Fi 6) wireless standard, 25, 182, 183
802.11b (Wi-Fi 1) wireless standard, 24, 181, 183
802.11g (Wi-Fi 3) wireless standard, 24, 181, 182, 183
802.11i wireless standard, 183
802.11n (Wi-Fi 4) wireless standard, 24, 181, 182, 183
802.11r wireless standard, 183
802.16a (WiMAX) wireless standard, 200
1000BASE-LX cabling, 41
1000BASE-SX cabling, 41

INDEX 3

FIGURE I-6

Companion Website

The companion website includes the captured data packets used throughout the book. It also includes the Net-Challenge 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.

1

CHAPTER

Introduction to Computer Networks

Chapter Outline

Objectives

- Explain the various LAN topologies
- Define the function of a networking protocol
- Describe CSMA/CD for the Ethernet protocol
- Describe the structure of an Ethernet frame
- Define the function of a network interface card
- Describe the purpose of a MAC address on a networking device
- Discuss how to determine the MAC address for a computer
- Discuss the fundamentals of IP addressing
- Discuss the issues involved in configuring a home network
- Discuss the issues involved in assembling an office LAN

Key Terms

local area network (LAN)
protocol
topology
Token Ring network
Token passing
IEEE
deterministic
Token Ring hub
bus topology
star topology
hub
multiport repeater
broadcast
switch
port
mesh topology
OSI model
physical layer
data link layer
network layer
transport layer
session layer
presentation layer
application layer
CSMA/CD
frame
network interface card (NIC)
MAC address
organizationally unique identifier (OUI)
Ethernet address, physical address, hardware address, or adapter address
ipconfig /all
IANA
IP address
network number
host number
host address
ISP
private addresses
intranet
IP internetwork
TCP/IP
wired network
wireless network
Wi-Fi Alliance
wireless router
range extender
hotspot
service set identifier (SSID)
firewall protection
stateful packet inspection (SPI)
virtual private network (VPN)
network address translation (NAT)

Key Terms continued

overloading
port address translation (PAT)
port forwarding (or port mapping)
CAT6 (Category 6)
RJ-45
Mbps
numerics
crossover
straight-through
uplink port
link light
link integrity test
link pulses
client
peer
peer-to-peer network
client/server network
ping
ICMP
ipconfig

1-1 INTRODUCTION

Each day, computer users use their computers for browsing the Internet, sending and retrieving email, scheduling meetings, sharing files, preparing reports, exchanging images, downloading music, and checking the current prices of auction items. A network connects computers with the goal of sharing their resources. The networks around the world that are connected together form the Internet. Networking requires that computers be able to access multiple networks and share their resources. This chapter looks at the various types of computer networks that are in use today.

This book introduces the essentials involved in implementing modern computer networks, stepping you through the various modern networking technologies. The accompanying textbook web link takes you to the Net-Challenge simulator software developed specifically for this text. This software gives you invaluable insight into the inner workings of computer networking and the experience of configuring routers and switches for use in computer networks.

The ease of connecting to the Internet and the dramatic decrease in the cost of computer systems have led to an explosion in the use of computer systems. Organizations such as corporations, colleges, and government agencies have acquired large numbers of single-user computer systems. Such systems might be dedicated to word processing, scientific computation, or process control, or they might be general-purpose computers that perform many tasks. Interconnection of locally distributed computer networks enables users to exchange information (data) with other network members. It also makes possible resource sharing, enabling many to access expensive equipment such as file servers and high-quality graphics printers as well as more powerful computers for tasks too complicated for the local computer to process.

The networks in use today can be generally categorized based on their geographic span:

- **Personal area network (PAN):** A PAN is the smallest type of network and has a limited span, interconnecting personal devices such as those that are Bluetooth enabled.

- **Local area network (LAN):** A LAN is a network commonly used to interconnect and share computer resources inside a building or multiple buildings in a limited area.
- **Campus area network (CAN):** A CAN—often called simple an *enterprise network*—spans multiple buildings in a campus environment such as a university or another large organization.
- **Metropolitan area network (MAN):** A MAN spans multiple buildings in a city area.
- **Wide area network (WAN):** A WAN is much larger than the other network types and can span many areas, such as cities, states, or countries.

Local Area Network (LAN)
A network of users that share computer resources in a limited area

Table 1-1 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 1-1 **Chapter 1 CompTIA Network+ Objectives**

Domain/Objective Number	Domain/Objective Description	Section(s) Where Objective Is Covered
1.0	**Networking Fundamentals**	
1.1	Compare and contrast the Open Systems Interconnection (OSI) model layers and encapsulation concepts.	1-3, 1-4
1.2	Explain the characteristics of network topologies and network types.	1-2, 1-5, 1-7
1.3	Summarize the types of cables and connectors and explain which is the appropriate type for a solution.	1-6
1.4	Given a scenario, configure a subnet and use appropriate IP addressing schemes.	1-4, 1-5
1.5	Explain common ports and protocols, their application, and encrypted alternatives.	1-3, 1-7
1.6	Explain the use and purpose of network services.	1-5, 1-7
1.7	Explain basic corporate and datacenter network architecture.	1-3
1.8	Summarize cloud concepts and connectivity options	1-4, 1-5, 1-6
2.0	**Network Implementations**	
2.1	Compare and contrast various devices, their features, and their appropriate placement on the network.	1-2, 1-4, 1-5, 1-6
2.2	Compare and contrast routing technologies and bandwidth management concepts.	1-5

Domain/Objective Number	Domain/Objective Description	Section(s) Where Objective Is Covered
2.3	Given a scenario, configure and deploy common Ethernet switching features.	1-3, 1-4, 1-5, 1-6
2.4	Given a scenario, install and configure the appropriate wireless standards and technologies.	1-5
3.0	**Network Operations**	
3.1	Given a scenario, use the appropriate statistics and sensors to ensure network availability.	1-3, 1-4, 1-5
3.3	Explain high availability and disaster recovery concepts and summarize which is the best solution.	1-5, 1-6
4.0	**Network Security**	
4.3	Given a scenario, apply network hardening techniques.	1-5
4.5	Explain the importance of physical security.	1-6
5.0	**Network Troubleshooting**	
5.2	Given a scenario, troubleshoot common cable connectivity issues and select the appropriate tools.	1-5, 1-6
5.3	Given a scenario, use the appropriate network software tools and commands.	1-3, 1-4, 1-5, 1-7
5.4	Given a scenario, troubleshoot common wireless connectivity issues.	1-5, 1-6

1-2 NETWORK TOPOLOGIES

This chapter presents the networking topologies commonly used in computer networks today. It is important for students to understand the structure of the star topology. Students should also understand the Token Ring and bus topologies even though they are seldom used today.

A LAN is defined in terms of the **protocol** and the **topology** used for accessing the network. The networking protocol is the set of rules established for users to exchange information. The topology is the network architecture used to interconnect the networking equipment. The most common architectures for LANs are the point-to-point, ring, bus, and star/hub-and-spoke architectures, as illustrated in Figure 1-1.

The simplest network topology is a point-to-point architecture, where two computers are connected directly together. In this topology, communication flows only between the two computers. Figure 1-2 shows an example of a LAN configured using the ring topology. This topology is predominantly used by **Token Ring networks**, in which a token (indicated with the letter T in the network diagram) is placed in the data channel and circulates around the ring (hence the

Protocol
A set of rules established for users to exchange information

Topology
The architecture of a network

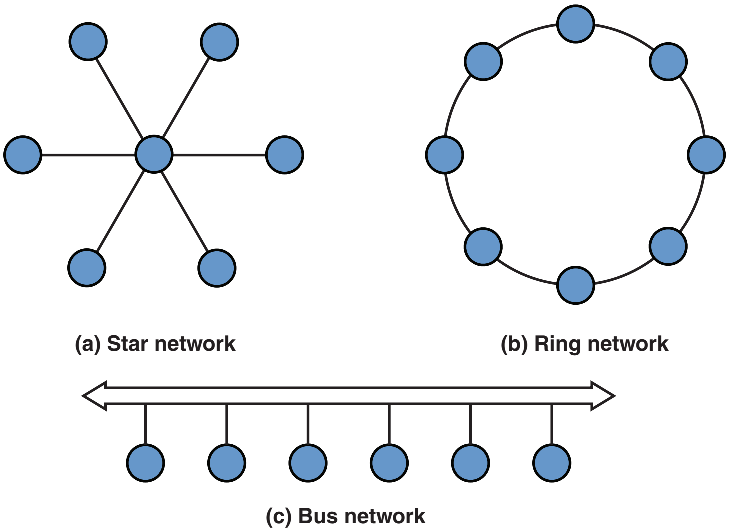
Token Ring Network
A network topology configured in a logical ring that complements the token passing protocol

name *Token Ring*). If a user wants to transmit, the computer waits until it has control of the token. This technique, called **token passing**, is based on the IEEE 802.5 Token Ring Network standard. (**IEEE** is the Institute of Electrical and Electronics Engineers.) A Token Ring network is a **deterministic** network, which means each station connected to the network is ensured access for transmission of its messages at regular or fixed time intervals.

Token Passing
A technique in which an electrical token circulates around a network, and control of the token enables the user to gain access to the network

IEEE
Institute of Electrical and Electronics Engineers, one of the major standards-setting bodies for technological development

Deterministic
A type of network in which access to the network is provided at fixed time intervals


(a) Star network

(b) Ring network

(c) Bus network

FIGURE 1-1 Network topologies. (From *Modern Electronic Communication* 9/e, by G. M. Miller & J. S. Beasley, © 2008 Pearson Education, Inc. Upper Saddle River, NJ.)

One disadvantage of the Token Ring topology is that if an error changes the token pattern, the token may stop circulating. In addition, ring networks rely on each system to relay the data to the next user. A failed station can cause data traffic to cease. Token Ring networks also have disadvantages in terms of troubleshooting and maintenance. In order to remove a device from a Token Ring network or add a device to the network, the Token Ring path must be temporarily broken (that is, the path must be interrupted). This results in downtime for the network. One way to fix this issue is by attaching all the computers to a central **Token Ring hub**, which is a device that manages the passing of the token rather than relying on individual computers to pass it, thereby improving the reliability of the network.

Token Ring Hub
A hub that manages the passing of the token in a Token Ring network

It is important to note that Token Ring has been replaced by Ethernet technology in almost all modern computer networks.

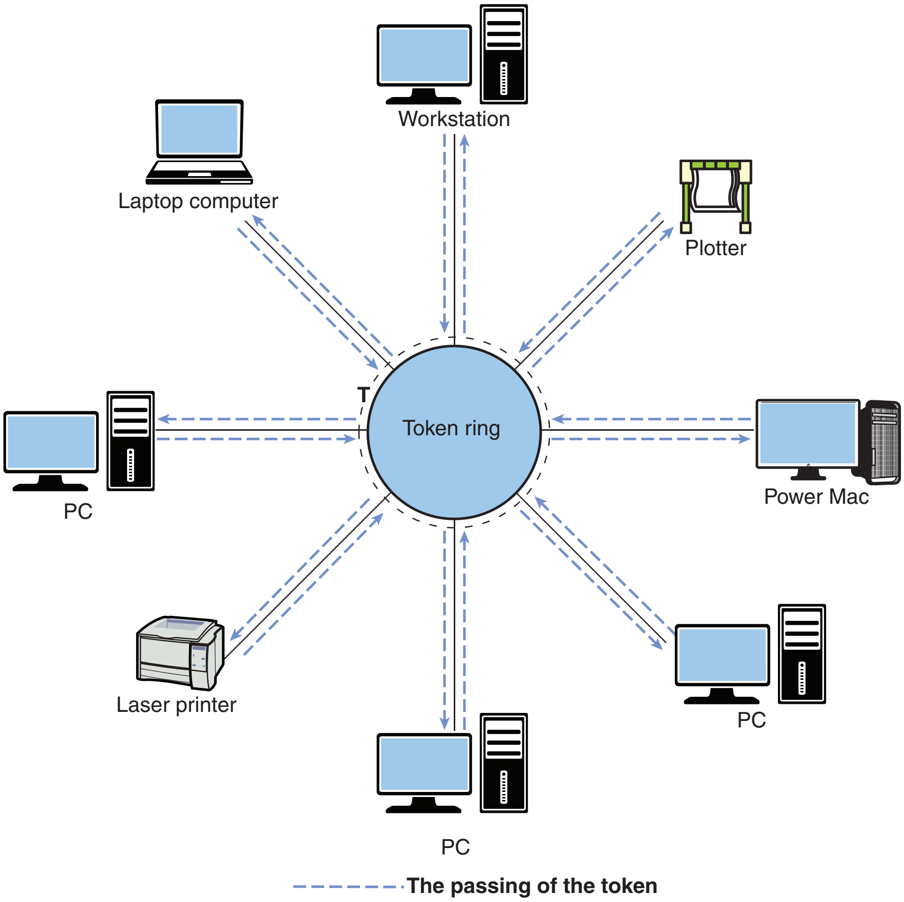


FIGURE 1-2 The Token Ring network topology.

Bus Topology
A system in which the computers share the media (coaxial cable) for data transmission

Figure 1-3 illustrates a **bus topology**, in which the computers share the media (coaxial cable) for data transmission. In this topology, a coaxial cable (called *ThinNet*) is looped through each networking device to facilitate data transfer.

In a bus topology, all LAN data traffic is carried over a common coaxial cable link. In Figure 1-3, for example, if computer 1 is printing a large file, the line of communications is between computer 1 and the printer. However, in a bus system, all networking devices can see computer 1's data traffic to the printer, and the other devices have to wait for pauses in transmission or until transmission is complete before they can initiate their own transmissions. If more than one computer's data is placed on the network at the same time, the data is corrupted and has to be retransmitted. This means that the use of a shared coaxial cable in a bus topology prevents data transmission from being very bandwidth efficient. This is one reason—but not the only reason—bus topologies are seldom used in modern computer networks.

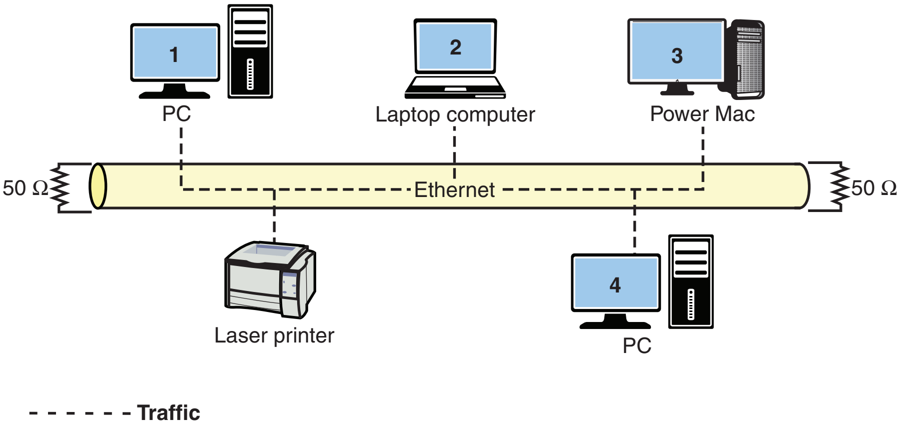


FIGURE 1-3 The bus topology.

The **star topology** (also called hub-and-spoke topology), illustrated in Figure 1-4, is the most common networking topology in today's LANs. Twisted-pair cables with modular plugs are used to connect the computers and other networking devices (see Chapter 2, "Physical Layer Cabling: Twisted-Pair"). At the center of a star network is either a switch or a hub that connects the network devices and facilitates the transfer of data. For example, if computer 1 in Figure 1-4 wants to send data to the network laser printer, the hub or switch provides the network connection. If a hub is used, computer 1's data is sent to the **hub**, which then forwards it to the printer. However, a hub is a **multiport repeater**, which means the data it receives is **broadcast** and seen by all devices connected to its ports. Therefore, the hub broadcasts computer 1's data traffic to all networking devices that are interconnected in the star network. Figure 1-4 shows this data traffic path as solid black arrowed lines going to all networking devices. Much as with the bus topology, all data traffic on the LAN is being seen by all computers. Because a hub broadcasts all data traffic to the devices connected to its network ports, this device is of limited use in a large network.

To minimize unnecessary data traffic and isolate sections of a network, you can use a **switch** at the center of a star network, as shown in Figure 1-4. Each networking device, such as a computer, has a hardware or physical address. (This concept is fully detailed in Section 1-4, "The Ethernet LAN.") A switch stores the hardware or physical address for each device connected to its ports. The storage of the address enables the switch to directly connect two communicating devices without broadcasting the data to all devices connected to its **ports**.

Star Topology
The most common networking topology in today's LANs, where all networking devices connect to a central switch or hub

Hub
A device that broadcasts the data it receives to all devices connected to its ports

Multiport Repeater
Another name for a hub

Broadcast
Transmission of data by a hub to all devices connected to its ports

Switch
A device that forwards a frame it receives directly out the port associated with its destination address

Port
A physical input/output interface to networking hardware