

Networking

Second Edition

Jeffrey S. Beasley

Software Enclosed



Networking, Second Edition

Jeffrey S. Beasley

Many of the designations used by manufacturers and sellers to distinguish their products are claimed as trademarks. Where those designations appear in this book, and the publisher was aware of a trademark claim, the designations have been printed with initial capital letters or in all capitals.

The author and publisher have taken care in the preparation of this book, but make no expressed or implied warranty of any kind and assume no responsibility for errors or omissions. No liability is assumed for incidental or consequential damages in connection with or arising out of the use of the information or programs contained herein.

The publisher offers excellent discounts on this book when ordered in quantity for bulk purchases or special sales, which may include electronic versions and/or custom covers and content particular to your business, training goals, marketing focus, and branding interests. For more information, please contact:

U.S. Corporate and Government Sales
(800) 382-3419
corpsales@pearsontechgroup.com

For sales outside the United States please contact:

International Sales
international@pearson.com

Visit us on the Web: www.informit.com/ph

Library of Congress Cataloging-in-Publication Data

Beasley, Jeffrey S., 1955-

Networking / Jeffrey S. Beasley. — 2nd ed.

p. cm.

ISBN-13: 978-0-13-135838-6 (hardcover w/cd)

ISBN-10: 0-13-135838-3

1. Computer networks—Design and construction. 2. TCP/IP (Computer network protocol) 3. Internetworking (Telecommunication) I. Title.

TK5105.5.B39 2008

004.6—dc22

2008032371

Copyright © 2009 Pearson Education, Inc.

All rights reserved. Printed in the United States of America. This publication is protected by copyright, and permission must be obtained from the publisher prior to any prohibited reproduction, storage in a retrieval system, or transmission in any form or by any means, electronic, mechanical, photocopying, recording, or likewise. For information regarding permissions, write to:

Pearson Education, Inc
Rights and Contracts Department
501 Boylston Street, Suite 900
Boston, MA 02116
Fax (617) 671 3447

ISBN-13: 978-0-13-135838-6

ISBN-10: 0-13-135838-3

Text printed in the United States at Edwards Brothers in Ann Arbor, Michigan.

First printing August 2008

Associate Publisher

David Dusthimer

Senior Development Editor

Christopher Cleveland

Managing Editor

Patrick Kanouse

Senior Project Editor

Tonya Simpson

Copy Editor

Language Logistics, LLC

Indexer

Heather McNeil

Proofreader

Arle Writing and Editing

Technical Reviewers

Dan Bosch, Tami Day-Orsatti,
Jim Geier, Randy Ivener,
Steve McQuerry,
Shawn Merdinger,
Piyasat Nilkaew, Matt Peralta,
Allan Reid, Holly Ricketts,
Able Sanchez, Lee Shombert,
Toby Skandier, Randy Zhang

Publishing Coordinator

Vanessa Evans

Multimedia Developer

Dan Scherf

Preface

This book provides a comprehensive look at computer networking from the point of view of the network administrator. It guides readers from an entry-level knowledge in computer networks to advanced concepts in 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, the network server, Linux networking, and industrial networks. After covering the entire text, readers will have gained a solid knowledge base in computer networks.

In my years of teaching, I 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. Show the students the technology, how it is used, and why, and they will take the applications of the technology to the next level. Allowing them to experiment with the technology helps them to develop a greater understanding. This book does just that.

ORGANIZATION OF THE TEXT

This text is designed to cover two semesters. The recommended chapters for the first semester are Chapters 1 to 8. Throughout the semester, the students will gain an appreciation of how basic computer networks and related hardware are interconnected to form a network. This involves understanding the concepts and issues of twisted-pair cable, interconnecting LANs, configuring TCP/IP, subnet masking, basic router configuration, and configuring routing protocols and wide area networking.

Chapters 9 to 16 are recommended for the second semester—configuring and managing the campus network, network security, wireless LANs, and optical networks. The instructor can choose from the following topics to complete the semester: installing and configuring Windows 2008/2003 network server, Voice over IP, Linux configuration, and industrial networks.

Key Pedagogical Features

- *Chapter Outline, Objectives, Key Terms, and Introduction* at the beginning of each chapter clearly outline specific goals for the reader. An example of these features is shown in Figure P-1.

Chapter Outline

CHAPTER OUTLINE

8-1 Introduction
8-2 The Line Connection
8-3 Frame Relay
8-4 ATM
8-5 Dial-in Access
8-6 VPN

OBJECTIVES

- Describe line coding and framing format
- Describe the function of the CSU/DSU
- Describe how to create a frame relay connection
- Demonstrate the configuration for a point-to-point connection
- Discuss the ATM role of operation
- Describe a wide area network
- Describe how to configure dial-in access on a Windows 2003/2000 Server
- Describe how to configure a VPN tunnel
- Describe the different types of WAN connections
- Describe the steps for configuring Internet routing

KEY TERMS

wide area network (WAN)	X.25	XDSL
HDSL	committed information rate (CIR)	DSL
CSU/DSU	burst	ADSL (asymmetric DSL)
DS0-DS3, T1-T3	committed burst information rate (CBIR)	RIS
DS	micro cloud	DCEP
micro cloud	PIG	VPN
fractional T1	frame relay cloud	IP tunnel
switch-to-switch	cloud tag	PPP
point of presence (POP)	AVL	L2TP
line of demarcation	packet switching	stubby areas
CSU/DSU	payload	totally stubby areas
DSU framing	virtual path connection (VPC)	BGP
AVL	virtual channel connection (VCC)	multihomed
bipolar coding	AS	ASN
BIS	AS	peering
minimum ones density	VPI	EIGRP
bipolar violation	VCI	IGRP
HFC	LAN/L3/L4	NCC
PPP	V62/V60	collocated data traffic
frame relay network	asynchronous operation	collocated data traffic
public data network	callback modem	collocated data traffic
	trunking	IPX
	ISDN	

Chapter Objectives

8-1 INTRODUCTION

Wide Area Network (WAN)
uses the telecommunication network to interconnect sites that are geographically distributed throughout a region, the country, or even the world. Connections can include extensions of the campus LAN to remote members of the network. For example, the corporate office for a company could be located in one part of a state and the engineering, manufacturing, and sales sites could be at different locations in the state. An example of a WAN is shown in Fig. 8-1. The wide area network in this example shows connections for the Internet, a frame relay network, a VPN network, and dial-in access through a remote access server.

This chapter examines each of these wide area networking technologies. An introduction to setting up a connection to the communications carrier is examined in section 8-2. The CSU/DSU, serial line clocking, and line coding formats are examined. The important concept of configuring frame relay networks is next examined in section 8-3. This section includes an example of configuring a frame relay network within a simulated Teles "cloud."

Section 8-4 examines the asynchronous transfer mode (ATM) and its important role in carrying high-speed data traffic around the country and the world. Wide area networking is not complete without dial-in access for the user. Section 8-5 examines establishing a point-to-point dial-in connection using a phone modem, cable modem,

FIGURE 8-1 An example of a wide area network.

233

234 Chapter 8 • Wide Area Networking

Key Terms for this chapter

FIGURE P-1

- *Net-Challenge Software* provides a simulated, hands-on experience in configuring routers. Exercises provided in the text (see Figure P-2) and on the CD challenge readers to undertake certain router/network configuration tasks. The challenges check the students' ability to enter basic networking commands and to set up router function, such as configuring the interface (Ethernet and Serial) and routing protocols (that is, OSPF, BGP, EIGRP, IGRP, RIP, and static). The software has the look and feel of actually being connected to the router's console port.
- *Protocol Analyzer Software* packaged with the text uses the Finisar Surveyor Demo. Examples of using the software to analyze data traffic are included throughout the text, as shown in Figure P-3.
- *Numerous worked-out examples* are included in every chapter to reinforce key concepts and aid in subject mastery, as shown in Figure P-3.



The Cisco 4300 series cable access router. (Courtesy of Cisco Systems)

A command used for displaying only the OSPF routes is `sh ip route ospf`. The results for this command from RouterA are shown:

```

RouterA#sh ip route ospf
 10.0.0.0/24 is subnetted, 6 subnets
 O   10.10.5.0 [110/74] via 10.10.100.2, 00:10:03, Ethernet2
 O   10.10.10.0 [110/74] via 10.10.200.2, 00:10:03, Ethernet1
 O   10.10.150.0 [110/128] via 10.10.200.2, 00:10:03, Ethernet1
    [110/128] via 10.10.100.2, 00:10:03, Ethernet2
  
```

Another command used for displaying protocol information for the router is `sh ip protocol`. The results for entering this command for RouterA are shown:

```

RouterA#sh ip protocol
Routing Protocol is "ospf 100"
  Sending updates every 9 seconds
  Invalid after 0 seconds, hold down 0, flushed after 0
  Outgoing update filter list for all interfaces is
  Incoming update filter list for all interfaces is
  Redistributing: ospf 100
  Routing for Networks:
    10.10.200.250/32
    10.10.100.1/32
    10.10.200.1/32
  Routing Information Sources:
    Gateway         Distance      Last Update
  10.10.100.1       110           00:06:01
  10.10.200.2       110           00:06:01
  Distance: (default is 110)
  
```

Net-Challenges are found throughout the text

Network Challenge—OSPF

Use the Net Challenge simulator software included with the text's Companion CD-ROM to demonstrate that you can configure OSPF for Routers in the campus LAN (the campus LAN is shown in Fig. 7-12 and is displayed on the computer screen once the software is started). Make sure that you have configured your computer's display to meet the 800 × 600 pixel display resolution requirement. Place the Net-Challenge

CD-ROM in your computer's drive. Open the **Net-Challenge** folder, click on **Net-Challenge.exe**. Once the software is running, click on the **Select Router Challenge** button. This opens a **Select Router Challenge** drop-down menu. Select **Chapter 7—OSPF**. This opens a check box that can be used to verify that you have completed all of the tasks.

1. Enter the privileged EXEC mode on the router.
2. Enter the router's terminal configuration mode, `Router(config)#`.
3. Set the hostname to `RouterA`.
4. Configure the Ethernet0 interface with the following:
 - IP address 10.10.20.250
 - Subnet mask 255.255.255.0
5. Enable the E0 interface.
6. Configure the Ethernet1 interface with the following:
 - IP address 10.10.20.250
 - Subnet mask 255.255.255.0
7. Enable the E1 interface.
8. Configure the Ethernet2 interface with the following:
 - IP address 10.10.100.1
 - Subnet mask 255.255.255.0
9. Enable the E2 interface.
10. Enable OSPF with a network number of 100.
11. Use a single command line instruction to configure RouterA to run OSPF on all three of the Ethernet interfaces (see task 100).
12. Use the `sh ip int brief` command to check the interface status.
13. Use the `sh ip protocol` command to see if OSPF is running on RouterA.
14. Use the `sh ip route` command to verify that the three Ethernet ports are connected to RouterA.
15. Use the `sh run` command to view the running-configuration file on RouterA. Verify that OSPF is enabled and the proper network address is specified.

7-7 EIGRP—ENHANCED INTERIOR GATEWAY ROUTING PROTOCOL

This section introduces techniques for configuring a router's interface to run EIGRP, the Enhanced Interior Gateway Routing Protocol. EIGRP is an enhanced version of the Interior Gateway Routing Protocol (IGRP). EIGRP is a Cisco proprietary link-state protocol. EIGRP calculates route metrics in a similar way as IGRP but uses a technique to improve the detail on metrics.

EIGRP allows the use of variable-length subnet masks, which is beneficial when trying to conserve the uses of IP addresses. EIGRP also uses "Hello" packets to verify that a link from one router to another is still active. This is similar to the OSPF "Hello" packet described in section 7-6. The routing table updates are exchanged when there is a change in the network. In other words, the routers don't exchange unnecessary information unless a route changes. This helps conserve the limited bandwidth of the network data link. When route information is exchanged, EIGRP quickly converges to the new route selection.

214 Chapter 7 • Routing Protocols Section 7-7 • EIGRP—Enhanced Interior Gateway Routing Protocol 215

Exercises challenge readers to undertake certain tasks

FIGURE P-2



FIGURE P-2 The setup for the capture of the TCP connections.

FIGURE P-3 An example of the three packets exchanged in the initial TCP handshake.

in packet 1 ($x + 1$). Remember, Host A and Host B each have their own sequence numbers. This completes the three-packet handshake that establishes the TCP connection. This handshake appears at the beginning of all TCP data transfers.

The following is an example of a TCP packet transmission captured using the Surveyor Demo protocol analyzer software provided on the text's Companion CD-ROM. The network setup is shown in Fig. 5-4. Host A (the client) is establishing an FTP connection with Host B. The captured file is `5-5.cap` and is also provided on the CD-ROM in the **Capture** folder. Portions of the captured data packets are shown in Fig. 5-5.

Packet 1 (ID 000001) is the SYN or synchronizing packet. This packet is sent from the host computer on the network that wants to establish a TCP network connection. In this example, Host A is making a TCP connection for an FTP file transfer. The summary information for packet 1 specifies that this is a TCP packet, the source port is 1054 (SP = 1054), and the destination port is 21 (DP = 21). Port 1054 is an arbitrary port number that the FTP client picks or is assigned by the operating system. The destination port 21 is the well-known FTP port (see Table 5-3). The packet has a starting sequence number, 997462768, and there is no acknowledgement (ACK = 0). The length of the data packet is 0 (LEN = 0). This indicates that the packet does not contain any data. The window size = 16384 (WS = 16384). The `window size` indicates how many data packets can be transferred without an acknowledgement.

Packet 2 is the SYN-ACK packet from the FTP server. The sequence number SEQ = 3909625466 is the start of a new sequence for the data packet transfers from Host B. The source port is 21 (SP = 21) and the destination port for packet 2 is 1054 (DP = 1054). ACK = 997462769 is an acknowledgement by host B (the FTP server) that the first TCP transmission was received. Note that this acknowledgement shows an increment of 1 from the starting sequence number provided by host A in packet 1.

Packet 3 is an acknowledgement from the client (host A) back to the FTP server (host B) that packet 2 was received. Note that the acknowledgement is ACK = 3909625467, which is an increment of 1 from the SEQ number transmitted in packet 2. This completes the initial handshake establishing the TCP connection. The next part is the data packet transfer. At this point, the two hosts can begin transferring data packets.

The last part of the TCP connection is terminating the session for each host. The first thing that happens is a host sends a FIN (finish) packet to the other connected host. This is shown in Fig. 5-6. Host B sends a FIN packet to Host A indicating the

1. Divide the decimal number by 2, record the remainder of 0 or 1 and write the quotient or result of the division by 2.
2. Divide the quotient by 2 and record the remainder of 0 or 1. Write the quotient and repeat this step until the quotient is 0.
3. Write the remainder numbers (0 and 1) in reverse order to obtain the binary equivalent value.

Example 5-2

Convert the decimal number 12 to binary.

Solution:

Divide 12 by 2. This equals 6 with a remainder of 0. Divide 6 by 2. This equals 3 with a remainder of 0. Divide 3 by 2. This equals 1 with a remainder of 1. Divide 1 by 2. This equals 0 with a remainder of 1. The quotient is 0; therefore the conversion is done. Write the remainder numbers in reverse order to generate the binary equivalent value. This yields a value of 1100. The calculation for this is shown:

$$\begin{array}{r} 12 \div 2 = 6 \text{ R } 0 \\ 6 \div 2 = 3 \text{ R } 0 \\ 3 \div 2 = 1 \text{ R } 1 \\ 1 \div 2 = 0 \text{ R } 1 \end{array}$$

You can verify the answer by converting the binary number back to decimal.

$$\begin{array}{r} 8 & 4 & 2 & 1 \\ 1 & 1 & 0 & 0 \\ (1 \times 8) + (1 \times 4) = 12 \end{array}$$

Example 5-3

Convert 33 to its binary equivalent.

Solution:

Use the decimal-to-binary steps listed previously.

$$\begin{array}{r} 33 \div 2 = 16 \text{ R } 1 \\ 16 \div 2 = 8 \text{ R } 0 \\ 8 \div 2 = 4 \text{ R } 0 \\ 4 \div 2 = 2 \text{ R } 0 \\ 2 \div 2 = 1 \text{ R } 0 \\ 1 \div 2 = 0 \text{ R } 1 \end{array}$$

The answer is 100001.

118 Chapter 5 • TCP/IP Section 5-3 • Number Conversion 125

Numerous worked-out examples aid in subject mastery

FIGURE P-3

- *Configuring, Analyzing, or Troubleshooting* sections, as shown in Figure P-4, are included with each chapter to guide the reader through advanced techniques in networking.

Screen captures guide students through the different hands-on exercises

FIGURE P-4-10 The window displaying a summary of the server options selected.

FIGURE P-4-16 The window confirming the installation of the salsa active directory.

FIGURE P-4-17 Restarting Windows to activate the changes made to the Active Directory.

Configuring Windows 2003 Server
The steps for configuring the 2003 server vary depending on the current status of the operating system installed on the server. This section assumes that the current operating system is Windows 2000 server.

Configuring, analyzing, and troubleshooting sections guide readers through advanced techniques in networking

Configuring the IP Address
The next step is to configure the IP address for the network server. The network administrator typically selects the IP address. Make sure that you have a confirmed IP address prior to placing the server on the network. If two computers connected to the network have an IP address conflict, neither computer will function properly on the network.
First, right click on **My Network Places > Properties** > right mouse click on **Local Area Connection > Properties**, or (Windows 2000 Server) click on **Start > Settings > Network and Dialup Connections** > right click on **Local Area Connection > Properties**.
(Windows 2003 Server) click on **Start — Control Panel — Network Connections —** right mouse click on **Local Area Connection — Properties**.
At this point you should be placed in the **Local Area Connection Properties** menu as shown in Fig. 14-18. Double click on **Internet Protocol TCP/IP**. This places you in the **Internet Protocol (TCP/IP) Properties** menu shown in Fig. 14-19.
Click on **Use the following IP address** and set the address specified for your network. In this example, the private IP address 10.10.10.4 has been selected and a subnet mask of 255.0.0.0 is being used. The other option, **Obtain an IP address automatically**, is used when the IP addresses are assigned dynamically and when a dynamic host control (DHCP) server is used. Click **OK** once this step is complete.
At this point you want to verify that the computer has accepted the requested IP address change, which you do by entering the command prompt in the Start menu. Click **Start > Run**, enter command, and at the command prompt enter `ipconfig`, then hit **Return** or **Enter**. The new IP address 10.10.10.4 for the computer should be listed.

To install the 2003 server, click on **start > programs > administrative tools > Configure Your Server Wizard**. This will open a “Welcome to the Configure Your Server” menu. Click “Next” to begin. You will be prompted with a menu asking you to verify that you have completed some preliminary setup steps. Review the setup and click on **Next** when done. This opens the **Server Role** menu. This menu allows you to select the services desired (e.g., file server, print server, mail server, etc.). For the basic setup, select **file server** and click on **next**.
If you are upgrading a Windows 2000 server to 2003, you will be advised that there are some compatibility issues between 2000 and 2003 server. You will be directed to exit the configurations wizard and start the **command prompt**. You will be instructed to enter the **386** directory on the installation CD-ROM. Enter the command
`adprep/forest prep`
`c <enter>`
Next, while still in the 386 directory on the installation CD-ROM enter
`adprep/domain prep`
After completing these steps, restart to **Configure Your Server Wizard**. The remaining steps for the 2003 server installation will be fairly automatic and you will see a limited number of menus. The two adprep commands upgraded the 2000 server active directory so that it is now compatible with Windows 2003 Server. The 2003 server should now be running the Windows 2000 “salsa” domain configuration.

Section 14-2 • Installing and Configuring the Network Server 439

440 Chapter 14 • The Network Server

FIGURE P-4

- *Key Terms* and their definitions are highlighted in the margins to foster inquisitiveness and ensure retention. This is illustrated in Figure P-5.
- *Extensive Summaries, Questions, and Problems* as well as *Critical Thinking Questions* are found at the end of each chapter, as shown in Figure P-6.

Illustrations and photos enhance the text

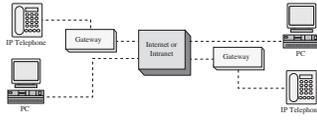


FIGURE P-5 The various ways of placing voice over IP telephone calls.



A Cisco Voice over IP system. (Courtesy of Cisco Systems.)

RTP
Real-time Protocol

The frames are then placed into a packet. An **RTP** (Real-time Protocol) header is added to each frame. The RTP header provides the following:

- Packet sequence number
- Timestamp

RTCP
Real-time Control Protocol

A companion protocol to RTP is **RTCP**, the Real-time Control Protocol. The purpose of RTCP is to manage packet synchronization and identification and the transport of the data.

Packet Sequence Number
used to keep track of the order of the data packets

The **packet sequence number** is used to keep track of the order of the data packets and to detect any lost packets. RTP uses UDP for transporting the data. There is always a chance that packets could be lost in a congested network, or the packets could arrive out of order. The RTP packet sequence number enables a processor to reassemble the data packets. Lost digital voice data packets will cause annoying pops and clicks when converted back to analog at the receiver. One technique is to fill in

8-9 ANALYZING INTERNET DATA TRAFFIC

A campus network operations center (NOC) receives many emails and calls about suspected problems with the network. Many times network problems are due to operational errors by the users and possible hacker attacks. On occasion, network equipment failure can be causing the problem. The bottom line is that the network administrator must have some expected performance measure of the network. The administrator will want to know the expected normal usage of the network, what type(s) of normal data traffic is expected, what is typical of "outbound" and "inbound" Internet data traffic, and who are the "big" data users on the network. **Outbound data traffic** is data leaving the network, and **inbound data traffic** is data entering the network. This section provides an overview of the Internet data traffic patterns a NOC might monitor. These patterns are only examples of data traffic activity for a network. Data traffic patterns will vary significantly for each network and each network will have its own typical data traffic. Also, data traffic will change during the day. Examples of this are presented in Chapter 9 in section 9-6, Analyzing Campus Network Data Traffic. The data traffic images shown in this section were captured using the Finisar-Shomiti Portable Surveyor.

The first capture, shown in Fig. 8-57, is a composite view of the data traffic activity for an Internet connection to and from a campus network. The image has four screens showing various data traffic information. This screen setup might be typical of the screen display at a network monitoring center. This does not imply that someone watches the screen continually but the screen is looked at when a possible data traffic problem is mentioned.

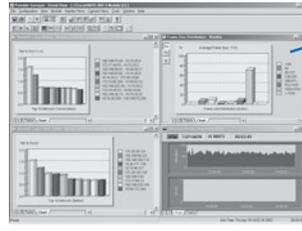


FIGURE 8-57 A composite view of network data traffic activity.

NOC
network operations center

Key Terms are defined in the margin

Outbound Data Traffic
data traffic leaving the network
Inbound Data Traffic
data traffic entering the network

Screen captures aid student understanding

FIGURE P-5

Summary of key concepts

Summary

This chapter has presented an overview of the fundamentals of the TCP/IP protocol suite. TCP/IP is well established and carries the data traffic over the Internet. The student should understand the following:

- The layers of TCP/IP and their relationship to the OSI layers
- The basic structure of a 32-bit IPv4 address
- How to subnet a network
- How to apply subnet masks in networks
- The purpose of CIDR blocks and supernetting
- The data structure of an IPv6 hexadecimal address
- How to examine TCP/IP data packets with the Finisar Surveyor Demo Protocol Analyzer

Questions and Problems

Section 5-2

1. What are the four layers of the TCP/IP model?
2. Which layer of the TCP/IP model processes requests from hosts to make sure a connection is made to the appropriate port?
3. What are *well-known ports*?
4. Identify the port numbers for the following applications.
 - a. Telnet
 - b. HTTP
 - c. FTP
 - d. DNS
 - e. DHCP
5. Define the purpose of a *connection-oriented protocol*. Give an example.
6. What three packets are exchanged between two hosts when establishing a TCP connection?
7. What is the purpose of a sequence number (SEQ=) in TCP data packets?
8. Explain how a host knows if a data packet was not received.
9. Describe how a TCP connection is terminated.
10. What is a *connectionless protocol*? Give an example.
11. What is the purpose of the Internet layer in the TCP/IP protocol suite?
12. What is the purpose of an ARP request?
13. What is the purpose of an ARP reply?
14. What important networking-troubleshooting tool is part of ICMP and how does it test a network connection?
15. When is IGMP used?
16. The network interface layer of the TCP/IP model defines how the host connects to what network?

Section 5-3

17. Convert the following 8-bit binary number to decimal: 10010011
18. Convert the following octet to decimal: 11000000
19. Convert the following 8-bit number to decimal: 11111100
20. Convert the following binary number to decimal: 11111111

47. How is a network address of 192.168.6.0 and a subnet mask of 255.255.254.0 written in CIDR?
48. A CIDR block contains the following subnets with IP addresses of
 - a. 192.168.69.0/22
 - b. 192.168.69.0/22
 - c. 192.168.70.0/22
 - d. 192.168.71.0/22
 Are there any problems with this group of subnets in the CIDR block? Show your work.

Section 5-7

49. How many bits are in an IPv6 address?
50. IPv6 numbers are written in what format?
51. Express the following IPv6 numbers using double-colon notation:
 - a. 5355:4821:0000:0000:0000:1234:5678:FEDC
 - b. 0000:0000:0000:1234:5678:FEDC:BA98:7654
 - c. 1234:5678:ABCD:EF 12:0000:0000:1122:3344
52. Express the IPv4 IP address 192.168.12.5 in IPv6 form using dotted decimal.
53. Recover the IPv6 address from the following double-colon notation: 1234:5678::AFBC

Section 5-8

54. What are the server port numbers for an FTP transfer?
55. How does a client notify a server that an ASCII data transfer is requested?

Critical Thinking

56. Your boss has read about IPv6 and wants to know if the network you is ready for the transition. Prepare a response based on the network computer operating systems used in your facility.
57. Use the Surveyor Demo protocol analyzer software to capture the start session in your network. Identify the packets that are part of the initial handshake.

Surveyor IP Problems

- The following questions use the *chapter 5-hwcap* file on the Net-Chat ROM.
58. What routing protocols are used in this network?
 59. In the FTP exchange, what operating system is the server running?
 60. What is the destination address for the FTP server?
 61. What is the source address for the FTP transfer?
 62. What is the username sent to the FTP server?
 63. What is the password sent to the FTP server?
 64. What is the name of the file sent over FTP?
 65. What are the contents of the file?
 66. From Packet ID# 7, what is the FTP server requesting from the host?

Critical Thinking questions and problems further develop analytical skills

FIGURE P-6

- An extensive *Glossary* is found at the end of the book and offers quick, accessible definitions to key terms and acronyms, as well as an exhaustive *Index* (Figure P-7).

Complete Glossary of terms and acronyms provide quick reference

Exhaustive Index provides quick reference

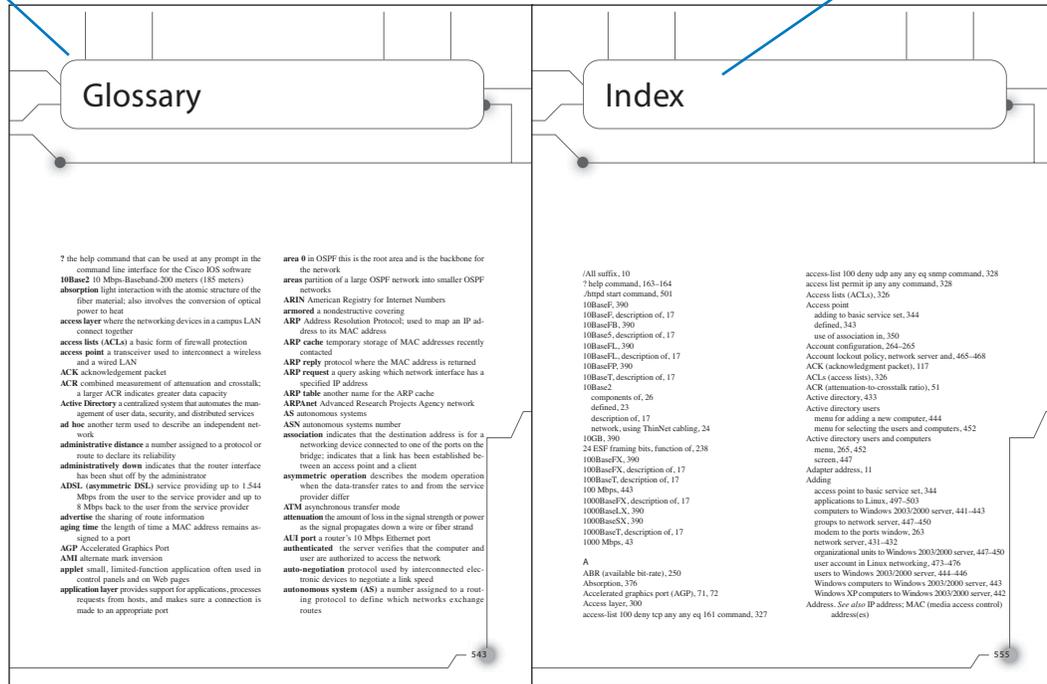


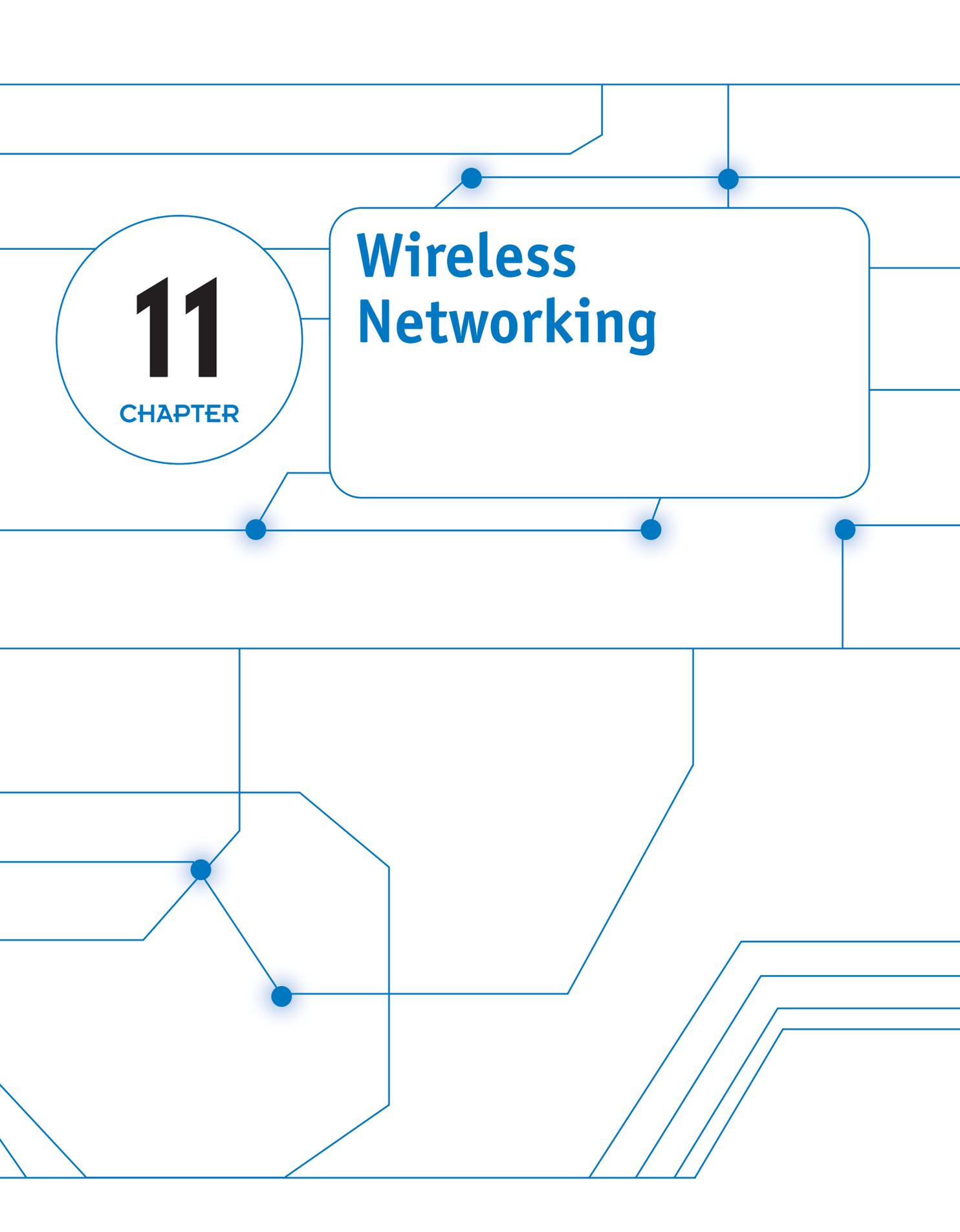
FIGURE P-7

Accompanying CD-ROM

The CD-ROM packaged with the text includes the Finisar Surveyor Demo software and captured data traffic used in the text. This software provides readers with the opportunity to capture data traffic on their own network. It also includes the Net-Challenge Software, which was developed specifically for this text.

Instructor Resources

The Instructor's Manual to accompany *Networking, Second Edition* (ISBN 0-13-135838-3) provides the entire book in PDF format along with instructor notes for each section within each chapter, recommending key concepts that should be covered in each chapter. Solutions to all chapter Questions and Problems sections are also included. In addition, the instructor will find a separate Solutions to the Net-Challenges Instructor's Edition PDF as well as a 18 laboratory exercises. Also a test bank with which to generate quizzes on the material found within the student edition of the book is provided.



11

CHAPTER

Wireless Networking

CHAPTER OUTLINE

- 11-1 Introduction
 - 11-2 The IEEE 802.11 Wireless LAN Standard
 - 11-3 802.11 Wireless Networking
 - 11-4 Bluetooth, WiMAX, and RFID
 - 11-5 Securing Wireless LANs
 - 11-6 Configuring a Point-to-Multipoint Wireless LAN: A Case Study
- Summary
Questions and Problems

OBJECTIVES

- Define the features of the 802.11 wireless LAN standard
- Understand the components of the 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	pseudorandom	WiMAX
Basic Service Set (BSS)	hopping sequence	BWA
ad hoc	OFDM	NLOS
access point	U-NII	last mile
transceiver	MIMO	Radio Frequency Identification (RFID)
Extended Service Set (ESS)	Wi-Fi	backscatter
hand-off	SSID	Slotted Aloha
roaming	site survey	beacon
CSMA/CA	inquiry procedure	WPA
DSSS	paging procedure	EAP
ISM	piconet	RADIUS
FHSS	pairing	
	Passkey	

WLAN

Wireless local area network

11-1 INTRODUCTION

This chapter examines the features and technologies used in the wireless local area network (**WLAN**). Wireless networking is an extension of computer networks into the RF (radio frequency) world. The 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 the 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.

This chapter addresses the basic issues of incorporating WLAN technologies into a network. The fundamentals of the IEEE 802.11 wireless LAN standard are examined in section 11-2. This includes an overview of wireless LAN concepts and terminology, frequency allocations, and spread spectrum communication. The applications of wireless LANs are presented in section 11-3. This includes a look at different types of wireless LAN configurations, such as point-to-point and point-to-multipoint. Other wireless networking technologies are examined in section 11-4. This section looks at Bluetooth, WiMAX, and RFID. Anytime 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 new security issues. Section 11-5 examines the basic issues of securing WLAN communications. The last section (11-6) presents an example of configuring a wireless LAN to provide access for users in a metropolitan area.

11-2 THE IEEE 802.11 WIRELESS LAN STANDARD

A typical computer network uses twisted-pair and fiber optic cable to interconnect LANs. Another media competing for use in higher data-rate LANs is wireless, based on the IEEE 802.11 wireless standard. The advantages of wireless include

- User mobility in the workplace
- A cost-effective networking media for use in areas that are difficult or too costly to wire

The concept of user mobility in the workplace opens the door to many opportunities to provide more flexibility. Workers can potentially access the network or their telephones (via IP telephony) from virtually any location within the workplace. Accessing information from the network is as easy as if the information were on a disk.

The benefits of wireless networks in the workplace are numerous. To provide wireless connectivity, the network administrator must be sure the network services are reliable and secure. Providing reliable network services means the administrator must have a good understanding of wireless LAN 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, and 802.11g and 802.11n; and how WLANs are configured.

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

The PHY (physical) layer defines

- The method of transmitting the data, which may be either RF or infrared (although infrared is rarely used)

The MAC (media access control) layer defines

- The reliability of the data service
- Access control to the shared wireless medium
- Protecting the privacy of the transmitted data

The wireless management protocols and services are

- Authentication, association, data delivery, and privacy

The fundamental topology of the WLAN is the **Basic Service Set (BSS)**. This is also called the independent Basic Service Set, or **ad hoc** network. An example of an ad hoc network is provided in Figure 11-1. 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.

Basic Service Set (BSS)

Term used to describe an independent network

Ad Hoc

Another term used to describe an independent network

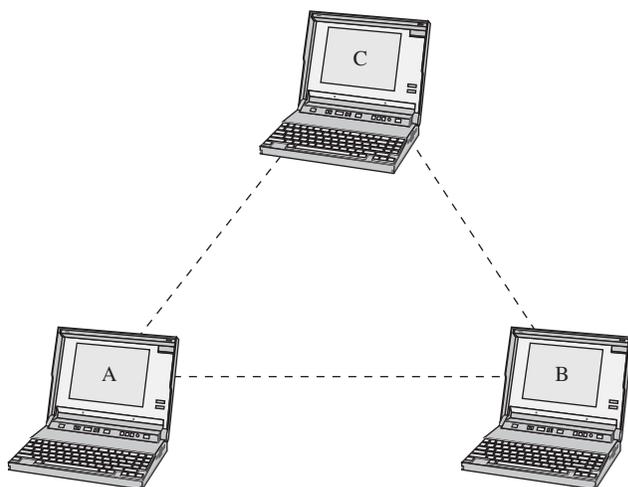


FIGURE 11-1 An example of the independent Basic Service Set or “ad hoc” network.

The performance of the Basic Service Set can be improved by including an **access point**. The access point is a transmit/receive unit (**transceiver**) that interconnects data from the wireless LAN to the wired network. Additionally, 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 11-2.

Access Point

A transceiver used to interconnect a wireless and a wired LAN

Transceiver

A transmit/receive unit

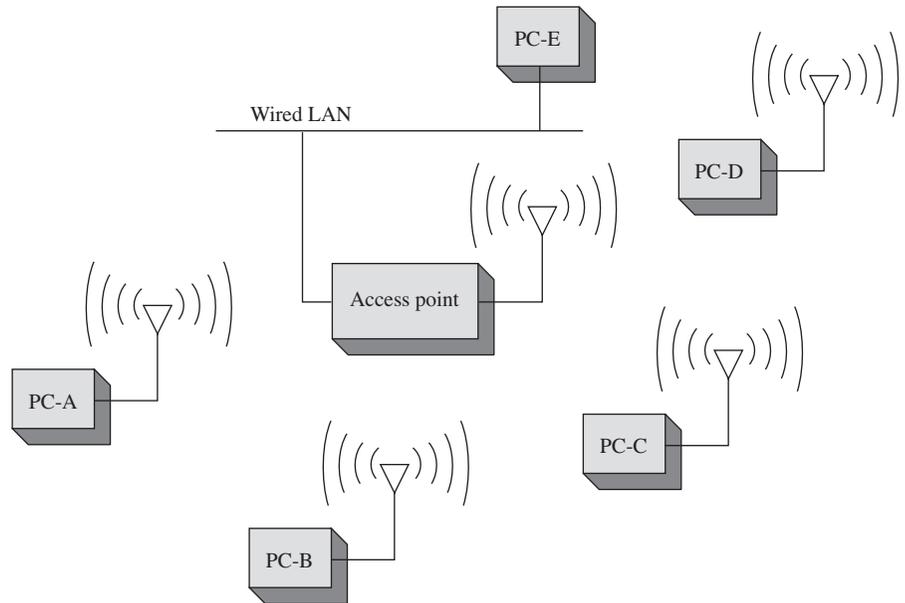


FIGURE 11-2 Adding an access point to the Basic Service Set.

If data is being sent from PC-A to PC-D, 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. 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 will first pass through the access point and then to PC-E in the wired LAN.

The problem with the Basic Service Set is that mobile users can travel outside the radio range of a station's wireless link with 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)**. An example is provided in Figure 11-3. The mobile computer will establish an authorized connection with the access point that has the strongest signal level (for example, AP-1). As the user moves, the signal strength of the signal from AP-1 will decrease. At some point, the signal strength from AP-2 will exceed AP-1, and the wireless bridge will establish a new connection with AP-2. This is called a **hand-off**. This 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/collision avoidance (CSMA/CA). In **CSMA/CA**, the client station listens for other users of the wireless network. If the channel is quiet (no data transmission), the client station may 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. There are currently four physical layer technologies being used in 802.11 wireless networking. These are 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

Extended Service Set (ESS)

The use of multiple access points to extend user mobility

Hand-off

When the user's computer establishes an association with another access point

Roaming

The term used to describe a users' ability to maintain network connectivity as they move through the workplace

CSMA/CA

Carrier sense multiple access/collision avoidance

OFDM is used in 802.11a, 802.11g, and 802.11n. Note that 802.11g/n use both DSSS and OFDM modulation.

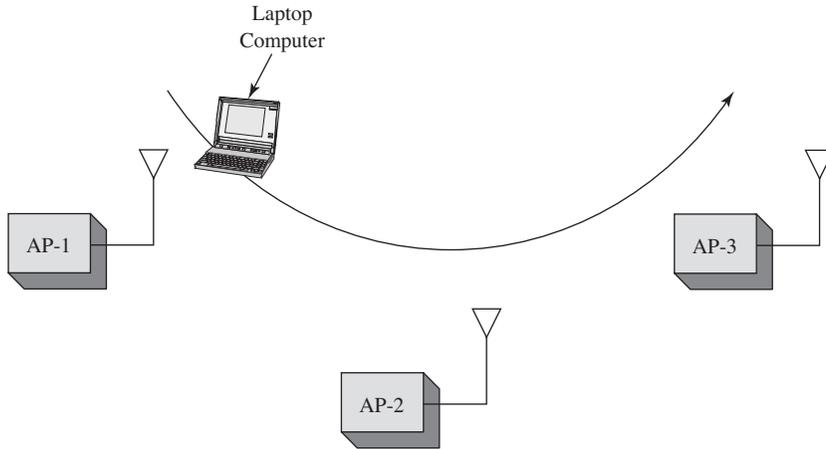


FIGURE 11-3 An example of an Extended Service Set used for increased user mobility.

802.11 **DSSS** implements 14 channels (each consuming 22 MHz) over approximately 90 MHz of RF spectrum in the 2.4 GHz **ISM** (industrial, scientific, and medical) band. The frequency channels used in North America are listed in Table 11-1. An example of the frequency spectrum for three-channel DSSS is shown in Figure 11-4.

DSSS

Direct sequence spread spectrum

ISM

Industrial, scientific, and medical

TABLE 11-1 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

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 1 MHz wide) in the ISM 2.4 GHz 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 1 and 2 Mbps. 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.

FHSS

Frequency hopping spread spectrum

Pseudorandom

The number sequence appears random but actually repeats

Hopping Sequence

The order of frequency changes

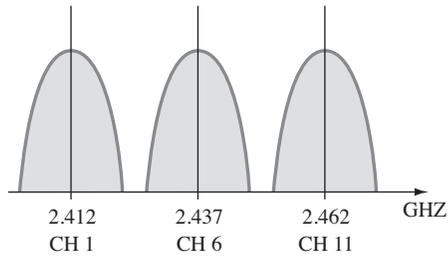


FIGURE 11-4 An example of the three channels in the DSSS spectrum.

The maximum transmit power of 802.11b wireless devices is 1000 mW; however, the nominal transmit power level is 100 mW. The 2.4 GHz 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 2.4 GHz 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 5 GHz range and provides significant improvement over 802.11b with respect to RF interference.

The 802.11a standard uses a technique called orthogonal frequency division multiplexing (**OFDM**) to transport the data over 12 possible channels in the **U-NII** (Unlicensed National Information Infrastructure). U-NII was set aside by the FCC to support short-range, high-speed wireless data communications. Table 11-2 lists the operating frequencies for 802.11a. Table 11-3 lists the transmit power levels for 802.11a.

OFDM

Orthogonal frequency division multiplexing

U-NII

Unlicensed National Information Infrastructure

TABLE 11-2 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	
149	5.745	
153	5.765	Upper Band
157	5.785	
161	5.805	

TABLE 11-3 Maximum Transmit Power Levels for 802.11a with a 6dBi Antenna Gain

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

IEEE 802.11a equipment is not compatible with 802.11b, 802.11g, or 802.11n. The good aspect of this is that 802.11a equipment will not interfere with 802.11b, g, or n; therefore, 802.11a and 802.11b/g/n links can run next to each other without causing any interference. Figure 11-5 illustrates an example of the two links operating together.

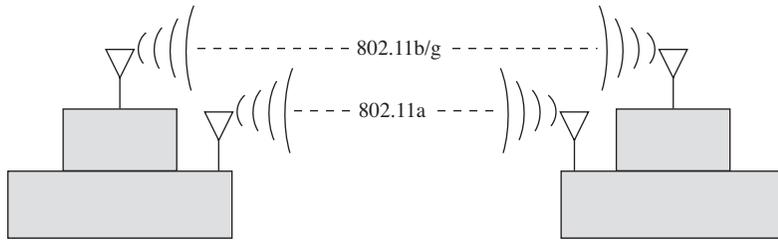


FIGURE 11-5 An example of an 802.11a installation and an 802.11b link running alongside each other.

The downside of 802.11a is 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 or even greater than that of 802.11b/g/n.

Another IEEE 802.11 wireless standard is IEEE 802.11g. The 802.11g standard supports the higher data transmission rates of 54 Mbps but operates in the same 2.4 GHz range as 802.11b. The 802.11g equipment is also backward compatible with 802.11b equipment. This means that 802.11b wireless clients will be able to communicate with the 802.11g access points, and the 802.11g wireless client equipment will communicate with the 802.11b access points.

The obvious advantage of this is that companies with an existing 802.11b wireless network will be able to migrate to the higher data rates provided by 802.11g without having to sacrifice network compatibility. In fact, new wireless equipment support both the 2.4 GHz and 5 GHz standards, giving it the flexibility of high speed, compatibility, and noninterference.

Another entry into wireless networks is the 802.11n. This wireless technology can operate in the same ISM frequency as 802.11b/g (2.4GHz) and can also operate in the 5 GHz band. A significant improvement with 802.11n is **MIMO** (Multiple Input Multiple Output). MIMO uses a technique called space-division multiplexing, where 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 there can be increased power consumption. The 802.11n specification includes a MIMO power-save mode. With this, 802.11n only uses multiple data paths when faster data transmission is required—thus saving power.

Table 11-4 lists the 802.11n frequency bands. This table shows frequencies in both the 2.4 GHz and 5 GHz range. The frequencies being used in the 5 GHz band are the same as those used in 802.11a, and note that there is the possibility of using both 20MHz and 40MHz channels.

MIMO

A space-division multiplexing technique where the data stream is split into multiple parts called spatial streams

TABLE 11-4 The 802.11n Frequency Bands

Frequency Band (GHz)	Independent 20 MHz Channels	Possible 40 Mhz Channels
2.40–2.485	3	1
5.15–5.25	4	2
5.25–5.35	4	2
5.47–5.75	10	5
5.75–5.85	4	2

Wi-Fi

Wi-Fi Alliance—an organization that tests and certifies wireless equipment for compliance with the 802.11x standards

Wireless networks also go by the name **Wi-Fi**, which is the abbreviated name for the Wi-Fi Alliance (Wi-Fi stands for wireless fidelity). The Wi-Fi Alliance is an organization whose function is to test and certify wireless equipment for compliance with the 802.11x 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:

- **802.11a (Wireless-A):** This standard can provide data transfer rates up to 54 Mbps and an operating range up to 75 feet. It operates at 5 GHz (Modulation—OFDM)
- **802.11b (Wireless-B):** This standard can provide data transfer rates up to 11 Mbps with ranges of 100 to 150 feet. It operates at 2.4 GHz. (Modulation—DSSS)
- **802.11g (Wireless-G):** This standard can provide data transfer rates up to 54 Mbps up to 150 feet. It operates at 2.4 GHz. (Modulation—DSSS or OFDM)
- **802.11n (Wireless-N):** This is the next generation of high-speed wireless connectivity promising data transfer rates over 200+ Mbps. It operates at 2.4 GHz and 5 GHz. (Modulation—DSSS or OFDM)
- **802.11i:** This standard for wireless LANs (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 handoffs between access points or cells in a wireless LAN. This standard is a critical addition to 802.11 WLANs if voice traffic is to become widely deployed.

11-3 802.11 WIRELESS NETWORKING

A wireless LAN can be configured in many ways to meet the needs of an organization. Figure 11-6 provides an example of a basic 802.11b/g/n WLAN configuration. Each PC is outfitted with a wireless LAN adapter card. The PC cards come in many styles, such as PCI, ISA, or PCMCIA, and some units are external to the computer. The wireless adapter (wireless LAN adapter) is the device that connects the client to the wireless medium. The medium is typically a radio wave channel in the 2.4 GHz ISM band. The wireless medium can also be infrared, although this is not used very often. The following services are provided by the wireless LAN adapter:

- Delivery of the data
- Authentication
- Privacy

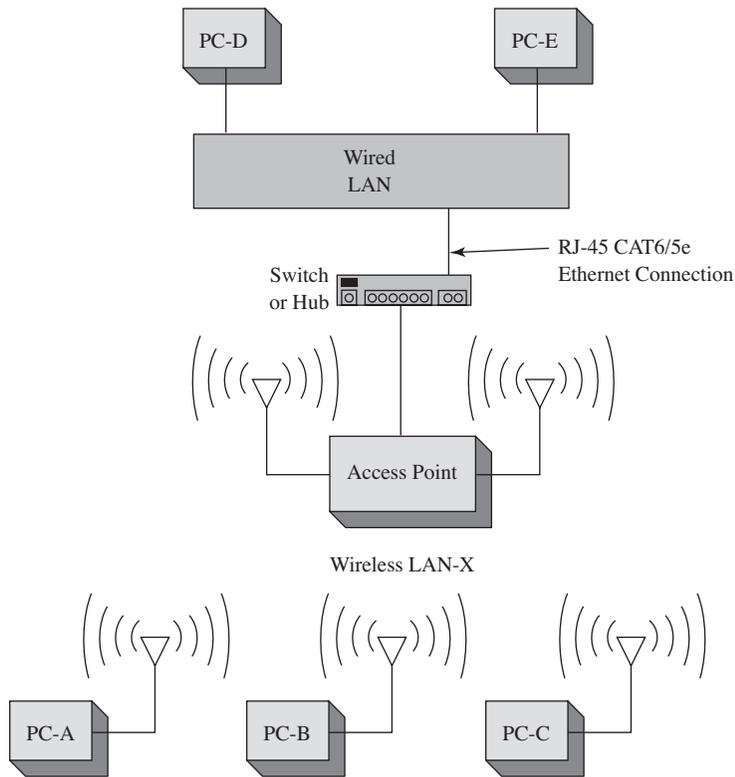


FIGURE 11-6 The setup for a basic wireless LAN.

The connection to a wired LAN is provided by a wireless access point, which provides a bridge between the wireless LAN and the wired network. A physical cable connection (typically CAT6/5e) ties the access point to the wired network's switch or hub (typically Ethernet).

For example, computer PC-A shown in Figure 11-6 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 the 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.

A question should come up at this point: “How does the access point know that the wireless data packet is being sent from a client in the wireless LAN?”

SSID
Service set identifier

The answer is 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*, basically a password that 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 that a wireless connection has been obtained.

Another common question is, “Why does the access point have two antennas?” The answer is the two antennas implement what is called “spatial diversity.” This antenna arrangement improves received signal gain and performance.

Figure 11-7 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 this MAC address has been “added” to the list of associations. This type of information is typically available via the wireless management software that typically comes with the wireless PC or PCMCIA adapter.

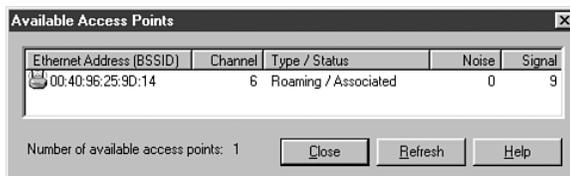


FIGURE 11-7 An example of the information displayed when an association is made by a client with an access point.

Access points use the association to build a table of users (clients) on the wireless network. Figure 11-8 provides an example of an association table. The association table lists the MAC addresses for each networking device connected to the wireless network. The access point then uses this table to forward data packets between the access point and the wireless network. The wireless client adapter will also notify the user if the client has lost an association with the access point. An example of this also is provided in Figure 11-8.

A wireless bridge is a popular choice for connecting LANs (running similar network protocols) together even if the LANs are miles apart. Examples are provided in Figure 11-9 (a) and (b). Figure 11-9 (a) shows a point-to-point wireless bridge. Each building shown in Figure 11-9 (a) has a connection from the wireless bridge to the building’s LAN, as shown in Figure 11-10. The wireless bridge then connects to an antenna placed on the roof, and there must be a clear (line-of-sight) transmission path between the two buildings, or there will be signal *attenuation* (loss) or possible signal disruption. Antenna selection is also critical when configuring the connection. This issue is addressed in section 11-5. The antenna must be selected so that the signal strength at the receiving site is sufficient to meet the required received signal level.



FIGURE 11-8 An example of a “lost” association.

Figure 11-9 (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 11-10. 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).

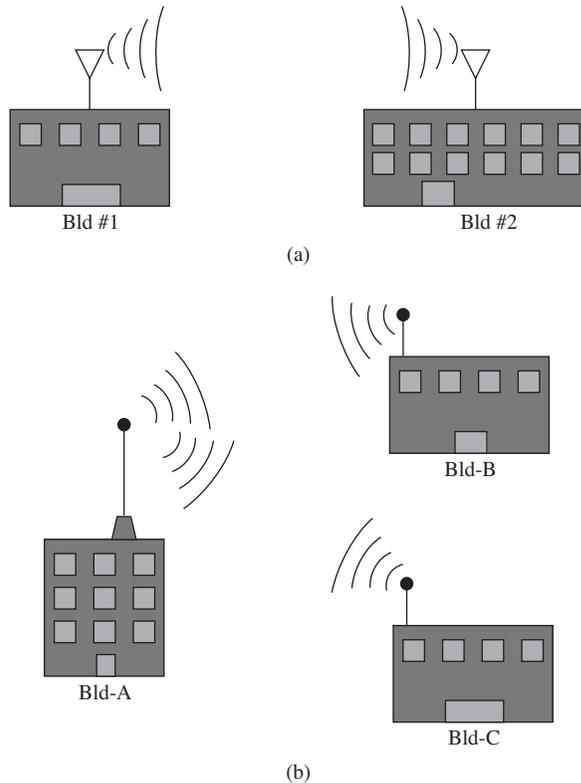


FIGURE 11-9 Examples of (a) point-to-point and (b) point-to-multipoint wireless bridge configurations.

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

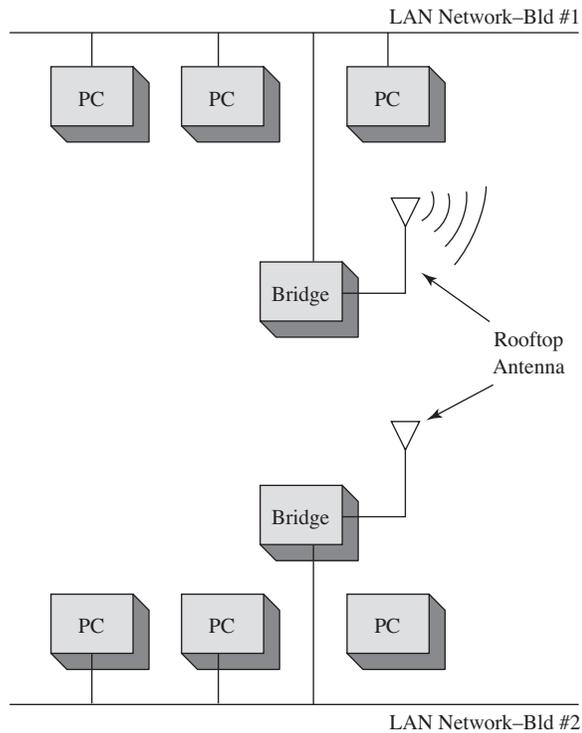


FIGURE 11-10 The wireless bridge connection to the wired network inside the building.

A solution is to place multiple wireless access points within the facility, as shown in Figure 11-11. Mobile clients will be able to maintain a connection as they travel through the workplace because the wireless client will automatically select 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 in the shape of circles in Figure 11-11. In actual practice, the radiation patterns are highly irregular due to reflections of the transmitted signal.

It is important to verify that sufficient RF signal level is available for the users in the 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 the wireless clients. Site surveys are also done with outside installations to determine the coverage area.

Site Survey

Performed to determine the best location(s) for placing the access point(s) to provide maximum RF coverage for the wireless clients

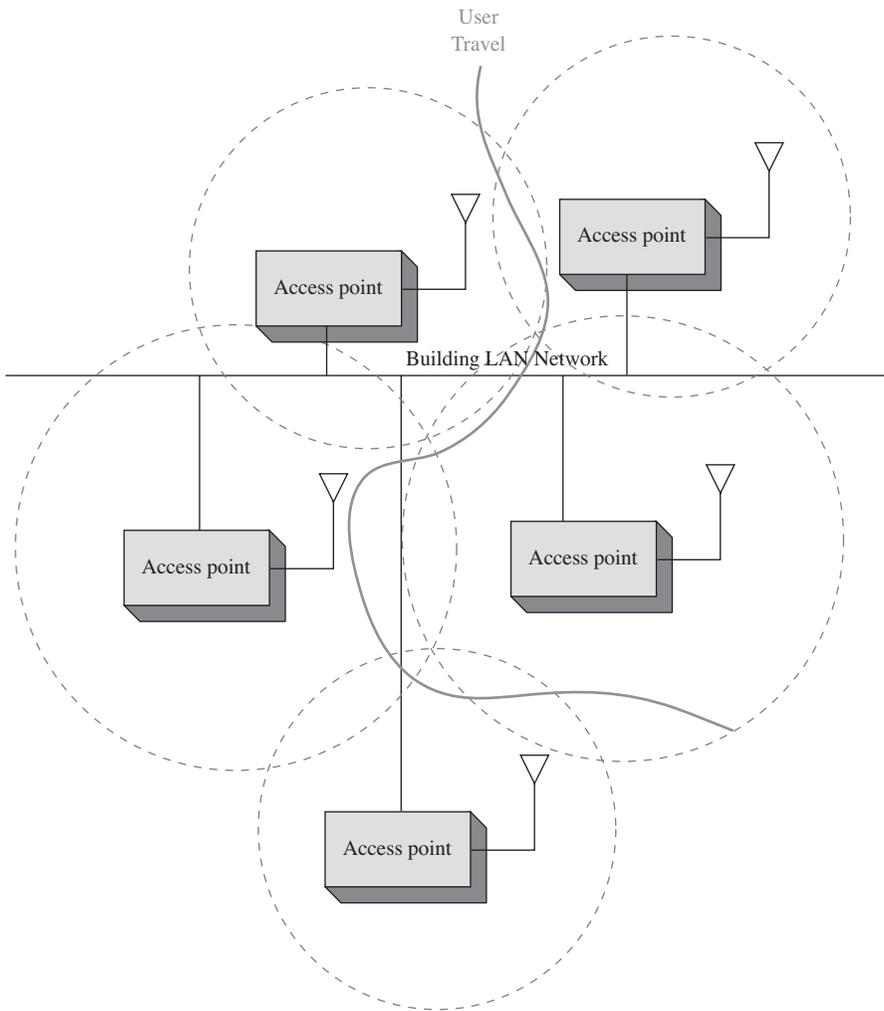


FIGURE 11-11 An example of configuring multiple access points to extend the range for wireless connectivity.

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
- Identify any significant RF interference

For example, a site survey was conducted to determine access point placement to provide wireless network connectivity for a building. The objective was to provide mobile client access throughout the building. The building already had two wired connections available for placing an access point. Figure 11-12 provides the floor plan for the building.

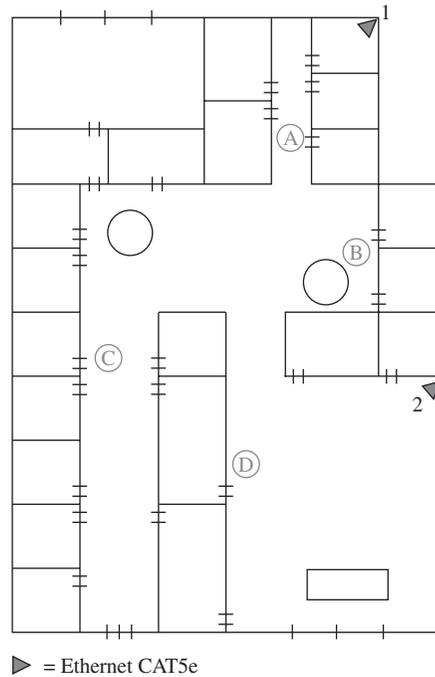


FIGURE 11-12 The floor plan of the building being surveyed for a wireless LAN.

The available wired network connections are indicated in the drawing. The site survey began with placing an access point at position 1. A wireless mobile client was used to check the signal throughout the building. The wireless management software that came with the WLAN adapter was used to gather the test results.

The first measurement was taken at point A as shown in Figure 11-13. Notice that the data speed is 11 Mbps. This will change if the signal level decreases significantly. The wireless PCMCIA card also comes with a way to check the signal statistics as illustrated in Figure 11-14. This figure provides a plot of the signal quality, the missed access point (AP) beacons, transmit retries, the signal strength, and the transmit rate.

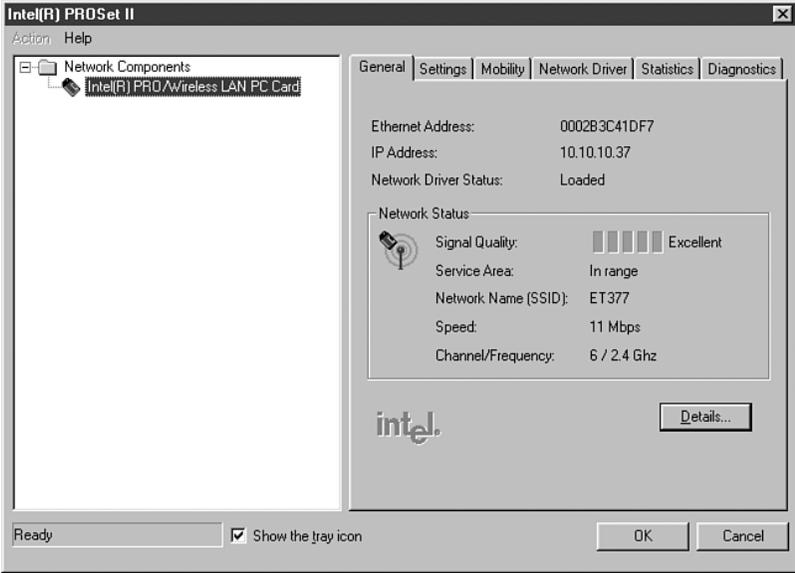


FIGURE 11-13 The RF signal level observed at point A.

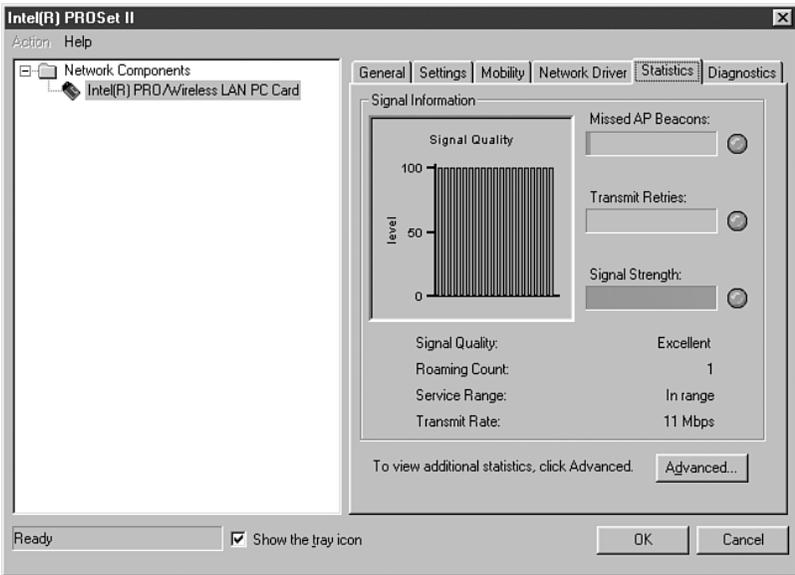


FIGURE 11-14 The signal statistics from point A.

The next observation was made at point B. A signal level of “Good” and a transmit rate of 11 Mbps was observed. The signal has decreased somewhat, but the “Good” indicates that a connection is still available. Figure 11-15 shows the observation made at point B. The signal level drops to “Fair” at point C as shown in Figure 11-16.

The mobile client was moved to point D in the building, and a signal quality of “Out of range” was observed. This is also called a *loss of association* with the access point. Figure 11-17 shows the observed signal level.

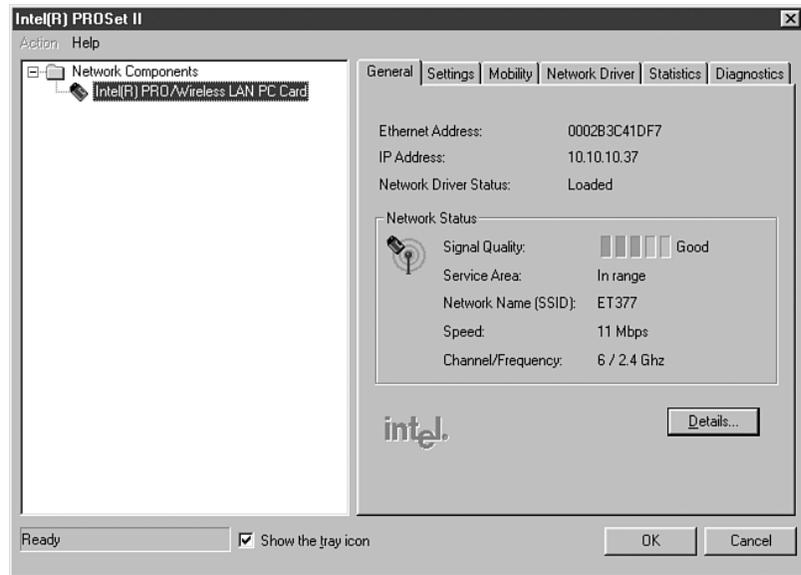


FIGURE 11-15 The signal quality of “Good” at point B.

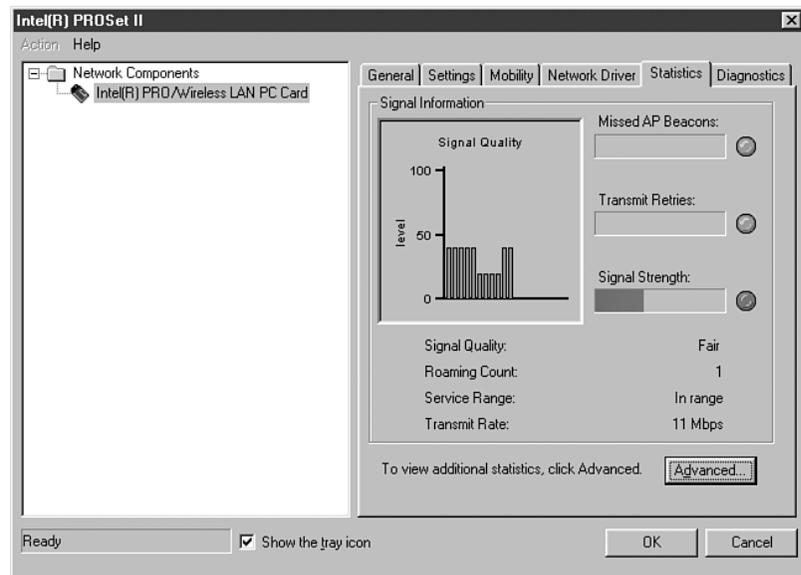


FIGURE 11-16 The drop in the signal quality to “Fair” at point C.

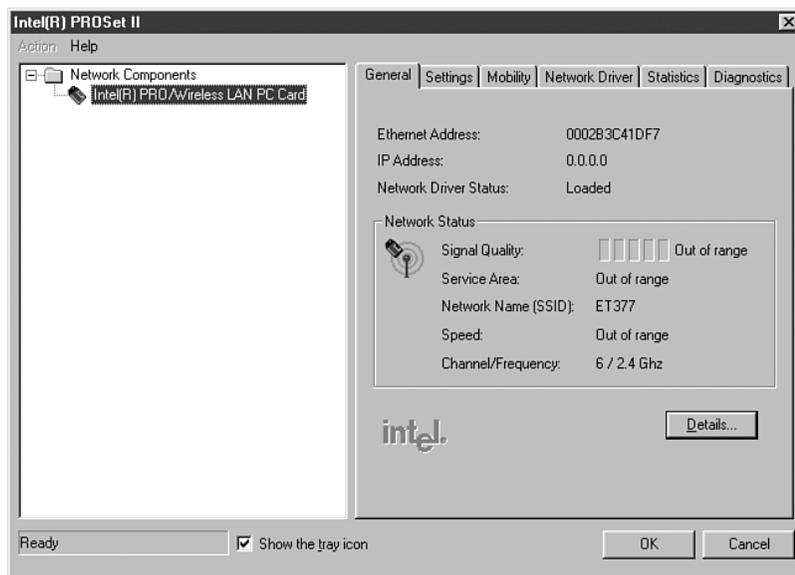


FIGURE 11-17 The “Out of range” measurement for point D.

The site survey shows 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 was decided to place another access point at point 2. The site survey was repeated, and it showed that “Excellent” signal strength was obtained throughout the building. In some cases, a *range extender* can be used to provide additional wireless coverage. This device basically extends the reach of the wireless network.

11-4 BLUETOOTH, WIMAX, AND RFID

This section looks at three different wireless technologies: Bluetooth, WiMAX, and RFID. Each of these technologies plays important roles in the 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

This section examines another wireless technology called *Bluetooth*, 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 2.4 GHz ISM frequency band, which is the same frequency band used by 802.11b/g/n. There are three output power classes for Bluetooth. Table 11-5 lists the maximum output power and the operating distance for each class.

TABLE 11-5 Bluetooth Output Power Classes

Power Class	Maximum Output Power	Operating Distance
1	20 dBm	~ 100 m
2	4 dBm	~ 10 m
3	0 dBm	~ 1 m

Inquiry Procedure

Used by Bluetooth to discover other Bluetooth devices or to allow itself to be discovered

Paging Procedure

Used to establish and synchronize a connection between two Bluetooth devices

Piconet

An ad hoc network of up to eight Bluetooth devices

When a Bluetooth device is enabled, it uses an **inquiry procedure** to determine whether any other Bluetooth devices are available. This procedure is also used 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. The **paging procedure** is used to establish and synchronize a connection between two Bluetooth devices. When the procedure for establishing the connection has been completed, the Bluetooth devices will have established a **piconet**. A piconet is 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 master) is responsible for providing the synchronization clock reference. All other Bluetooth devices are called slaves.

The following is an example of setting up a Bluetooth network linking a Mac OS X computer to another Bluetooth enabled device. To enable Bluetooth on the Mac OS X, click **Apple—Systems Preferences**. Under hardware, select **Bluetooth—Settings**, and the window shown in Figure 11-18 is opened. Click the **Bluetooth Power** button to turn on Bluetooth. Click **Discoverable**. This enables other Bluetooth devices to find you.



FIGURE 11-18 The window for configuring the Bluetooth settings.

Pairing

When a Bluetooth device is set up to connect to another Bluetooth device.

In the next step you will select the device with which you will be establishing a Bluetooth connection. Select **Devices—Set-up New Device—Turn Bluetooth On** if it is not already on. You will next be guided using the **Bluetooth Setup Assistant** and will be asked to select the device type. You have the choice of connecting to a mouse, keyboard, mobile phone, printer, or other device. In this case, **Other Device** is selected. This choice is selected when connecting to another computer. The **Bluetooth Device Setup** will search for another Bluetooth device. There will be a notification on the screen alerting you when another Bluetooth device is found. Select continue if this is the device you want to connect to. It is called **pairing** when another

Bluetooth device is set up to connect to another Bluetooth device. You may be asked for a Passkey. The **Passkey** is used in Bluetooth Security to limit outsider access to the pairing. Only people with the Passkey will be able to pair with your Bluetooth device.

Passkey

Used in Bluetooth Security to limit outsider access to the pairing

At this point, you are now able to transfer files between the paired devices. This requires that the file exchange settings for the device have been set to allow files to come in. An example of the setup for the file transfer is shown in Figure 11-19.



FIGURE 11-19 The window showing the settings for a file transfer.

The screen shown in Figure 11-20 shows an incoming text file. The File Transfer menu enables the user to select where received files are saved. In this case, the incoming files are being saved to the desktop.

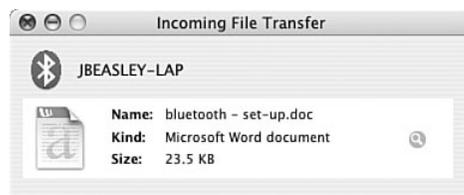


FIGURE 11-20 The window showing that a text file is coming in from another Bluetooth device.

This example has demonstrated setting up Bluetooth on a Mac OS X. The steps for setting up Bluetooth on a Windows XP or Vista computer or even a Blackberry differ slightly, but the basic steps are the same. The following are the basic steps you need to complete to pair with another Bluetooth device:

1. Enable the Bluetooth radio.
2. Enable Discoverability (this enables other Bluetooth devices to find you).
3. Select the device for pairing.

WiMAX

A broadband wireless system based on the IEEE 802.16e standard

BWA

Broadband wireless access

NLOS

Non line-of-sight

WiMAX

WiMAX (Worldwide Interoperability for Microwave Access) is a broadband wireless system that has been developed for use as broadband wireless access (**BWA**) for fixed and mobile stations and can provide a wireless alternative for last mile broadband access in the 2 GHz to 66 GHz 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 3.5 GHz while the United States uses both the unlicensed 5.8 GHz and the licensed 2.5 GHz spectrum. There are also investigations with adapting WiMAX for use in the 700 MHz 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 the bandwidth.

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

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

Additionally, 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, it is allocated a time slot by the base station, thereby providing the WiMAX with 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 make sure time-sensitive data is delivered on time. Additionally, WiMAX operates in a collision-free environment, which improves channel throughput.

WiMAX has a range of up to 31 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 the telecommunications provider to the customer. The cost of the last mile connection can be expensive, which makes a wireless alternative attractive to the customer.

The 802.16e WiMAX standard holds a lot of promise for use as a mobile air interface. Another standard, 802.20, is a mobile air interface being developed for consumer use. This standard plans to support data rates over 1 Mbps, which is comparable to DSL and cable connections. Additional 802.20 is being developed to support high-speed mobility. In other words, the user could be in a fast car or train and still have network connectivity.

RFID (Radio Frequency Identification)

Radio Frequency Identification (RFID) is a technique that uses radio waves to track and identify people, animal, objects, and shipments. This is done by the principle of modulated **backscatter**. The term “backscatter” is referring to the reflection of

Last Mile

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

Radio Frequency Identification (RFID)

A technique that uses radio waves to track and identify people, animals, objects, and shipments

Backscatter

Refers to the reflection of the radio waves striking the RFID tag and reflecting back to the transmitter source

the radio waves striking the RFID tag and reflecting back to the transmitter source with its stored unique identification information.

Figure 11-21 illustrates the basic block for an RFID system.

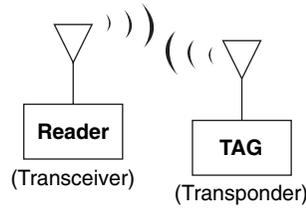


FIGURE 11-21 Basic block diagram of an RFID system.

The RFID system consists of two things:

- An RFID tag (also called the RF transponder) includes an integrated antenna and radio electronics.
- A reader (also called a transceiver) consists of a transceiver and an antenna. A transceiver is the combination of a transmitter and receiver.

The reader (transceiver) 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, the transportation industries, and the Department of Defense. Additionally, RFID applications are being used in Homeland Security in tracking container shipments at border crossings. Additionally, RFID is being incorporated into wireless LAN (WLAN) computer networks to keep better track of inventory. Wireless technologies are becoming more important for the enterprise. RFID technology is being used as a wireless means for asset tracking and as a result is placing more importance on its role in the network. The tracking technology is even being extended to tracking WiFi devices within the WLAN infrastructure.

There are three parameters that define an RFID system. These include the following:

- 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. The three different classifications are passive, semi-active, and active.

- **Passive:** Power is provided to the 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 11-22 shows an example of a passive RFID tag (also called an inlay). The tag inlays include both the RFID chip and the antenna mounted on a substrate.
- **Semi-active:** The tags use a battery to power the electronics on the tag but use the property of backscatter to transmit information back to the reader.
- **Active:** Use a battery to power the tag and transmit a signal back to the reader. Basically this is a radio transmitter. New active RFID tags are incorporating wireless Ethernet, the 802.11b–WiFi connectivity. An example is the G2C501 Active RFID tag from G2 Microsystems shown in Figure 11-23. The power consumption of the G2C501 is 10 μ A in the sleep mode and uses two AA batteries with an expected lifetime of five years. The G2C501 also works in the standard 915 MHz range. The G2C501 also 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.

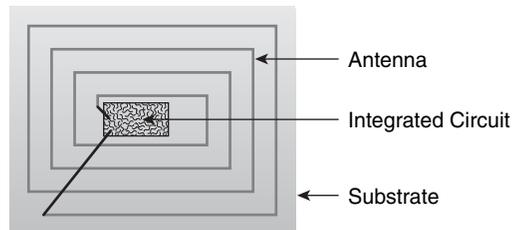


FIGURE 11-22 Examples of an RFID inlay.

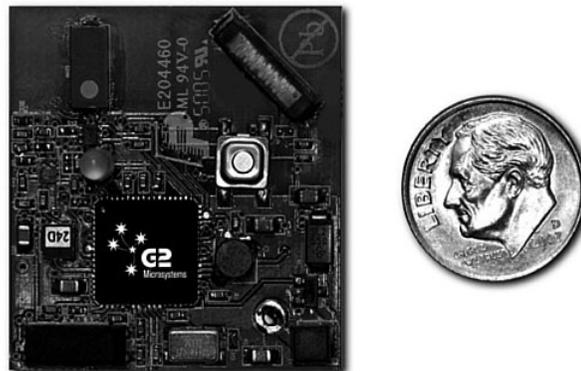


FIGURE 11-23 The G2C501 Active RFID tag from G2Microsystems (courtesy of G2Microsystems).

Frequency of Operation The RFID tags must be tuned to the reader's transmit frequency to turn on. RFID systems typically use three frequency bands for operation, LF, HF, and UHF as shown in Figure 11-24:

- **Low-frequency (LF)** tags typically use frequency-shift keying (FSK) between the 125/134 kHz frequencies. The data rates from these tags is low (~12 kbps) and they are not appropriate for any applications requiring fast data transfers. However, the low-frequency tags are suitable for animal identification, such as 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 .33 meters.
- **High-frequency (HF)** tags operate in the 13.56 MHz industrial band. High-frequency tags have been available commercially since 1995. It is known that the longer wavelengths of the HF radio signal are less susceptible to absorption by water or other liquids. Therefore, these tags are better suited for tagging liquids. The read range for high-frequency 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.
- **Ultra-high frequency (UHF)** tags work at 860–960 MHz and at 2.4 GHz. The data rates for these tags can be from 50–150 kbps and greater. These tags are popular for tracking inventory. The read range for passive UHF tags is 10–20 feet, which make it a better choice for reading pallet tags. However, if an active tag is used, a read range up to 100 meters is possible.

LF	HF	UHF
125/134 kHz	13.56 MHz	860 - 960 MHz 2.4 GHz

FIGURE 11-24 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 technique similar to the Ethernet protocol. In a Slotted Aloha protocol, the tags are only allowed to transmit at predetermined times after being energized. This technique reduces the chance of data collisions between RFID tag transmissions and allows for the reading of up to 1000 tags per second. (Note: This is 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 a possible RF data collision can 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 technique similar to the Ethernet protocol

11-5 SECURING WIRELESS LANS

This section provides an overview of securing 802.11 wireless LANs. The network administrator must be aware of the security issues when configuring a wireless LAN. The fact is, RF (radio frequencies) will pass through walls, ceilings, and floors of a

building even with low signal power. Therefore, the assumption should never be made that the wireless data is confined to only the user's area. The network administrator must assume that the wireless data can be received by an unintended user. In other words, the use of an unsecured wireless LAN is opening a potential threat to network security.

To address this threat to WLAN security, the network administrator must make sure the WLAN is protected by firewalls and intrusion detection (see Chapter 10), and most importantly the network administrator must make sure that the wireless security features are

TURNED ON!!!!!!

This might seem to be a bold statement, but surprisingly enough, many WLANs are placed on a network without turning on available wireless security features. Many times the user in the WLAN assumes that no one would break into his or her computer because nothing important exists on the system. This may be true, but to an attacker, the user has one very important item, access to the wired network through an unsecured client.

WLANs use an SSID (service set identifier) to authenticate users, but the problem is that the SSID is broadcast in radio link beacons about 10 times per second. In WLAN equipment, the **beacons** are transmitted so that a wireless user can identify an access point to connect to. The SSID can be turned off so it isn't transmitted with a beacon, but it is still possible for the SSID to be obtained by packet sniffing. As noted previously, *packet sniffing* is a technique used to scan through unencrypted data packets to extract information. In this case, an attacker uses packet sniffing to extract the SSID from data packets. Disabling SSID broadcasting will make it so that most client devices (such as Windows PCs and laptops) won't notice that the wireless LAN is present. This at least keeps "casual snoopers" off the network. Enterprise-grade access points implement multiple SSIDs, with each configured SSID having its own VLAN and wireless configuration. This allows the deployment of a common wireless LAN infrastructure that supports multiple levels of security, which is important for some venues such as airports and hospitals (where there are both public and private users).

IEEE 802.11 supports two ways to authenticate clients: open and sharekey. *Open* authentication basically means that the correct SSID is being used. In *sharekey* authentication, a packet of text is sent by the access point to the client with the instruction to encrypt the text and return it to the access point. This requires that wired equivalent privacy (WEP) be turned on. WEP is used to encrypt and decrypt wireless data packets. The exchange and the return of the encrypted text verifies that the client has the proper WEP key and is authorized to be a member of the wireless network. It is important to note that shared key authentication is extremely vulnerable. As a result, it's standard practice to avoid the use of shared key authentication. An example of the setting for WEP encryption is provided in Figure 11-25 (a and b). In Figure 11-25 (a), the user has the WEP options of disabled (No Privacy), 64-bit WEP (Privacy), and 128-bit WEP (More Privacy). Figure 11-25 (b) shows the wireless security settings in Windows Vista. There are clearly more options, and these newer wireless security settings are discussed next.

There is some concern that WEP isn't a strong enough encryption to secure a wireless network. There is published information about WEP vulnerabilities, but even with this, WEP does provide some basic security and is certainly better than operating the network with no security.

Beacon

Used to verify the integrity of a wireless link

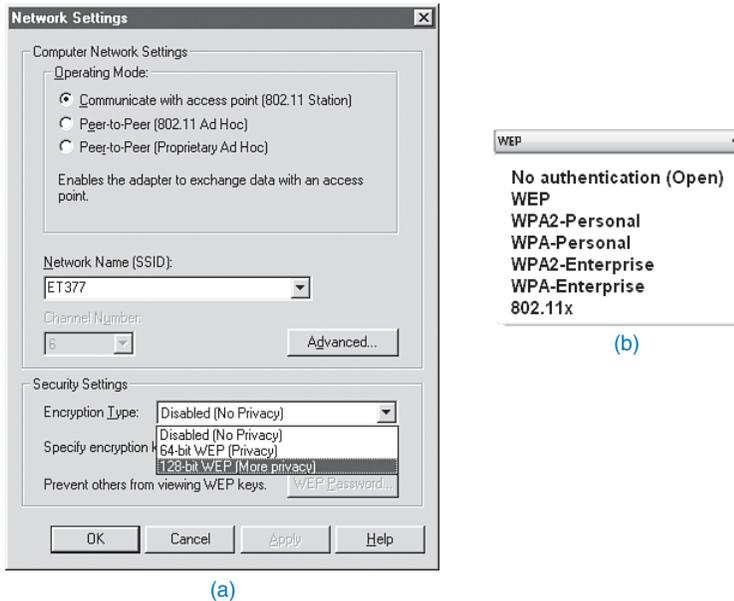


FIGURE 11-25 An example of setting WEP encryption on a wireless client.

An improvement with wireless security is provided with WPA and WPA2. **WPA** stands for Wi-Fi Protected Access, and it supports the user authentication provided by 802.1x and replaces WEP as the primary way for securing wireless transfers. WPA2 is an improved version of WPA. The 802.1x standard enhances wireless security by incorporating authentication of the user. Cisco Systems uses an 802.1x authentication system called LEAP. In Cisco LEAP, the user must enter a password to access the network. This means that if the wireless client is being used by an unauthorized user, the password requirement will keep the unauthorized user out of the network.

WPA is considered to be a higher level of security for wireless systems. In the 802.1x system, a user requests access to the wireless network via an access point. The next step is for the user to be authenticated. At this point, the user can only send EAP messages. **EAP** is the Extensible Authentication Protocol and is used in both WAP and WAP2 by the client computer and the access point. The access point sends an EAP message requesting the user's identity. The user (client computer) returns the identity information that is sent by the access point to an authentication server. The server will then accept or reject the user's request to join the network. If the client is authorized, the access point will change the user (client's) state to authorized. A Remote Authentication Dial-In User Service (**RADIUS**) service is sometimes used to provide authentication. This type of authentication helps prevent unauthorized users from connecting to the network. Additionally, this authentication helps to keep authorized users from connecting to a rogue of unauthorized access points.

Another way to further protect data transmitted over a WLAN is to establish a VPN connection (see Chapter 8). In this way, the data is protected from an attacker. The following are basic guidelines for wireless security:

- Make sure the wireless security features are turned on.
- Use firewalls and intrusion detection on your WLAN.

WPA

Wi-Fi Protected Access

EAP

Extensible Authentication Protocol

RADIUS

Remote Authentication Dial-In Service

- Improve authentication of the WLAN by incorporating 802.1x features.
- Consider using third-party end-to-end encryption software to protect the data that might be intercepted by an unauthorized user.
- Whenever possible, use encrypted services such as SSH and Secure FTP.

The bottom line is that the choice of the level of security will be based on multiple factors within the network. For example, what is the cost benefit ratio of increased security? How will incorporating or not incorporating increased wireless security affect users? The network administrator and the overall management will have to make the final decision regarding wireless security before it is installed and the network becomes operational.

11-6 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. 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 (home network). This example addresses the following issues:

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 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. A simple terrain profile of the proposed area is shown in Figure 11-26. The data rate for the wireless connection to remote users needs to be at least 2 Mbps.

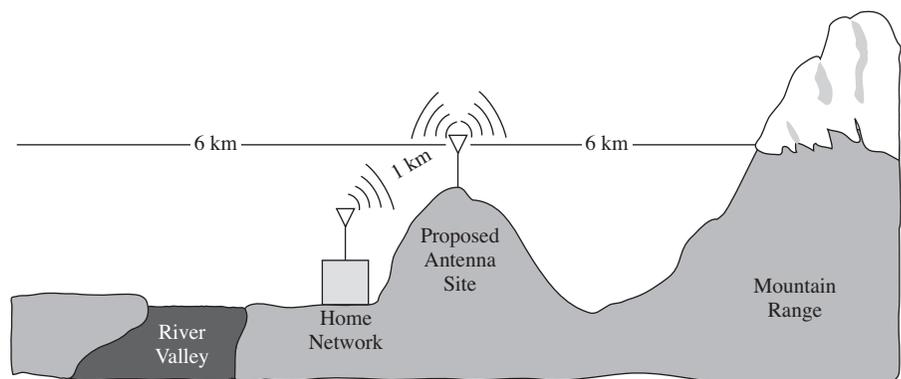


FIGURE 11-26 The terrain profile of the area to be supported by the proposed point-to-multipoint wireless network.

1. Antenna Site Survey

The proposed antenna site (see Figure 11-26) is on top of a hill approximately 1 kilometer (km) 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 km 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 11 Mbps wireless link back to the home network.

2. Establishing a Point-to-Point Wireless Link to the Home Network

The cost is too high to put in a wired connection back to the home network; therefore, 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 11-27 shows the proposed wireless connection.

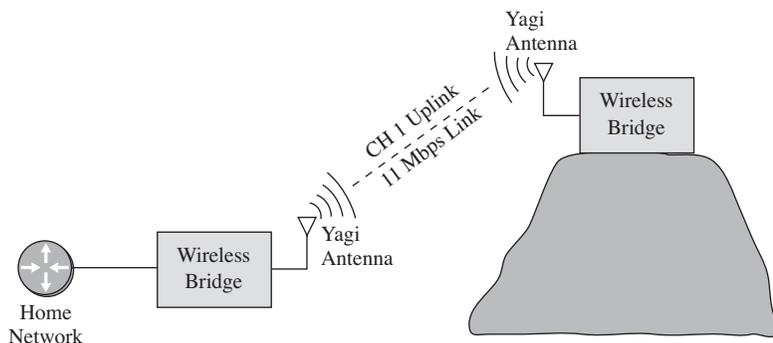


FIGURE 11-27 The proposed point-to-point wireless link from the home network to the antenna site.

There are many manufacturers of antennas that support wireless networking, and there are many types of antenna that 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 11-6.

TABLE 11-6 Sample of 802.11b Wireless Antennas

Antenna	Type	Radiation Pattern	Range in km at 2 Mbps	Range in km at 11 Mbps	Costs
A.	Omni	Omnidirectional	7	2	Moderate
B.	Yagi	Directional	12	7.5	Moderate
C.	Dish	Highly directional	38	18	High

Antenna A has an omnidirectional radiation pattern. This means the antenna can receive and transmit signals in a 360-degree pattern. Figure 11-28 (a) shows the radiation pattern for an omnidirectional antenna. Antenna A supports a 2 Mbps data rate up to 7 km from the antenna and supports an 11 Mbps data rate at a maximum distance of 2 km. Table 11-6 also indicates that this antenna has a moderate cost.

Antenna B is a Yagi antenna with a directional radiation pattern as shown in Figure 11-28 (b). The Yagi antenna supports a 2 Mbps data rate for a maximum of 12 km.

Antenna C is a “dish” antenna or parabolic reflector. These antennas provide extremely high directional gain. In this example, the dish antenna supports 11 Mbps up to 18 km away and 2 Mbps up to 38 km away. The cost of the dish antenna can be quite high relative to the cost of the Yagi or omnidirectional antenna.

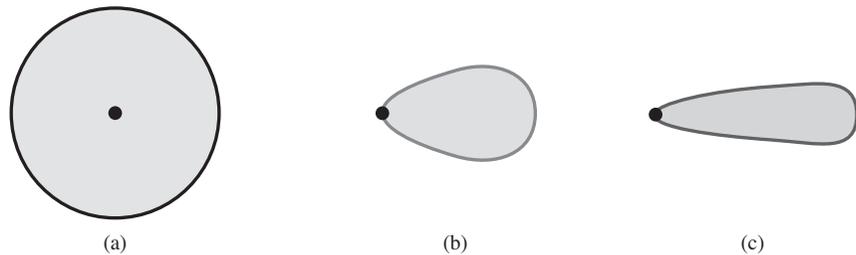


FIGURE 11-28 Antenna radiation patterns for (a) omnidirectional, (b) Yagi, and (c) dish [parabolic reflector] antenna, and supports 11 Mbps up to 7.5 km from the antenna. The cost of the Yagi antenna is comparable to the omnidirectional antenna.

Antenna B, the directional Yagi, is selected for the point-to-point link. The antenna meets the distance requirement and also meets the 11 Mbps 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

3–4. Configuring the Multipoint Distribution/Conducting an RF Site Survey

At this point, an 11 Mbps 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 2 Mbps 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 km in each direction. Antenna A (see Table 11-6) provides an omnidirectional radiation pattern for 7 km. This satisfies the coverage area and 2 Mbps data rate. Antenna A is mounted on the antenna site tower, connected to a lightning arrestor and then connected to the output of a wireless bridge. An RF site survey of the planned coverage area is next done to verify the signal quality provided by the antenna selected. Measurements are made from multiple locations within the planned coverage area. All remote sites within 4 km of the distribution show a signal strength of “Excellent,” as shown in Figure 11-29.

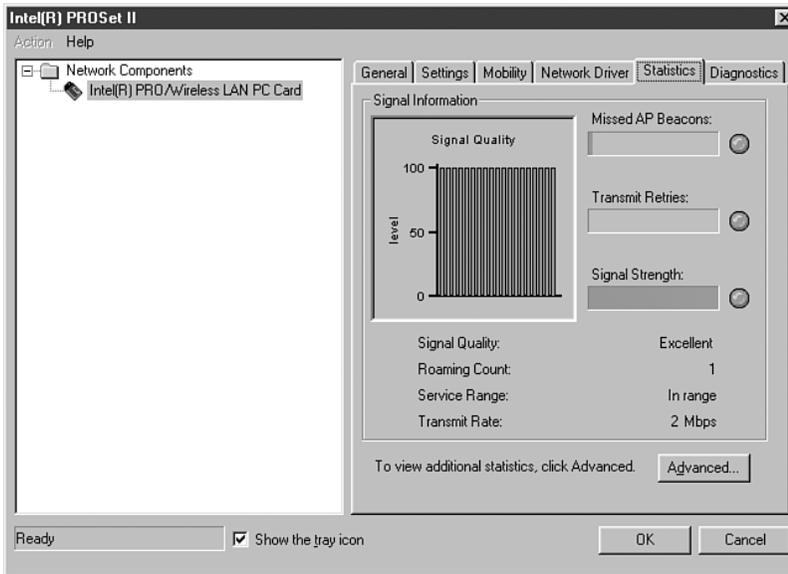


FIGURE 11-29 The signal quality of “Excellent” measured for the multipoint distribution.

The signal quality drops to “Good” at 6 km at all surveyed remote locations except for one area that shows a “Poor.” The measurement for this site is provided in Figure 11-30. Apparently the signal is being affected by multipath distortion off 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 is to add antenna “diversity.” Basically this means that multiple antennas are placed on the receiving tower, and the best signal is used for the connection.

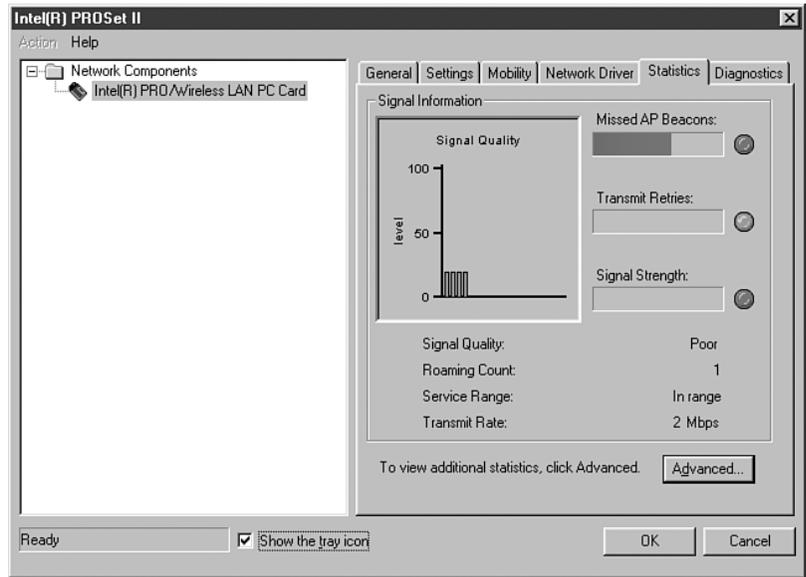


FIGURE 11-30 The signal quality of “Poor” measured at the remote site near the lake.

5. Configuring the Remote Installations

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

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

Antenna B (see Table 11-6) is selected for the directional antenna. This antenna will provide sufficient RF signal level for the remote user. Each remote user will need a wireless bridge and a switch to connect multiple users. (Note that the bridge is set for a 2 Mbps data rate.) Figure 11-31 shows the setup for the remote user.

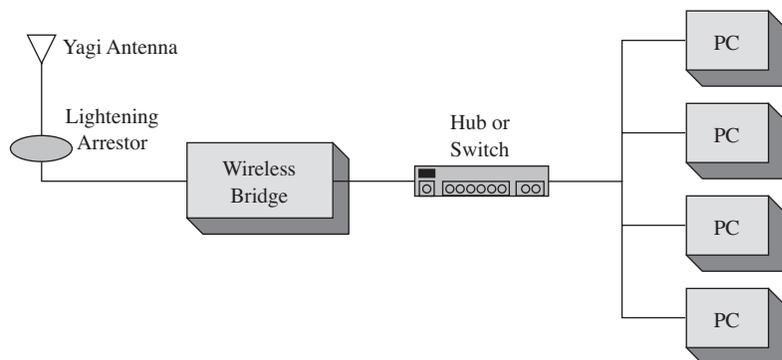


FIGURE 11-31 The setup for the remote user in the proposed point-to-multipoint wireless network.

SUMMARY

This chapter presented an overview of wireless networking. The fundamental concept and example networks were also presented. The vendors of wireless networking equipment have made them very easy to integrate into existing networks, but the reader must understand that the key objective of the network administrator is to provide a fast, reliable, and secure computer network. Carelessly integrating wireless components into the network can easily compromise this objective. Students should understand the following from reading this chapter:

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

A final note: The new wireless networking technologies have greatly simplified planning and installation. Anytime you are working with RF (radio frequencies) 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 will 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 11-2

1. List two advantages of wireless networking.
2. What are the three areas defined for the IEEE 802.11 standard?
3. What is an *ad hoc network*?
4. What is the purpose of an Extended Service Set?
5. What are the four physical layer technologies being used in 802.11 wireless networking?
6. Describe the frequency spectrum for the DSSS channels in 802.11b wireless networking.
7. Define a *pseudorandom sequence* as it applies to FHSS.
8. What must the FHSS transmitting and receiving units know to communicate?
9. What is the frequency range used by 802.11a, and what modulation technique is used?
10. What is the maximum data rate for the following:
 - a. 802.11b
 - b. 802.11a
 - c. 802.11g
 - d. 802.11n
11. Define MIMO as it applies to 802.11n.
12. What is the purpose of the power-save mode in 802.11n?

Section 11-3

13. What is the purpose of an access point?
14. How does the access point know if a wireless data packet is intended for its network?
15. What is an *association*, and what is its purpose?
16. Draw a picture of a point-to-point wireless connection.
17. Draw a picture of a point-to-multipoint wireless network.
18. What are the key issues to be obtained from conducting a site survey for each of the following?
 - a. indoor
 - b. outdoor

Section 11-4

19. In what frequency band does Bluetooth operate?
20. How many output power classes does Bluetooth have? List the power level and the operating range for each class.
21. What is a piconet?
22. What is the purpose of the inquiry procedure in Bluetooth?
23. What is the purpose of the paging procedure in Bluetooth?
24. Define the term *backscatter*.
25. What are the three parameters that define an RFID system?
26. Explain how power is provided to a passive RFID tag.
27. Cite three advantages for using an active RFID tag.
28. What are the three frequency bands typically used for RFID tags?
29. What is the WiMax frequency standard for the United States?
30. Why was OFDM selected for WiMax?
31. How does WiMax differ from Wi-Fi?

Section 11-5

32. What is the most important thing to do if using a wireless network?
33. What is the purpose of wireless beacons?
34. What information can be obtained from a wireless beacon?
35. What is the purpose of WEP?
36. List four guidelines for wireless security.
37. Describe the steps used by WPA2 to authenticate a user.
38. What is a RADIUS server?

Section 11-6

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

40. 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

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

Critical Thinking

41. A wireless network receiving site is experiencing occasional loss of signal due to interference. Discuss the steps you would take to correct this problem.
42. Prepare a memo to your supervisor explaining why it is important to run encryption on your wireless network.

Index

NUMBERS

- 6to4 Prefix, 184
- 8P8C. *See* RJ-45 modular connectors
- 10 Gigabit Interface Adapters. *See* XENPAKs
- 10GBASE-T, 59
 - AXT, 83-84
 - signal balance, 84
 - signal transmission, 85-86
 - standard, 83
- 802.11 WLANs, 414
 - configuring, 420
 - access points*, 422
 - bridges*, 422
 - lost associations*, 422
 - range, extending*, 424
 - signals*, 423
 - site survey*, 424-428
 - SSIDs*, 421
 - MAC layer, 415
 - OFDM, 418-419
 - physical layer, 415
- 802.11a WLANs, 420
- 802.11b WLANs, 419-420
- 802.11g WLANs, 419-420
- 802.11i WLANs, 420
- 802.11n WLANs, 419-420
- 802.11r WLANs, 420
- 8P8C. *See* RJ-45 modular connectors

SYMBOLS

- ? (help) command, 207

A

- absorption, defined, 457
- Accelerated Graphics Port. *See* AGP
- access layer (campus networks), 356
- access list permit ip any any command, 400
- access lists. *See* ACLs
- access points
 - home networks, 20
 - WLANs, 415, 422
- account lockout policies (network servers), configuring, 552
 - connected users, viewing, 554
 - enabling user accounts, 554
 - locked out accounts, 553
 - messages to users, 555
- ACLs (access control lists), 396-398
 - blocking host IP addresses example, 403
 - blocking SMB data packets example, 400-401
 - extended, 399
 - named access list example, 401-402
 - routers, applying to, 399-400
 - standard, 399
- ACR (attenuation-crosstalk), 74, 79
- Active Directory, 514

ad hoc networks. *See* BSS

adapter addresses. *See* MAC addresses

adapters

home networks, 19

PC Card, 20

Wireless-N, 20

adaptive cut-through switching, 137

adding

clients to campus networks, 363

computers to Windows 2003/2008 server domain,
522-526

groups to Windows 2003/2008 server domain, 528-532

network servers, 513

organizational units to Windows 2003/2008 server do-
main, 528-529, 531-532

users to

Linux, 561-564

Windows 2003/2008 server domain, 526-527

Address Resolution Protocol. *See* ARP

addresses

anycast, 184

class network, 240

default gateway, 196

IP

assigning, 15, 173, 268

campus network assignments, 358, 360

CIDR blocks, 181-182

classes, 15, 170

defined, 15

format, 15

gateway of last resort, 233

groups. See private addresses

home networks, 29-30

host numbers, 16

IPv4, 15

IPv6, 182-185

lease time, 359

Linux configuration, 590

name translation, 361

network numbers, 16

network servers, configuring, 521-522

next hop, configuring, 231

non-internet routable, 173

octets, 172

office-type LANs, 34

OSPF “Hello” packets, 275

private, 173

RAS configuration, 321

structure, 171

verifying, 36

logical, 138

MAC

aging time, 134

bridge tables, 126

defined, 11

dynamic, 134

filtering, 28

OUIs, 11

retrieving, 12-13

samples, 14

secure, 134

static, 134

viewing, 12

multicast, 164, 184

network, 138

next hop, 199

private, defined, 16

unicast, 184

administration commands (Linux)

man, 577

mount, 581-582

ps, 579-580

shortcuts, 583

shutdown, 583

shutdown -h now, 583

su, 580

unmount, 583

administrative distance, 245

administratively down, defined, 220

ADSL (asymmetric DSL), 313

Advanced Research Projects Agency (ARPAnet), 156

advertising, 240

aging time, 134

AGP (Accelerated Graphics Port), 106-107

Alien Crosstalk. *See* AXT

American Registry for Internet Numbers. *See* ARIN

AMI (alternate mark inversion), 295

analog modem technologies, 309-310

analyzing

campus data traffic, 378

daily, 379

hourly, 379

weekly, 380

Internet data traffic

frame size distribution, 347

network layer host tables, 346

network layer matrix, 345-346

utilization/errors strip chart, 344

unsecured data packets

captured packets, 405-407

router connections, 406

telnet session packets, 407

telnetting to routers, 405

user verification, 406

VoIP data packets, 497

acknowledgement, 499, 502

call processor message, 499

call processors call plans, 502

collecting data packets, 498

IP network handshaking, 504

NBX call processor codes, 498

PCM voice data, 499

test setup, 502

anycast addresses, 184

Apache Web service installation (Linux), 588-589

applets, defined, 539

application layer

OSI model, 123

TCP/IP, 157-158

application servers, 512

architectures (optical networking)

building distribution, 470-472

campus distribution, 472-475

data rates, 469

defining optical networking, 468-470

fiber to the business, 469

fiber to the curb, 469

fiber to the desktop, 469

fiber to the home, 469

optical Ethernet, 469-470

standards, 468

area 0, 254

areas (OSPF), 251

ARIN (American Registry for Internet Numbers), 173

armored fiber optics, 628

ARP (Address Resolution Protocol), 39, 162

arp -a command, 127

ARP caches, 126

ARP replies, 39

ARP tables. *See* ARP caches

ARPAnet (Advanced Research Projects Agency), 156

AS (autonomous systems), 246, 339

ASNs (AS numbers), 339

associations, 421

checking, 125

WLANs, 422

asymmetric DSL. *See* ADSL

asymmetric operations, 309

ATA connections, 107

ATM (Asynchronous Transfer Mode), 305

classes, 306

connections, creating, 308

interfaces, viewing, 308

PVC interface, 306

router configuration, 307

router subinterface configuration, 307

VCI, 306

virtual channels, viewing, 308

VPI, 306

attacks (security)

DDoS, 396

DoS, 395-396

firewalls, 398

intrusions

detecting, 404

packet sniffing, 390

password cracking, 389-390

social engineering, 389

viruses, 393

vulnerable software, 391-393

wireless vulnerabilities, 394

worms, 393

attenuation, 71-72, 457

attenuation-crosstalk. *See* ACR

attenuators, 463

authentication, 436, 534

auto-negotiation protocol, 145

advantages/disadvantages, 148

FLPs, 146

full/half duplex, 146-147

process, 146

autonomous systems. See AS

available bit-rate class, 306

AXT (Alien Crosstalk), 83-84

B

B8ZS (bipolar 8 zero substitution) encoding, 296

backbone cabling structured cabling subsystem, 52

backbones, 251, 473

backdoors, 392

backhoe fading, 476

backscatter, 432

balanced mode, UTP, 58

bash (bourne again shell), 566

Basic Input Output System. See BIOS

Basic Service Set. See BSS

beacons, 436

BGP (Border Gateway Protocol), 338

configuring, 339-343

Net-Challenge configuration, 343-344

bin directory (Linux), 569

binary-decimal number conversions, 165-166

binary-hexadecimal number conversions, 170

BIOS (Basic Input Output System), 116

bipolar 8 zero substitution (B8ZS) encoding, 296

bipolar coding, 296

bipolar violations, 296

Blocking state (STP), 378

Bluetooth, 429

configuring, 430-431

inquiry procedure, 430

paging procedure, 430

piconets, 430

boot directory (Linux), 569

boot processes (Linux), troubleshooting, 598-600

boot sequence

BIOS, configuring, 116

defined, 116

boot services (Linux), troubleshooting, 602-603

BOOTP (Bootstrap Protocol), 359

Bootstrap Protocol. See BOOTP

Border Gateway Protocol. See BGP

bottlenecking, 59

bourne again shell. See bash

BPDU (Bridge Protocol Data Units), 377

branching devices, 463

bridges, 124

advantages/disadvantages, 128

ARP caches, 126

associations, checking, 125

broadcasts, handling, 125

data traffic, isolating, 126

Ethernet LANs, 125

MAC address entries, 126

multiport. *See* layer 2 switches

translation, 127

transparent, 127

wireless, 127

WLAN configurations, 422

bridging tables, defined, 124

broadband connections, 17

broadband modems/gateways, home networks, 23

broadband wireless access (BWA), 432

broadcast domains, 137, 195

broadcasts

bridges, 125

defined, 8

directed, 396

storms, 126

brute force attacks, 389

BSS (Basic Service Set), 415-416

buffer overflow attacks, 391

buffers, defined, 496

building distribution (optical networking), 470-472

building entrance structured cabling subsystem, 52

bursty data transmissions, 299

bus connections

AGP video card, 107

ATA, 107

Firewire, 106

ISA, 104

motherboard, 103-106

overview, 102

PCI, 104

USB, 105

bus topologies, 6-8

BWA (broadband wireless access), 432

C

cable modems, 23, 310

cables

CAT3, 58

CAT5 straight-through patch cables, configuring

crimping RJ-45 plug, 71

inserting wires into RJ-45 plug, 70

jacket stripping, 69

separating wire pairs, 70

CAT5e, 57

configuring straight-through patch cables, 69-71

four wire pairs, 61

test examples, 88, 92-93

CAT6, 32, 57

four wire pairs, 61

terminating horizontal links, 65-68

testing, 75

CAT6a, 57

CAT7, 59

color maps, 60

console, 201

crossovers, 33, 64

full channels, 71

industrial Ethernet, 627-628

link pulses, 34

links, 71

office-type LANs, 32-34

patch

configuring CAT5/5e straight-through, 69-71

defined, 56

horizontal cabling, 56

rollover, 201

STP, 51, 60

straight-through, 64, 69-71

structured

campus hierarchical topology, 53

EIA/TIA 568-B, 51

horizontal cabling, 54-56

standards, 51

subsystems, 52

telecommunications architecture, 52-53

TIA/EIA 568-A, 51

terminated, 55

testing, 71

ACR, 74

attenuation, 72

CAT6 links, 75-82

channel specifications, 72

delay skew, 74

ELFEXT, 74

NEXT, 72

propagation delay, 74

PSACR, 74

PSELFEXT, 74

PSNEXT, 73

return loss, 74

ThinNet, 6

transmit/receive pairs, aligning, 62-63

troubleshooting

cable stretching, 87

CAT5e test examples, 88, 92-93

failing to meet manufacturer specifications, 87

installation, 86

UTP, 51

balanced mode, 58

bottlenecking, 59

categories, 58-59

F/UTP, 84

full duplex gigabit Ethernet support, 59

high-performance, terminating, 60-61

RJ-45 modular plug example, 57

standards, 57

wire maps, 64

caches (ARP), 126

CAM (Content Addressable Memory), 136

campus area networks. *See* CANs

campus networks

data traffic analysis, 378

daily, 379

hourly, 379

weekly, 380

defined, 51, 122

- designing
 - access layer*, 356
 - core layer*, 354-355
 - data flow*, 356
 - distribution layer*, 355
 - load balancing*, 357-358
 - media selection*, 356-357
- DNS, 361
 - adding clients*, 363
 - hierarchy*, 362
 - local server administration*, 363
 - NS records*, 362
 - obtaining domain names*, 363
 - reverse*, 364
 - root servers*, 362
- fiber optics distribution, 472-475
- IP assignment with DHCP, 358-360
- Power over Ethernet (PoE)
 - benefits*, 367
 - networking hardware defined*, 368
 - PDs*, 368
 - PoE Plus*, 369
 - PSE*, 368
- SNMP, managing with, 365-367
- structured cabling hierarchical topology, 53
- switch configuration, 370
 - hostnames*, 371
 - line console*, 372-373
 - password protection*, 372
 - privileged mode*, 371
 - STP*, 377-378
- VLANs
 - membership assignments*, 370
 - Network Challenge software*, 376-377
 - static configuration*, 373-377
 - types*, 369
- CAN (controller area network), 619**
- CANs (campus area networks), 5**
- carrier sense multiple access with collision detection.**
See CSMA/CD protocol
- carrier sense multiple access/collision avoidance.** *See CSMA/CA*
- cat command (Linux), 568**
- CAT3 (category 3) cables, 58**
- CAT5 (category 5) cables, configuring straight-through patch cables**
 - jackets, stripping, 69-70
 - RJ-45 plugs, crimping, 71
 - wire pairs, separating, 70
- CAT5e (category 5 enhanced) cables, 57**
 - four wire pairs, 61
 - straight-through patch cables, configuring
 - inserting wires into RJ-45 plug*, 70
 - jacket, stripping*, 69
 - RJ-45 plug, crimping*, 71
 - wire pairs, separating*, 70
 - test examples, 92-93
 - certification report*, 91
 - FAIL result*, 88
 - PASS result*, 88
- CAT6 (category 6) cables, 32, 57**
 - four wire pairs, 61
 - horizontal link, terminating
 - bend-limiting strain relief boot*, 65, 68
 - jacket stripping*, 66
 - lacing tool*, 66
 - RJ-45 jack and lacing tool alignment*, 67
 - testing
 - ACR results*, 79
 - certification report*, 82
 - ELFEXT results*, 80
 - insertion loss*, 77
 - NEXT results*, 78
 - pair data*, 76
 - Power Sum NEXT results*, 79
 - PSACR results*, 79
 - PSELFTEXT results*, 80
 - return loss*, 81
 - setup*, 75
 - summary menu*, 75
 - wire-map test results*, 75
- CAT6a (category 6a) cables, 57**
- CAT7 (category 7) cables, 59**
- CBIR (committed burst information rate), 299**
- CBWFQ (class-based weighted fair queuing), 497**
- CCIE (Cisco Certified Internet Expert), 194**
- CCNA (Cisco Certified Network Associate), 194**
- CCNP (Cisco Certified Network Professional), 194**
- cd command (Linux), 569**

channel service unit/data service unit. *See* CSU/DSU

chgrp command (Linux), 576

chkconfig command (Linux), 602

chmod command (Linux), 573-575

chown command (Linux), 576

chromatic dispersion, 458

CIDR blocks (classless interdomain routing), 180

applying, 181

example, 181-182

CIP (Control and Information Protocol), 629

CIR (committed information rate), 298

Cisco 2500 series, 140-141

Cisco 2600 series, 140

Cisco 2800 series, 139

Cisco Catalyst 2960, 133

Cisco Certified Internet Expert. *See* CCIE

Cisco Certified Network Associate. *See* CCNA

Cisco Certified Network Professional. *See* CCNP

Cisco IOS (Internet Operating System). *See* IOS

Cisco Network Assistant. *See* CNA

Cisco VPN Client software, 337

Chile-VPN welcome menu, 334

connections, 335

handshake screen, 335

installing, 334

properties, 336

session statistics, 336

status, 334

cladding, 452

class D IP address ranges, 275

class network addresses, 240

class-based weighted fair queuing. *See* CBWFQ

classes

ATM, 306

IP addresses, 15, 170

classful addressing, 240

classful networks, 180, 246

classless interdomain routing. *See* CIDR blocks

CLI (command line interface), 194

client/server networks, defined, 511-512

clients

campus networks, adding to, 363

defined, 510

ftp, Linux, 595

RAS, configuring, 323-325

VPN remote, configuring

Cisco VPN Client software, 334-337

Mac OS X, 333

Windows Vista, 332

Windows XP, 332-333

clock rate command, 216

clusters, defined, 114

CNA (Cisco Network Assistant), 133

CODEC (coder/decoder), 490

collision domains, isolating, 136

color maps, 60

combo terminations, 102

command line (Linux), 563

command line interface. *See* CLI

command window, opening, 12

commands

access list permit ip any any, 400

arp -a, 127

clock rate, 216

commit, 269

commit and- quit, 270

configure, Juniper router hostnames, 268

configure terminal, 212, 371

copy run start, 235, 303

deny, 404

edit protocols, 269

edit routing-options static, 268

enable, 211

enable secret, 213, 372

encapsulation (encap), 297

encapsulation frame-relay, 302

frame-relay interface-dlci, 200, 302

help (?), 207

hostname, 212

int s0/0.1 point-to-point, 302

int tunnel0, 328

ip route, 231

ipconfig, IP address verification, 36

ipconfig /all, MAC addresses, 12

line ?, 213

Linux

chkconfig, 602

directory operations, 569-570

dmesg, 598

- file operations*, 571-573
- grep*, 585
- httpd restart*, 589
- httpd stop*, 589
- ifdown*, 591
- ifup*, 591
- ipconfig*, 590
- la system-config*, 604
- last*, 600
- listing files*, 565-566
- man*, 577
- mount*, 581-582
- netstat*, 603
- network start*, 592
- network stop*, 592
- nmap*, 601
- permissions/ownership*, 573-577
- pipe*, 585
- ps*, 579-580
- reboot*, 599
- route add default gw*, 592
- rpm -e*, 586
- rpm -i*, 586-587
- rpm -qa*, 584
- rpm -qf*, 585-586
- shortcuts*, 583
- shutdown*, 583
- shutdown -h now*, 583
- su*, 580
- system-config*, 604
- system-config-date*, 605
- system-config-firewall*, 605
- system-config-network*, 607
- system-config-packages*, 607
- system-config-printer*, 607
- system-config-services*, 609
- system-config-users*, 609
- unmount*, 583
- viewing file contents*, 567-569
- who*, 601
- net send*, 554
- net session*, 554
- netstat -a*, 392
- netstat -b*, 392
- netstat -r*, 228
- network*, 253
- no ip directed-broadcast*, 396
- no shutdown (no shut)*, 214
- ping*
 - hub-switch comparison*, 131-132
 - LANs, testing*, 35-36
 - Surveyor protocol analyzer*, 39-40
- route print*, 228
- router eigrp*, 259
- router igmp*, 246
- router ospf*, 253
- router RIP*, 240, 242
- routers, troubleshooting*, 218-220
- set protocols*, 270
- show, options*, 207
- show access-list*, 402
- show atm vc*, 308
- show controllers*, 216
- show controllers serial*, 216
- show flash*, 208
- show frame-relay PVC*, 304
- show interfaces brief, Juniper routers*, 267
- show ip interface brief*, 218-220
- show ip interface brief (sh ip int brief)*, 214, 218-220, 242
- show ip protocol (sh ip protocol)*, 242
- show ip route (sh ip route)*, 231-232
- show ip route igmp (sh ip route igmp)*, 249
- show ip route static (sh ip route static)*, 234
- show running config (sh run)*, 235, 303
- show startup config (sh start)*, 235
- show version*, 208
- snmp community public ro*, 365
- winipcfg, MAC addresses*, 13
- write memory (wr m)*, 235

commercial networks versus industrial networks, 619

commercial-off-the-shelf (COTS), 620

commit and- quit command, 270

commit command, 269

committed burst information rate (CBIR), 299

committed information rate. See CIR

computers

- BIOS boot sequence, configuring, 116
- bus connections
 - AGP video card*, 107
 - ATA*, 107
 - Firewire*, 106

- ISA, 104
- motherboard, 103-106
- overview, 102
- PCI, 104
- SCSI, 106
- USB, 105
- device drivers, 107
 - Mac OS X, 110-111
 - Windows Vista/XP, 108-109
- FAT, 114-115
- FAT32, 115
- memory, 112-113
- NTFS, 115
- routers
 - Cisco 2500 series, 140-141
 - Cisco 2600 series, 140
 - Cisco 2800 series, 139
 - gateways, 145
 - interface, 138
 - LANs, interconnecting, 138, 143-145
 - segments, 145
 - Windows 2003/2008 server domains, adding to, 522-526

Configuration BPDUs, 377

configuration mode (Juniper routers), 266-267

configure command, Juniper router hostnames, 268

configure terminal (conf t) command, 212, 371

configuring

- ACLs, 399-400
- ATM routers, 307
- BGP, 339-343
- BIOS boot sequence, 116
- Bluetooth, 430-431
- CAT5/5e straight-through patch cables
 - crimping RJ-45 plugs, 71
 - inserting wires into RJ-45 plug, 70
 - jacket stripping, 69
 - separating wire pairs, 70
- Fast Ethernet interfaces, 214
- Frame Relay networks, 299, 305
- HyperTerminal serial communications software, 203-204
- Juniper routers
 - hostnames, 268
 - IP address assignments, 268
 - OSPF, 270-271

- RIP, 269-270
- static routing, 268
- Linux networks
 - DNS, 597
 - etc/sysconfig/network-scripts, 594
 - Ethernet cards, 590
 - ftp clients, 595
 - ftp servers, 596
 - gateway addresses, 592
 - hostnames, 597
 - interface control, 591
 - IP address configuration, 590
 - loopbacks, 590
 - shutting down/starting interfaces, 592
 - SSH installations, 594-595
 - viewing interface configurations, 590
- network server account lockout policies, 552
 - connected users, viewing, 554
 - enabling user accounts, 554
 - locked out accounts, 553
 - messages to users, 555
- network server IP addresses, 521-522
- network servers, 514
- next hop IP addresses, 231
- office-type LANs
 - cabling, 32-34
 - devices, documenting, 30
 - IP addresses, 34
 - star topology connections, 32
- permissions, 533
 - Windows 2003, 539, 542-544
 - Windows 2008, 534-536, 539
- point-to-multipoint WLANs, 438
 - antenna site survey, 439
 - multipoint distribution, 440
 - point-to-point wireless links, 439-440
 - remote installations, 442
- point-to-point Frame Relay router connections, 302-304
- policies, 533
 - Windows 2003, 539, 542-544
 - Windows 2008, 534-536, 539
- RAS clients, 323-325
- RAS for Windows 2003 servers, 315-322
 - enabling RAS, 315
 - IP configuration, 321

- managing multiple servers, 318*
- modem configuration, 318, 320*
- protocol selection, 317*
- Routing and Remote Access Server Setup Wizard menu, 315*
- Routing and Remote Access window, 315*
- user accounts, 322*
- router serial interfaces, 214-216
- routes
 - EIGRP, 257, 259-261*
 - IGRP, 246-247, 249*
 - OSPF, 252, 254-256*
 - RIP, 242-244*
 - static routes, 234-235*
- SNMP, 365-367
- static routes, 234-235
- static VLANs, 373-377
- switches
 - campus networks, 370-371*
 - hostnames, 371*
 - line console, 372-373*
 - password protection, 372*
 - privileged mode, 371*
 - STP, 377-378*
- TFTP, 271-273
- VPNs
 - remote clients, 332-337*
 - router-to-router connections, 327-331*
 - servers, 331*
- Windows 2008 server, 521
- wireless networks, 27
- Z-Term serial communications software, 205

connection oriented protocol, 158

connections

- analog modem technologies, 309-310
- ATM, creating, 308
- broadband, 17
- bus
 - AGP video card, 107*
 - ATA, 107*
 - Firewire, 106*
 - ISA, 104*
 - motherboard, 103-106*
 - overview, 102*
 - PCI, 104*
 - SCSI, 106*
 - USB, 105*
- cable modems, 310
- Cisco VPN Client software, 335
- fiber connectorization, 466-467
- Frame Relay networks
 - creating, 301-302*
 - point-to-point router, 302-304*
- high-speed, 292
- ISDN, 310-312
- last miles, 432
- layer 3 network routers, 200
- office-type LAN star topology, 32
- point-to-point, Frame Relay clouds, 300
- PVCs (permanent virtual connections), 299
- remote access servers
 - client configuration, 323-325*
 - Windows 2003 server configuration, 315-322*
- router console ports, 201-202
- switch-56, 293
- VPN
 - remote clients, 332-337*
 - router-to-router, 326-331*
 - tunnel, 326*
- WAN lines
 - data channels, 292-293*
 - encoding formats, 295-298*
 - POP, 294*
 - T1 framing, 294-295*
- wireless networks, 27
- xDSL modems, 312-314

connectors (industrial networks), 628

console cables, 201

console port connections (routers)

- console cables, 201
- connectors, 201
- HyperTerminal serial communications software, configuring, 203-204
- rollover cables, 201
- RS-232 serial communications ports, 201
- settings, 202
- Z-Term serial communications software, configuring, 205

constant bit-rate class, 306

containers, defined, 524

Content Addressable Memory. See CAM

contiguous networks, 241
Control and Information Protocol. *See* CIP
control data, 620
controller area network. *See* CAN
controller level (industrial network hierarchy), 621
convergence, dynamic routing protocols, 237
converting
 IPv4 addresses to IPv6, 184-185
 numbers
 binary to decimal, 165-166
 binary to hexadecimal, 170
 decimal to binary, 166-168
 hexadecimal, 168-170
 hexadecimal to binary, 169
copy run start command, 235, 303
core layer (campus networks), 354-355
COTS (commercial-off-the-shelf), 620
country domains, 362
couplers, 464
cp command (Linux), 573
CPU utilization (industrial networks), 622
CQ (custom queuing), 497
cross connected devices, 33
cross-connects
 defined, 53
 horizontal, 53
 intermediate, 52
 main, 52
crossover cables, 64
crossovers, 33
crosstalk, 72
CSMA/CA (carrier sense multiple access/collision avoidance), WLANs, 416
CSMA/CD (carrier sense multiple access with collision detection) protocol, 10
CSU/DSU (channel service unit/data service unit), 294
custom queuing (CQ), 497
cut-through switching, 137

D

D4 framing, 294
daemons, 596
data channels, WANs, 292-293

Data Communications Equipment. *See* DCE
data encapsulation, 297-298
data flow, campus networks, 356
data link layer, OSI model, 123
data link negotiations, auto-negotiation protocol, 145
 advantages/disadvantages, 148
 full/half duplex, 146-147
 process, 146
data packets
 filtering, firewalls, 397
 FTP, 185
 “Hello” packets
 capturing, 276-277
 IP address ranges, 275
 parameters, 275
 RIDs, 276
 viewing, 277
 keepalive, 218
 layer 3 network exchange, 199
 OSPF “Hello” packets, 251
 sniffing, 436
 switching, 305
 unicast, 360
 unsecured
 captured packets, 407
 capturing packets setup, 405
 protecting, 408
 router connections, 406
 telnet session packets, 407
 telnetting to routers, 405
 user verification, 406
 VoIP, analyzing, 497
 acknowledgement, 499, 502
 call processor message, 499
 call processors call plans, 502
 collecting data packets, 498
 IP network handshaking, 504
 NBX call processor codes, 498
 PCM voice data, 499
 test setup, 502
Data Terminal Equipment. *See* DTE
data traffic, campus networks
 daily, 379
 hourly, 379
 weekly, 380

DataHighwayPlus protocol, 631

date/time, Linux, 605

DB-9 connectors, 201

DB-25 connectors, 201

DCE (Data Communications Equipment), 214

DDoS (Distributed Denial of Service) attacks, 396

DDR SDRAM (double-data-rate SDRAM), 113

DDR2 SDRAM (double-data-rate two SDRAM), 113

decimal-binary number conversions, 166-168

default gateways

- addresses, 196
- static routing, 227

delay skew, 74

Denial of Service attacks. *See* DoS

dense wavelength division multiplexing. *See* DWDM

deny command, 404

determinism, 6

- industrial Ethernet, 625
- industrial networks, 619

dev directory (Linux), 569

device drivers, 107

- Mac OS X, 110-111
- Windows Vista/XP, 108-109

device level (industrial network hierarchy), 620-621

Device Manager window, 108-109

device numbers, industrial networks, 623

Device Properties menu (Vista), 109

DeviceNet bus, 631

devices

- auto-negotiation, FLPs, 146
- cross connected, 33
- intelligent, 621
- interconnected link speeds. *See* auto-negotiation protocol
- LANs, interconnecting, 129

DFBs (distributed feedback) lasers, 462

DHCP (Dynamic Host Configuration Protocol), 317, 359

- IP assignment, campus networks, 358, 360
- servers, 513
- TCP packet transfers, 360-361

DHCP Offer packets. *See* MT Offer

dial-in access

- analog modem technologies, 309-310
- cable modems, 310
- ISDN, 310-312
- remote access servers
 - client configuration, 323-325*
 - Windows 2003 server configuration, 315-322*
- xDSL modems, 312-314

dictionary attacks, 389

digital signal (DS), 292

digital subscriber lines. *See* DSL

DIMM (dual in-line memory), 113

diode lasers. *See* DLs

Direct RAMBUS DRAM. *See* DRDRAM

direct sequence spread spectrum. *See* DSSS

directed broadcasts, 396

directory operations commands (Linux)

- cd, 569
- mkdir, 570
- pwd, 570
- rmdir, 570

Disabled state (STP), 378

discrete multitone (DMT) modulation, 313

dispersion

- compensation, 460-461
- dispersion compensating fiber, 461
- types, 458
- zero-dispersion wavelength, 459

distance (industrial networks), 623

distance vector protocols, 238-239

Distributed Denial of Service Attacks. *See* DDoS

distributed feedback lasers. *See* DFBs

distribution layer (campus networks), 355

dlci tags, 300

DLs (diode lasers), 461-462

dmesg command (Linux), 598

DMT (discrete multitone) modulation, 313

DNS (Domain Name Service). *See also* domains; names

- campus networks, 361
 - clients, adding, 363*
 - domain names, obtaining, 363*
 - hierarchy, 362*
 - local server administration, 363*
 - NS records, 362*

reverse, 364
root servers, 362
Linux configuration, 597
servers, 513

domain controllers, defined, 515

domains. *See also* DNS
broadcast, 137, 195
country, 362
top level, 362

DoS (Denial of Service) attacks, 395-396

dotted-decimal format, 171

double-data-rate SDRAM. *See* DDR SDRAM

double-data-rate two SDRAM. *See* DDR2 SDRAM

DRAM (dynamic random access memory), 113

DRDRAM (Direct RAMBUS DRAM), 113

DS (digital signal), 292

DS-0 to DS-3 data rates, 292

DSL (digital subscriber lines), 312

DSL modems, home networks, 25

DSSS (direct sequence spread spectrum), 417

DTE (Data Terminal Equipment), 214

DUAL finite state machine, 257

dual in-line memory. *See* DIMM

DWDM (dense wavelength division multiplexing), 451, 462

Dynamic Host Configuration Protocol. *See* DHCP

dynamic MAC address assignments, 134

dynamic random access memory. *See* DRAM

dynamic routing protocols, 236

- convergence, 237
- distance vector, 238-239
- features, 237
- link state, 239
- load balancing, 237
- metrics, 237
- path determination, 237

dynamic VLANs (virtual local area networks), 370

E

EAP (Extensible Authentication Protocol), 437

eBGP (external BGP), 339

ECC RAM (error-correcting code random access memory), 113

echo requests, 40

edit protocols command, 269

edit routing-options static command, 268

EDO RAM (Extended data-out RAM), 113

EF (entrance facilities). *See* building entrance structured cabling subsystem

efficiency (industrial networks), 622

EIA (Electronic Industries Alliance), 51

EIA/TIA 568-B, 51

- defined, 51
- structured cabling subsystems, 52
- wiring guidelines, 60

EIGRP (Enhanced Interior Gateway Routing Protocol)

- DUAL finite state machine, 257
- neighbor discovery recovery, 257
- Network Challenge software, 262
- protocol dependent modules, 257
- reliable transport protocol, 257
- route configuration, 257-261

EISA (Extended Industry Standard Architecture), 104

electromagnetic interference. *See* EMI

Electronic Industries Alliance. *See* EIA

ELFEXT (Equal Level FEXT), 74

ELTCTL (Equal Level Transverse Conversion Transfer Loss), 84

email servers, 512

EMI (electromagnetic interference), 60

enable command, 211

enable secret command, 213, 372

encapsulation (encap) command, 297

encapsulation frame-relay command, 302

encoding

- multilevel, 85
- WAN line connections
 - AMI, 295
 - B8ZS, 296
 - data encapsulation, 297-298

encryption, home networks, 28

endpoint PSE, 368

Enhanced Interior Gateway Routing Protocol. *See* EIGRP

Enterprise networks, defined, 143

entrance facilities (EF). *See* building entrance structured cabling subsystem

Equal Level FEXT. *See* ELFEXT

Equal Level Transverse Conversion Transfer Loss. *See* ELTCTL

ER (equipment room) structured cabling subsystem, 52

error thresholds, 137

error-correcting code random access memory. *See* ECC RAM

ESF (extended superframe framing), 295

ESS (Extended Service Set), 416

etc directory (Linux), 569

Ethernet

10GBASE-T

AXT, 83-84

signal balance, 84

signal transmission, 85-86

standard, 83

bridges, 125

CSMA/CD protocol, 10

Fast Ethernet, 59, 214

full duplex gigabit support, 59

gigabit, 59

industrial

cabling, 627-628

components, 627-628

determinism, 625

protocols, 628-630

switching, 627

topologies, 626-627

IP addresses

assigning, 15

classes, 15

format, 15

groups. See private addresses

host numbers, 16

IPv4, 15

network numbers, 16

Linux Ethernet cards, 590

MAC addresses, 11

retrieving, 12-13

samples, 14

viewing, 12

optical, 469-470

packets, 10-11

PoE

benefits, 367

campus networks, 367-369

networking hardware defined, 368

PDs, 368

PoE Plus, 369

PSE, 368

Ethernet addresses. *See* MAC addresses

Ethernet rings, 626

Ethernet/IP protocol, 629

events, 481

executable (x) permission (Linux), 575

extended ACLs, 399

Extended data-out RAM. *See* EDO RAM

Extended Industry Standard Architecture. *See* EISA

Extended Service Set. *See* ESS

extended superframe framing. *See* ESF

Extensible Authentication Protocol. *See* EAP

external BGP. *See* eBGP

F

F/UTP (foil over twisted-pair cabling), 84

far-end crosstalk. *See* FEXT

fast link pulses. *See* FLPs

fast-forward switching, 137

FastEthernet, 59

interface configuration, 214

port naming, 143

FAT (file allocation table), 114-115

FAT32, 115

fax servers, 513

FC fiber connectors, 466

FEXT (far-end crosstalk), 74

FHSS (frequency hopping spread spectrum), 417

fiber Bragg grating, 461

fiber cross-connects, 471

fiber optic networks, wavelengths, 452

fiber optics

advantages, 450

architectures

building distribution, 470-472

campus distribution, 472-475

- data rates*, 469
- defining optical networking*, 468-470
- fiber to the business*, 469
- fiber to the curb*, 469
- fiber to the desktop*, 469
- fiber to the home*, 469
- optical Ethernet*, 469-470
- standards*, 468
- armored, 628
- attenuators, 463, 478
- branching devices, 463
- cable loss example, 478
- cable losses, 476
- color code for 12 fibers in a bundle, 474
- components, 449
- connections and splicing, 465-466
- connector losses, 476
- connectorization, 466-467
- construction, 452
- couplers, 464
- designing, 475-478
- diode lasers, 461
- distance-limiting parameters
 - attenuation*, 457
 - dispersion*, 458-460
 - dispersion compensation*, 460-461
- distributed feedback lasers, 462
- DLs versus LEDs, 462
- environments, 475
- extra losses, 476
- extra margins, 478
- fiber strands, 453
- fibers, 463
- graded-index fibers, 454-455
- isolators, 463
- LEDs, 461
- light detectors, 464
- light reflection, 451
- light refraction, 451-452
- maintenance margins, 476
- mode field diameter, 456
- multimode fibers, 453
- numerical aperture, 453
- operational margins, 476
- optical fiber types, 453-454
- optical-line amplifiers, 464

- receive signal power, 476
- receiver sensitivity, 477
- safety, 479-480
- single-mode fibers, 455-457
- single-mode/multimode, compared, 456
- spectrum notation, 451
- splice losses, 476
- splitters, 463
- transmitter power output, 476
- troubleshooting, 481
- tunable lasers, 462
- types of fiber, 456
- vertical cavity emitting lasers, 462
- wavelength division multiplexers, 464
- fiber to the business (FTTB)**, 469
- fiber to the curb**. *See* FTTC
- fiber to the desktop**. *See* FTTD
- fiber to the home**. *See* FTTH
- fibers**, 463
- fieldbus protocols**, 618
- FIFO (first in, first out)**, 496
- file allocation table**. *See* FAT
- file structure (Linux)**
 - directory operations, 569-570
 - cd*, 569
 - mkdir*, 570
 - pwd*, 570
 - rmdir*, 570
 - file operation commands
 - cp*, 573
 - mv*, 572
 - rm*, 571
 - listing files
 - file permissions block attributes*, 566
 - install.log file attributes*, 566
 - ls*, 565
 - ls -l*, 565-566
 - ls -la*, 566-567
 - permissions/ownership, 577
 - chgrp*, 576
 - chmod*, 573-575
 - chown*, 576
 - viewing file contents, 569
 - cat*, 568
 - more*, 567

file system formats

- FAT, 114-115
- FAT32, 115
- NTFS, 115

File Transfer Protocol. *See* FTP

filtering

- MAC addresses, 28
- packets, firewalls, 397
- traffic, 354

Finisar Surveyor Demo protocol analyzer, 37

- installing, 38
- packets, captured, 38-42
- pinging computers, 39-40

Finisar-Shomiti utilization/errors strip chart, 344

firewalls, 396, 513

- ACLs, 398
 - applying to routers, 399-400*
 - blocking host IP addresses example, 403*
 - blocking SMB data packets example, 400-401*
 - extended, 399*
 - named access list example, 401-402*
 - standard, 399*
- attack prevention, 398
- defined, 28
- home networks, 28
- Linux, 605
- packet filtering, 397
- proxy servers, 397
- stateful, 397

Firewire connections, 106

first in, first out. *See* FIFO

flat networks, defined, 195

flooding, 137

FLPs (fast link pulses), 146

flyers, 456

foil over twisted-pair cabling. *See* F/UTP

forests, defined, 516

formatting

- file systems
 - FAT, 114-115*
 - FAT32, 115*
 - NTFS, 115*
- IP addresses, 15
- IPv6 addresses, 183

WAN line data encoding

- AMI, 295*
- B9ZS, 296*
- data encapsulation, 297-298*

forward domain name service, 361

forwarding frames, 137

Forwarding state (STP), 378

Foundation Fieldbus, 630

Foundation Fieldbus HSE protocol, 629

fractional T1 data rates, 293

fragment-collisions, 137

fragment-free switching, 137

Frame Relay clouds, 299

Frame Relay networks, 298

- configuring, 299, 305
- connections, creating, 301-302
- point-to-point connections, 300-304
- PVCs, 300
- subinterfaces, 300

Frame Relay PVCs, 299

frame-relay interface-dlci 200 command, 302

frames, forwarding, 137

frequency hopping spread spectrum. *See* FHSS

frequency of operation (RFID), 435

fstab file (Linux), 581

FTP (File Transfer Protocol), 185

- clients, Linux, 595
- data packets, 185
- servers, 513, 596

FTTB (fiber to the business), 469

FTTC (fiber to the curb), 469

FTTD (fiber to the desktop), 469

FTTH (fiber to the home), 469

full channels, cables, 71

full duplex, 59, 146-147

full duplex gigabit Ethernet support, 59

full IPv6 addresses, 182

fusion splicing, 465

G - H

gateway of last resort, 233

gateways, 145

- default, static routing, 227
- defined, 145

- layer 3 networks, 197
- VoIP, 488, 492
- GBICs (Gigabit Interface Converters), 471**
- gigabit Ethernet, 59**
- glass. *See* fibers
- graded-index fibers, 454-455
- grep command (Linux), 585
- grouping IP addresses. *See* private addresses
- groups, adding to Windows 2003/2008 server domains, 528-532
- GUI window (Linux), 561

- H.323 protocols, 489**
- half duplex, 146-147**
- hand-offs, 416**
- hardware addresses. *See* MAC addresses
- HART bus, 631**
- HCs (horizontal cross-connects), 53**
- HDLC (high-level data link control), 296**
- heavy duty industrial network areas, 627**
- “Hello” packets, 251**
 - capturing, 276-277
 - Hello intervals, 275
 - IP address ranges, 275
 - parameters, 275
 - RIDs, 276
 - viewing, 277
- help (?) command, 207**
- hexadecimal numbers, 168-170**
- HF (high-frequency), 435**
- hierarchies**
 - DNS, 362
 - industrial networks, 619, 622
 - controller level, 621*
 - device level, 620-621*
 - information level, 620*
- high-frequency (HF), 435**
- high-level data link control. *See* HDLC**
- high-speed connections, 292**
- high-speed serial interfaces. *See* HSSIs**
- history command (Linux), 583**
- holddowns, 245**
- home directory (Linux), 569**

- home networks**
 - appearance, 25
 - costs, 25
 - data speed, 25
 - equipment, 17
 - access points, 20*
 - broadband modems/gateways, 23*
 - cable modems, 23*
 - DSL modems, 25*
 - hubs, 18*
 - network adapters, 19*
 - routers, 20*
 - switches, 19*
 - wireless routers, 21*
 - home access, 26
 - implementation ease, 25
 - IP addressing, 29-30
 - planning, 25
 - public access, 26
 - routers, 17
 - security, 27-28
 - troubleshooting, 26
 - wired, advantages/disadvantages of, 17
 - wireless
 - advantages, 17*
 - configuring, 27*
 - connections, 27*
 - hotspots, 27*
 - range extenders, 27*
 - routers, 17*
 - standards, 17*
 - Wi-Fi Alliance, 17*
- hopping sequences, 417**
- horizontal cabling, 54**
 - patch cables, 56
 - structured cabling subsystem, 52
 - terminated, 55
- horizontal cross-connects. *See* HCs**
- host numbers, 16**
- hostname command, 212**
- hostnames**
 - Juniper router configuration, 268
 - Linux configuration, 597
 - routers, 212
 - switch configuration, 371

hosts
 defined, 402
 LANs, interconnecting, 129

hot standby configurations, 623

hotspots, defined, 27

HSSIs (high-speed serial interfaces), 292

httpd restart command (Linux), 589

httpd script, 588

httpd stop command (Linux), 589

httpd.conf file (Linux), 589

hubs
 broadcasting, 8
 defined, 8
 home networks, 18
 link lights, 33
 switches, compared, 130-132

hybrid echo cancellation circuits, 85

HyperTerminal serial communications software, configuring, 203-204

I

IANA (Internet Assigned Numbers Authority), 15

IANA website, 15

iBGP (internal BGP), 339

ICANN (Internet Corporation for Assigned Names and Numbers), 157

ICMP (Internet Control Message Protocol), 35, 163

ICs (Interconnect Fibers), 471

ICs (intermediate cross-connects), 52

IDA (Interface for Distributed Automation) protocol, 630

IDCs (Intermediate Distribution Closets), 471

IDE (Integrated Drive Electronics), 105

IEEE (Institute of Electrical and Electronics Engineers), 6

IEEE 1394, 105

IEEE OUI and company ID assignment database website, 14

IETF (Internet Engineering Task Force), 250

ifdown command (Linux), 591

ifup command (Linux), 591

IGMP (Internet Group Message Protocol), 164

IGP (Interior Gateway Protocol), 277

IGRP (Interior Gateway Routing Protocol)

administrative distance, 245

autonomous systems, 246

classful networks, 246

enabling, 246

enhanced. *See* EIGRP

holddowns, 245

metrics, 245

Network Challenge software, 250

OSPF, compared, 251

routes, configuring, 246-249

split horizons, 245

implicit messages, 629

inbound data traffic, 344

index-matching gel, 466

industrial Ethernet
 cabling, 627-628
 components, 627-628
 determinism, 625
 protocols, 628
Ethernet/IP, 629
Foundation Fieldbus HSE, 629
IDA, 630
MMS, 630
Modbus TCP, 630
Profinet, 630
 switching, 627
 topologies, 626-627

industrial networks
 characteristics, 619
 commercial networks, compared, 619
 determinism, 619
 distance/number of devices, 623
 efficiency, 622
 Ethernet
cabling, 627-628
components, 627-628
determinism, 625
protocols, 628-630
switching, 627
topologies, 626-627
 hierarchy, 619, 622
controller level, 621
device level, 620-621
information level, 620

interoperability, 623-624
message length, 624
open buses, 630-631
open industrial networking standard, 618
overview, 618-619
proprietary buses, 631
redundancy, 619
timing considerations, 622
topology/redundancy, 623
vendor support, 625

industrial, scientific, and medical (ISM), 417

Industry Standard Architecture. See ISA

information level (industrial network hierarchy), 620

information servers, 512

infrared lights, defined, 452

input ports, 33

inquiry procedure (Bluetooth), 430

insertion loss. See attenuation

install.log file attributes (Linux), 566

installing

- cables, troubleshooting, 86
- Cisco VPN Client software, 334
- network servers, 514
- SSH, 594-595
- Surveyor protocol analyzer, 38

Institute of Electrical and Electronics Engineers. See IEEE

int s0/0.1 point-to-point command, 302

int tunnel0 command, 328

Integrated Drive Electronics. See IDE

Integrated Services Digital Network. See ISDN

intelligent devices, 621

Interconnect Fibers. See ICs

interconnecting LANs

- bridges, 124-128
- layer 3 networks, 196
- OSI model, 122-124
- routers, 138, 143-145
- switches, 128-129

Interface for Distributed Automation. See IDA protocol

Interior Gateway Protocol. See IGP

Interior Gateway Routing Protocol. See IGRP

intermediate cross-connects. See ICs

Intermediate Distribution Closets. See IDCs

internal BGP. See iBGP

Internal Ethernet interface, 267

Internet Assigned Numbers Authority. See IANA

Internet Control Message Protocol. See ICMP

Internet Corporation for Assigned Names and Numbers. See ICANN

Internet data traffic, analyzing

- frame size distribution, 347
- network layer host tables, 346
- network layer matrix, 345-346
- utilization/errors strip chart, 344

Internet Engineering Task Force. See IETF

Internet Group Message Protocol. See IGMP

Internet layer (TCP/IP)

- ARP, 162
- ICMP, 163
- IGMP, 164
- IP, 162

Internet Operating System. See IOS

Internet Protocol. See IP

Internet routing, 338

- autonomous systems, 339
- BGP, configuring, 339-343
- Net-Challenge BGP configuration, 343-344

Internet Service Providers. See ISPs

Internetworking Packet Exchange. See IPX

interoperability, 621-624

Interrupt Request. See IRQ

intranets, defined, 16

intrusions (security)

- detecting, 404
- packet sniffing, 390
- password cracking, 389-390
- social engineering, 389
- viruses, 393
- vulnerable software, 391-393
- wireless vulnerabilities, 394
- worms, 393

inverse mask bits. See wild card bits

IOS (Internet Operating System), 194

- console connection confirmation, 206
- help command, 207
- show command options, 207
- show flash command, 208

show version command, 208
User EXEC mode, entering, 206

IP (Internet Protocol), 162

addressing

- assigning, 15, 173*
- campus network assignments, 358-360*
- CIDR blocks, 181-182*
- classes, 15, 170*
- defined, 15*
- experimental ranges, 275*
- format, 15*
- gateway of last resort, 233*
- groups. See private addresses*
- home networks, 29-30*
- host numbers, 16*
- IPv4, 15*
- IPv6, 182-185*
- Juniper interface assignments, 268*
- lease time, 359*
- Linux configuration, 590*
- name translation, 361*
- network numbers, 16*
- network server configuration, 521-522*
- next hop configuration, 231*
- non-internet routable, 173*
- octets, 172*
- office-type LANs configuration, 34*
- OSPF “Hello” packets, 275*
- private, 173*
- RAS configuration, 321*
- structure, 171*
- verifying, 36*

internetwork, defined, 16

security. *See* IPsec

telephony. *See* VoIP

tunnels, 325

ip route command, 231

ipconfig /all command, MAC addresses, 12

ipconfig command

IP address verification, 36

Linux, 590

IPng. See IPv6

IPsec (IP security), 334, 390

IPv4 (IP version 4) addressing, 15

assigning, 173

classes, 170

octets, 172

private IP addresses, 173

structure, 171

IPv6 (IP version 6) addressing

format, 183

full, 182

IPv4 conversions, 183-185

types, 184

IPX (Internetworking Packet Exchange), 345

IRQ (Interrupt Request), 106

ISA (Industry Standard Architecture), 104

ISDN (Integrated Services Digital Network), 310, 312

ISM (industrial, scientific, and medical), 417

isolating collision domains, 136

isolators, 463

ISPs (Internet Service Providers), 16

J

jitter, VoIP, 495-496

Juniper routers

configuration mode, 266-267

hostname configuration, 268

interfaces

- assigning IP addresses, 268*

- types, 266*

- viewing, 267-268*

JUNOS CLI User Guide website, 271

operating system (JUNOS), 262

operational mode

- command completion, 264*

- help command (?), 263*

- {master} mode, 263*

- network connectivity, 266*

- PICs, 266*

- prompts, 263*

- router configuration, viewing, 265*

- routing engines, 265*

- version information, 264*

OSPF configuration, 270-271

RIP configuration, 269-270

static route configuration, 268

JUNOS (Juniper router operating system), 262

configuration mode, 266-267

hostname configuration, 268

- interfaces, viewing, 267-268
- IP addresses, assigning to interfaces, 268
- JUNOS CLI User Guide* website, 271
- operational mode
 - command completion*, 264
 - help command (?)*, 263
 - {master mode}*, 263
 - network connectivity*, 266
 - PICs*, 266
 - prompts*, 263
 - router configuration, viewing*, 265
 - routing engines*, 265
 - version information*, 264
- OSPF configuration, 270-271
- RIP configuration, 269-270
- static route configuration, 268

just-in-time strategies, 625

K - L

keepalive packets, 218

kill/kill -9 commands (Linux), 580

Konqueror program (Linux), 583

L2TP (Layer 2 Tunneling Protocol), 331

LANs (local area networks)

- campus
 - access layer*, 356
 - core layer*, 354-355
 - data flow*, 356
 - data traffic analysis*, 378-380
 - daily*, 379
 - distribution layer*, 355
 - DNS*, 361-364
 - hourly*, 379
 - IP assignment with DHCP*, 358-360
 - load balancing*, 357-358
 - managing with SNMP*, 365-367
 - media selection*, 356-357
 - Power over Ethernet (PoE)*, 367-369
 - static VLAN configuration*, 373-377
 - switch configuration*, 370-373, 377-378
 - VLANs*, 369-370
 - weekly*, 380

- defined, 5
- Ethernet, 10
 - bridges*, 125
 - CSMA/CD protocol*, 10
 - industrial Ethernet*, 625-630
 - IP addresses*, 15-16
 - MAC addresses. See Ethernet; MAC addresses*
 - optical*, 469-470
 - packets*, 10-11
- fiber optics, 475
- interconnecting
 - bridges*, 124-128
 - layer 3 networks*, 196
 - OSI model*, 122-124
 - routers*, 138, 143-145
 - switches*, 128-129
- IP addresses, verifying, 36
- office-type
 - cabling*, 32-34
 - devices, documenting*, 30
 - IP addresses*, 34
 - star topology connections*, 32
- sizes, 194
- testing, 35-36
- topologies, 5
 - bus*, 6-8
 - mesh*, 9
 - star*, 8
 - token-ring*, 6
- VLANs
 - dynamic*, 370
 - membership assignments*, 370
 - static. See static VLANs*
 - types*, 369

last command (Linux), 600

last miles, 432

latency

- switches, 137
- VoIP, 496

layer 2 switches, 128

Layer 2 Tunneling Protocol. See L2TP

layer 3 networks, 195, 201

- components, 200
- data flow to/from gateways, 197
- data packet exchange, 199

- default gateway addresses, 196
- finding destination networks with subnet masks, 198
- LANs, interconnecting, 196
- next hop addresses, 199
- router connections, 200
- segments, 199

layers

- campus networks
 - access, 356
 - core, 354-355
 - distribution, 355
- OSI model, 123
- TCP/IP, 156
 - application, 157-158
 - Internet, 162-164
 - network interface, 164
 - transport, 158-162

LC fiber connectors, 466

LCL (Longitudinal Conversion Loss), 84

lean strategies, 625

Learning state (STP), 378

lease time, 359

LEDs (light-emitting diodes), 461-462

legacy protocols, 624

LF (low-frequency), 435

lib directory (Linux), 569

light detectors, 464

light duty industrial network areas, 627

light pipes. *See* fibers

light reflection, 451

light refraction, 451-452

light-emitting diodes. *See* LEDs

line ? command, 213

line connections, WANs

- data channels, 292-293
- encoding formats, 295-298
- POP, 294
- T1 framing, 294-295

line of demarcation, 294

linear network topology, industrial Ethernet, 626

link integrity tests, 33

link lights, 33

link pulses, 34

link state advertisements. *See* LSAs

link state protocols, 239

links, cables, 71

Linux

administration commands

- man*, 577
- mount*, 581-582
- ps*, 579-580
- shortcuts*, 583
- shutdown*, 583
- shutdown -h now*, 583
- su*, 580
- umount*, 583

application management

- Apache Web service installation*, 588-589
- file searches*, 585-586
- installed applications, viewing*, 584
- installing Red Hat applications*, 586-587
- Mozilla*, 588
- RPM man page*, 584
- uninstalling telnet applications*, 586

bash, 566

command line, 563

directories, 569

file structure

- directory operations*, 569-570
- file operations*, 571-573
- listing files*, 565-566
- permissions/ownership*, 573-577
- viewing file contents*, 567-569

fstab file, 581

Konqueror, 583

logging on, 560-561

main GUI window, 561

managing, 604

net masks, 590

network configuration

- DNS*, 597
- etc/sysconfig/network-scripts*, 594
- Ethernet cards*, 590
- ftp clients*, 595
- ftp servers*, 596
- gateway addresses*, 592
- hostnames*, 597
- interface control*, 591
- IP address configuration*, 590
- loopbacks*, 590

- shutting down/starting interfaces, 592*
- SSH installations, 594-595*
- viewing interface configurations, 590*
- root access, 560
- system config tools
 - date/time, 605*
 - firewalls, 605*
 - network menu, 607*
 - printers, 607*
 - services, 609*
 - software management, 607*
 - users, 609*
 - viewing, 604*
- troubleshooting
 - boot processes, 598-600*
 - boot services, 602-603*
 - security, 601*
 - users, 600-601*
- users, adding, 561-563
 - Create New User window, 562*
 - logout option, 564*
 - Red Hat User Manager window, 562*
- website, 565

Listening state (STP), 378

listing files commands (Linux)

- file permissions block attributes, 566
- install.log file attributes, 566
- ls, 565
- ls -l, 565-566
- ls -la, 566-567

lo (loopback), 590

load balancing

- campus networks, 357-358
- dynamic routing protocols, 237
- per-destination, 358
- per-packet, 358

local area networks. See LANs

logical addresses, 138

logical fiber maps, 472-473

long haul applications, 456

long-haul fiber optic systems, 475

Longitudinal Conversion Loss. See LCL

loopbacks

- defined, 228
- Linux, 590

lost+found directory (Linux), 569

low-frequency (LF), 435

ls command (Linux), 565

ls -l command (Linux), 565-566

ls -la command (Linux), 566-567

LSAs (link state advertisements), 251

M

MAC addresses (media access control)

- aging time, 134
- bridge tables, 126
- defined, 11
- dynamic, 134
- filtering, 28
- OUIs, 11
- retrieving, 12-13
- samples, 14
- secure, 134
- static, 134
- viewing, 12

Mac OS X

- device drivers, 110-111
- memory requirements, 112
- RAS client configuration, 325
- VPN client configuration, 333
- Z-Term serial communications software configuration, 205

macrobending, 457

main cross-connects. See MCs

man command (Linux), 577

managed switches

- aging time, 134
- benefits, 136
- broadcast domains, 137
- CAM, 136
- Cisco Catalyst 2960, 133
- flooding, 137
- frames, forwarding, 137
- IP addresses, configuring, 136
- isolating the collision domains, 136
- MAC address assignments, 134

Management Ethernet interface, 266

management information base. See MIB

managing

campus networks

Power over Ethernet (PoE), 367-369

SNMP, 365-367

Linux applications, 584

Apache Web service installation, 588-589

file searches, 585-586

installed applications, viewing, 584

installing Red Hat applications, 586-587

Mozilla, 588

RPM man page, 584

system config tools, 604-609

uninstalling telnet applications, 586

MANs (metropolitan area networks), 5

manufacturer specifications for cables, 87

Manufacturing Message Specification. *See* MMS

masks (subnet)

8 subnet division example, 177-178

binary/decimal equivalents, 176

CIDR notation, 180

creating, 173-175

prefix length notation, 180

router-to-router link example, 179-180

{master} mode (JUNOS), 263

Mbps (megabits per second), 32

MCs (main cross-connects), 52

mechanical splices, 466

media access control. *See* MAC addresses

megabits per second. *See* Mbps

membership, VLANs, 370

memory

amount installed, verifying, 113

operating system requirements, 112

types, 113

mesh topologies, LANs, 9

message length (industrial networks), 624

message overhead (industrial networks), 622

message quantity (industrial networks), 622

message type ACK. *See* MT ACK

message type discover. *See* MT Discover

message type request. *See* MT Request

messages (multicast), defined, 129

metrics

dynamic routing protocols, 237

IGRP, 245

metropolitan area networks. *See* MANs

MIB (management information base), 364

microbending, 457

midspan PSE, 368

MIMO (Multiple Input Multiple Output), 419

minimum ones density, 296

mkdir command (Linux), 570

mm (multimode) fibers, 473

MMS (Manufacturing Message Specification), 630

mnt directory (Linux), 569

modal dispersion, 458

ModBus, 631

Modbus TCP protocol, 630

mode field diameter (fibers), 456

modems

broadband, 23

cable, 23, 310

DSL, 25

RAS configuration, 318-320

xDSL, 312-314

more command (Linux), 567

motherboard bus connections, 103-106

mount command (Linux), 581-582

Mozilla, 588

MT ACK (message type ACK), 361

MT Discover (message type discover), 361

MT Offer (DHCP Offer packets), 361

MT Request (message type request), 361

MT-RJ fiber connectors, 466

multi-homed users, 338

multicast addresses, 164, 184

multicast messages, defined, 129

multilayer switches, 137-138

multilevel encoding, 85

multimode (mm) fibers, 453, 473

Multiple Input Multiple Output. *See* MIMO

multiplexing, 293

multiport bridges. *See* layer 2 switches

multiport repeaters. *See* hubs

mv command (Linux), 572

My Network Places connection

Windows 2000, 550-551

Windows XP, 546-549

N

name server records. *See* NS records

names. *See also* DNS

FastEthernet ports, 143

hostnames

Juniper router configuration, 268

Linux configuration, 597

routers, 212

switch configuration, 371

IP address translation, 361

serial ports, 143

nanometers (nm), 451

NAT (Network Address Translation), 29

ncftp (Linux), 595

NCP (network control protocol), 156

near end crosstalk. *See* NEXT

near-end testing, 72

neighbor discovery recovery (EIGRP), 257

net masks, 590

net send command, 554

net session command, 554

Net-Challenge software

BGP configuration, 343-344

router configuration privileged EXEC mode, 216-217

router configuration User EXEC mode, 209-211

NetBIOS, defined, 517

netstat command (Linux), 603

netstat -a command, 392

netstat -b command, 392

netstat -r command, 228

“Network,” 546

network adapters, home networks, 19

Network Address Translation. *See* NAT

network addresses, 138

Network Challenge software

EIGRP, 262

Frame Relay networks, 305

IGRP, 250

OSPF, 256-257

static routes, 236

static VLANs, 376-377

TFTP, 274-275

network command, 253

network congestion. *See* bottlenecking

Network connection (Windows Vista), verifying, 546

network control protocol (NCP), 156

network interface cards. *See* NICs

network interface layer (TCP/IP), 164

network latency, VoIP, 496

network layer, OSI model, 123

network mask parameter (“Hello” packets), 275

Network Neighborhood connection (Windows NT/98), verifying, 552

network numbers, defined, 16, 253

network operations centers. *See* NOCs

network servers

account lockout policies, configuring, 552

enabling user accounts, 554

locked out accounts, 553

messages to users, 555

viewing connected users, 554

adding, 513

computers, adding, 522-526

configuring, 514

groups, adding, 528-532

installing, 514

IP addresses, configuring, 521-522

My Network Places connection

Windows 2000, 550-551

Windows XP, 546-549

Network connection (Windows Vista), verifying, 546

Network Neighborhood connection (Windows NT/98), verifying, 552

network types

client/server, 511-512

peer-to-peer, 510-511

organizational units, adding, 528-532

permissions, 533-534

policies, 533-534

Windows 2003, 539, 542-544

Windows 2008, 534-536, 539

server types, 512-513

- users, adding, 526-527
- Windows 2003 servers, creating, 514
 - Configure DNS window*, 519
 - Create or Join Forest window*, 516
 - DNS warning*, 518
 - domain controller types*, 515
 - file directory locations*, 517
 - NetBIOS Domain Name window*, 517
 - New Domain Name window*, 516
 - options summary*, 520
 - Permissions window*, 519
 - Shared System Volume window*, 517
 - Welcome screen*, 515
- Windows 2008, configuring, 521
- network slowdowns**, 126
- network start command (Linux)**, 592
- network stop command (Linux)**, 592
- network types**
 - client/server, 511-512
 - peer-to-peer, 510-511
- Networking Challenge software, RIP**, 244-245
- New Technology File System**. *See* NTFS
- NEXT (near end crosstalk)**, 71-72
- next hop addresses**, 199, 231
- NICs (network interface cards)**
 - combo terminations, 102
 - defined, 11
 - Ethernets, 11
- NLOS (non line-of-sight)**, 432
- nm (nanometers)**, 451
- nmap command (Linux)**, 601
- no ip directed-broadcast command**, 396
- no shutdown (no shut) command**, 214
- NOCs (network operations centers)**, 344
- nominal velocity of propagation (NVP)**, 74
- non line-of-sight**. *See* NLOS
- non-internet routable IP addresses**, 173
- NS (name service) records**, 362
- NTFS (New Technology File System)**, 115
- numbering systems**
 - binary-decimal conversions, 165-166
 - binary-hexadecimal, 170
 - decimal-binary conversions, 166-168
 - hexadecimal, 168-170

- numerical aperture**, 453
- numerics**
 - office-type LANs, 32-33
 - optical Ethernet, 470
- NVP (nominal velocity of propagation)**, 74

O

- OCs (optical carriers)**, 292
- OFDM (orthogonal frequency division multiplexing), 802.11 WLANs**, 418
- office-type LANs, configuring**
 - cabling, 32-34
 - devices, documenting, 30
 - IP addresses, 34
 - star topology connections, 32
- open authentication**, 436
- open buses, industrial networks**, 630-631
- Open Shortest Path First**. *See* OSPF
- Open Shortest Path First Interior Gateway Protocol**. *See* OSPFIGP
- open system interconnect**. *See* OSI
- openssh applications**, 594
- operating systems (OS), MAC address retrieval**, 13
- operational mode (Juniper routers)**
 - command completion, 264
 - help command (?), 263
 - {master} mode, 263
 - network connectivity, 266
 - PICs, 266
 - prompts, 263
 - router configuration, viewing, 265
 - routing engines, 265
 - version information, 264
- optical carriers**. *See* OCs
- optical Ethernet**, 469-470
- optical networking**
 - advantages, 450
 - architectures
 - building distribution*, 470-472
 - campus distribution*, 472-475
 - data rates*, 469
 - defining optical networking*, 468-470
 - fiber to the business*, 469
 - fiber to the curb*, 469

- fiber to the desktop*, 469
- fiber to the home*, 469
- optical Ethernet*, 469-470
- standards*, 468
- armored fiber optics, 628
- attenuators, 463, 478
- branching devices, 463
- cable losses, 476-478
- connections and splicing, 465-466
- connector losses, 476
- construction, 452
- couplers, 464
- designing, 475-478
- diode lasers, 461
- distance-limiting parameters
 - attenuation*, 457
 - dispersion*, 458-460
 - dispersion compensation*, 460-461
- distributed feedback lasers, 462
- DLs versus LEDs, 462
- environments, 475
- extra losses, 476
- extra margins, 478
- fiber color code for 12 fibers in a bundle, 474
- fiber connectorization, 466-467
- fiber optic components, 449
- fiber strands, 453
- fibers, 463
- graded-index fibers, 454-455
- isolators, 463
- LEDs, 461
- light detectors, 464
- light reflection, 451
- light refraction, 451-452
- maintenance margins, 476
- mode field diameter, 456
- multimode fibers, 453
- numerical aperture, 453
- operational margins, 476
- optical fiber types, 453-454
- optical-line amplifiers, 464
- receive signal power, 476
- receiver sensitivity, 477
- safety, 479-480
- single-mode fibers, 455-457
- single-mode/multimode, compared, 456
- spectrum notation, 451
- splice losses, 476
- splitters, 463
- step-index fibers, 455
- transmitter power output, 476
- troubleshooting, 481
- tunable lasers, 462
- types of fiber, 456
- vertical cavity emitting lasers, 462
- wavelength division multiplexers, 464
- wavelengths, 452
- optical spectrums, defined, 452**
- optical time-domain reflectometers. See OTDRs**
- optical-line amplifiers, 464**
- organizational units, adding to Windows 2003/2008 server domains, 528-532**
- organizationally unique identifiers. See OUIs**
- orthogonal frequency division multiplexing. See OFDM**
- OSI (open system interconnect) model**
 - defined, 122
 - layers, 123
 - network problems, isolating, 124
- OSPF (Open Shortest Path First), 250**
 - advantages/disadvantages, 252
 - area 0, 254
 - areas, 251
 - “Hello” packets, 251
 - capturing*, 276-277
 - IP address ranges*, 275
 - parameters*, 275
 - RIDs*, 276
 - viewing*, 277
 - Juniper routers configuration, 270-271
 - LSAs, 251
 - Network Challenge software, 256-257
 - RIP/IGRP, compared, 251
 - routes, configuring, 252-256
 - VLSMs, 251
 - wild card bits, 253
- OSPFIGP (Open Shortest Path First Interior Gateway Protocol), 277**
- OTDRs (optical time-domain reflectometers), 481**
- OUIs (organizationally unique identifiers), 11**
- outbound data traffic, 344**

overloading, 29

ownership commands (Linux), 577

chgrp, 576

chmod, 573-575

chown, 576

P

Packet Internet Groper. See ping command

packets

captured, 38-42

defined, 10

Ethernets, 10-11

filtering, firewalls, 397

sequence numbers, 490

sniffing, 390, 436

switching, 305

SPI, 28

paging procedure (Bluetooth), 430

pair data, CAT6 link tests, 76

passwords

cracking, 389-390

home networks, 27

line console, 372-373

protection, routers privileged EXEC mode, 213

routers line console, 213

switches, 372

PAT (Port Address Translation), 29

patch cables

CAT5/5e straight-through, configuring

inserting wires into RJ-45 plug, 70

jacket, stripping, 69

RJ-45 plug, crimping, 71

wire pairs, separating, 70

defined, 56

horizontal cabling, 56

path determination, dynamic routing protocols, 237

payloads, 306

PBX (private branch exchange), 488

tie lines, replacing, 491-493

upgrading, 493-494

PC Card adapters, 20

PCI (Peripheral Component Interconnect), 103

PCM (pulse code modulation), 489

PDNs (public data networks), 298

PDs (Powered Devices), 368

peer-to-peer networks, defined, 510-511

peering, 339

per-destination load balancing, 358

per-packet load balancing, 358

performance bottlenecks, 59

Peripheral Component Interconnect. See PCI

permanent interfaces, 266

permanent virtual connections. See PVCs

permissions, configuring, 533-534

permissions commands (Linux), 573-577

physical addresses. See MAC addresses

physical fiber maps, 473-474

physical interface cards. See PICs

physical layer (OSI model), 123

physical layer cabling

10GBASE-T

AXT, 83-84

signal balance, 84

signal transmission, 85-86

standard, 83

CAT5e/5 straight-through patch cables, configuring

crimping RJ-45 plugs, 71

four wire pairs, 61

inserting wires into RJ-45 plug, 70

jacket stripping, 69

separating wire pairs, 70

CAT6 horizontal link cables, terminating, 65

bend-limiting strain relief boot, 65, 68

four wire pairs, 61

jacket stripping, 66

lacing tool, 66

RJ-45 jack and lacing tool alignment, 67

crossover cables, 64

defined, 51

STP, 60

straight-through, 64

structured

campus hierarchical topology, 53

EIA/TIA 568-B, 51

horizontal cabling, 54-56

standards, 51

subsystems, 52

telecommunications architecture, 52-53

TIA/EIA 568-A, 51

- testing, 71
 - ACR*, 74
 - attenuation*, 72
 - CAT6 links*, 75-82
 - channel specifications*, 72
 - delay skew*, 74
 - ELFEXT*, 74
 - NEXT*, 72
 - propagation delay*, 74
 - PSACR*, 74
 - PSELFEXT*, 74
 - PSNEXT*, 73
 - return loss*, 74
- transmit/receive pairs, aligning, 62-63
- troubleshooting
 - cable stretching*, 87
 - CAT5e test examples*, 88, 92-93
 - failing to meet manufacturer specifications*, 87
 - installation*, 86
- UTP
 - balanced mode*, 58
 - bottlenecking*, 59
 - categories*, 58-59
 - full duplex gigabit Ethernet support*, 59
 - high-performance*, 60-61
 - RJ-45 modular plug example*, 57
 - standards*, 57

piconets, 430

PICs (physical interface cards), 266

ping (Packet Internet Groper), 35

ping command

- hub-switch comparison, 131-132
- LANs, testing, 35-36
- Surveyor protocol analyzer, 39-40

pipe command (Linux), 585

planning home networks, 25

PLCs (programmable logic controllers), 622

PoE (Power over Ethernet)

- benefits, 367
- campus networks, 367-369
- networking hardware defined, 368
- PDs, 368
- PoE Plus, 369
- PSE, 368

point of presence. See POP

point-to-multipoint WLAN configuration, 438

- antenna site survey, 439
- multipoint distribution, 440
- point-to-point wireless links, 439-440
- remote installations, 442

point-to-point connections, Frame Relay clouds, 300

point-to-point Frame Relay router connections, configuring, 302-304

point-to-point physical interfaces, 301

Point-to-Point protocol. See PPP

Point-to-Point Tunneling Protocol. See PPTP

polarization mode dispersion, 458

policies

- account lockout policies, configuring, 552
 - enabling user accounts*, 554
 - locked out accounts*, 553
 - messages to users*, 555
 - viewing connected users*, 554
- configuring, 533
 - Windows 2003*, 539, 542-544
 - Windows 2008*, 534-536, 539

POP (point of presence), 294

Port Address Translation. See PAT

port-based VLANs, 369

ports

- assignment website, 158
- defined, 8
- FastEthernet, naming, 143
- input, 33
- serial, naming, 143
- straight through, 33
- uplink, 33
- well-known, 157

Power Sourcing Equipment. See PSE

Power Sum Alien Attenuation to Crosstalk Ratio. See PSAACRF

Power Sum Alien Near-End Cross-Talk. See PSANEXT

Power Sum NEXT. See PSNEXT

power-sum attenuation-crosstalk. See PSACR

Powered Devices. See PDs

PPP (Point-to-Point protocol), 296

PPTP (Point-to-Point Tunneling Protocol), 331

PQ (priority queueing), 497

prefix length notation, 180

presentation layer (OSI model), 123
print servers, 513
printers, Linux, 607
priority queuing (PQ), 497
private addresses, defined, 16
private branch exchange. *See* PBX
private IP addresses, 173
privileged EXEC mode (routers)
 entering, 211
 Fast Ethernet interface configuration, 214
 hostname, 212
 line console passwords, 213
 Net-Challenge software, 216-217
 password protection, 213
 serial interface configuration, 214-216
privileged mode
 defined, 211
 switches, 371
probing, 404
proc directory (Linux), 570
Profibus, 630
Profinet protocol, 630
programmable logic controllers. *See* PLCs
propagation delay, 74
proprietary buses, industrial networks, 631
protocol analyzer (Surveyor), 37
 captured packets, 38-42
 installing, 38
 pinging computers, 39-40
protocol-based VLANs, 370
protocols
 ARP, 39, 162
 auto-negotiation, 145
 advantages/disadvantages, 148
 FLPs, 146
 full/half duplex, 146-147
 process, 146
 BGP, 338
 configuring, 339-343
 Net-Challenge configuration, 343-344
 connection oriented, 158
 CSMA/CD, 10
 DataHighwayPlus, 631
 defined, 5

DHCP, 317
 IP assignment for campus networks, 358-360
 TCP packet transfers, 360-361
distance vector, 238-239
dynamic routing, 236
 convergence, 237
 distance vector, 238-239
 features, 237
 link state, 239
 load balancing, 237
 metrics, 237
 path determination, 237
EAP, 437
EIGRP
 DUAL finite state machine, 257
 neighbor discovery recovery, 257
 Network Challenge software, 262
 protocol dependent modules, 257
 reliable transport protocol, 257
 route configuration, 257-261
fieldbus, 618
FTP, data packets, 185
H.323, 489
HDLC, 296
ICMP, 35
IGP, 277
IGRP
 administrative distance, 245
 autonomous systems, 246
 classful networks, 246
 enabling, 246
 *enhanced. *See* EIGRP*
 holddowns, 245
 metrics, 245
 Network Challenge software, 250
 OSPF, compared, 251
 route configuration, 246-249
 split horizons, 245
industrial Ethernet, 628
 Ethernet/IP, 629
 Foundation Fieldbus HSE, 629
 IDA, 630
 MMS, 630
 Modbus TCP, 630
 Profinet, 630
IP, 162

- IPX, 345
- L2TP, 331
- legacy, 624
- link integrity tests, 33
- link state, 239
- OSPF, 250
 - advantages/disadvantages*, 252
 - area 0*, 254
 - areas*, 251
 - Hello packets*, 251, 275-277
 - Juniper router configuration*, 270-271
 - LSAs*, 251
 - Network Challenge software*, 256-257
 - RIP/IGRP, compared*, 251
 - routes, configuring*, 252-256
 - VLSMs*, 251
 - wild card bits*, 253
- OSPFIGP, 277
- PPP, 296
- PPTP, 331
- RAS, selecting, 317
- RIP
 - classful addressing*, 240
 - enabling*, 240
 - initializing*, 241
 - Juniper router configuration*, 269-270
 - network advertising*, 240
 - Networking Challenge software*, 244-245
 - OSPF versus*, 251
 - route configuration*, 242-244
 - routing loops*, 239
- RTCP, 490
- RTP, 490
- RTPS, 630
- SIP, 489
- Slotted Aloha, 435
- SNMP
 - configuring*, 365-367
 - managing campus networks via*, 365-367
 - MIB*, 364
- SSIP, 489
- static routing
 - configuring*, 234-235
 - data packet flow between LANs*, 231
 - default gateways*, 227
 - gateway of last resort*, 233
 - host PC routing tables*, 228
 - loopbacks*, 228
 - Network Challenge software*, 236
 - next hop IP addresses*, 231
 - routing table codes*, 232
 - three-router campus network*, 228, 232
 - two-router network*, 229
 - variable length subnet masking*, 231
- STP
 - BPDUs*, 377
 - states*, 378
- Surveyor protocol analyzer, 37
 - captured packets, examining*, 38-39
 - installing*, 38
 - packets, capturing*, 40-42
 - pinging computers*, 39-40
- TCP/IP, 16
 - application layer*, 157-158
 - development*, 156
 - Internet layer*, 162-164
 - layers*, 156
 - network interface layer*, 164
 - transport layer*, 158-162
- TFTP
 - configuring*, 271-273
 - Network Challenge software*, 274-275
- UDP, 161-162
- WAN routing, 337
- X.25, 298
- proxy servers, 397, 513**
- ps command (Linux), 579-580**
- PSAACRF (Power Sum Alien Attenuation to Crosstalk Ratio), 83**
- PSACR (power-sum attenuation-crosstalk), 74, 79**
- PSANEXT (Power Sum Alien Near-End Cross-Talk), 83**
- PSE (Power Sourcing Equipment), 368**
- PSELFEXT (Power Sum Equal Level Far-End Cross-Talk), 74**
- pseudorandom, 417**
- PSNEXT (Power Sum NEXT), 73**
- PSTN (public switched telephone network), 488**
- public data networks. See PDNs**
- public switched telephone network. See PSTN**
- pulse code modulation. See PCM**

pulse dispersion, 454
PVCs (permanent virtual connections), 299
 ATM, 306
 Frame Relay networks, 300
pwd command (Linux), 570

Q - R

QoS (Quality of Service), VoIP

jitter, 495-496
network latency, 496
queuing, 496-497

queuing

CQ, 497
PQ, 497
VoIP, 496-497

Radio Frequency Identification. *See* RFID

RADIUS (Remote Authentication Dial-In User Service), 437

RAM (Random Access Memory). *See* memory

range extenders, defined, 27

ranging, 310

RAS (remote access server)

client configurations, 323-325
Windows 2003 server configurations
 enabling RAS, 315
 IP configuration, 321
 modem configuration, 318, 320
 multiple servers, managing, 318
 protocol selection, 317
 Routing and Remote Access Server Setup Wizard
 menu, 315
 Routing and Remote Access window, 315
 user accounts, 322

Real-Time Control Protocol. *See* RTCP

Real-Time Protocol. *See* RTP

Real-Time Publish-Subscribe Protocol. *See* RTPS

reboot command (Linux), 599

receive (RX), 62

receive cable pairs, aligning, 62-63

received signal levels. *See* RSLs

Red Hat Package Manager. *See* RPM

redundancy (industrial networks), 619, 623

refractive indexes, 451

remote access servers. *See* RAS

Remote Authentication Dial-In User Service. *See* RADIUS

Resistive Power Discovery, 368

resolv.conf file (Linux), 597

return loss, 74

reverse DNS

 campus networks, 364
 defined, 361

RFID (Radio Frequency Identification), 432-433

 air interface protocol, 435
 backscatter, 432
 frequency of operation, 435
 tags, powering, 434

RIDs (router IDs), 276

ring topologies, industrial networks, 623

RIP (Routing Information Protocol), 239

 classful addressing, 240
 enabling, 240
 initializing, 241
 Juniper routers configuration, 269-270
 network advertising, 240
 Networking Challenge software, 244-245
 OSPF versus, 251
 route configuration, 242-244
 routing loops, 239

RJ-45 modular connectors, 32, 57

rm command (Linux), 571

rmdir command (Linux), 570

roaming, 416

rollover cables, 201

root access, 560

root directory (Linux), 570

root servers, DNS, 362

route add default gw command (Linux), 592

route flapping, 252

route print command, 228

routed networks. *See* layer 3 networks

router dead intervals (“Hello” packets), 275

router eigrp command, 259

router IDs. *See* RIDs

router igrp command, 246

- router ospf command, 253**
- router RIP command, 240-242**
- Router#, 211**
- Router(config)#, 213**
- Router(config-if)#, 214**
- Router(config-line)#, 213**
- Router(config-router)# prompt, 247**
- router-to-router VPN connections, 326-331**
- routers, 138**
 - ACLs, applying, 399-400
 - ATM configuration, 307
 - Cisco 2500 series, 140-141
 - Cisco 2600 series, 140
 - Cisco 2800 series, 139
 - console port connections
 - connectors, 201*
 - console cables, 201*
 - HyperTerminal serial communications software, 203-204*
 - rollover cables, 201*
 - RS-232 serial communications ports, 201*
 - settings, 202*
 - Z-Term serial communications software, 205*
 - Frame Relay point-to-point connection configuration, 302-304
 - gateways, 145
 - home networks, 17, 20
 - interface, 138, 242
 - Juniper
 - assigning IP addresses to interfaces, 268*
 - configuration mode, 266-267*
 - hostname configuration, 268*
 - interfaces, 266*
 - JUNOS CLI User Guide website, 271*
 - operating system (JUNOS), 262*
 - operational mode, 263-266*
 - OSPF configuration, 270-271*
 - RIP configuration, 269-270*
 - static route configuration, 268*
 - viewing interfaces, 267-268*
 - LANs, interconnecting, 138, 143-145
 - layer 3 networks
 - components, 200*
 - data flow to/from gateways, 197*
 - data packet exchange, 199*
 - default gateway addresses, 196*
 - finding destination networks with subnet masks, 198*
 - interconnecting LANs, 196*
 - next hop addresses, 199*
 - router connections, 200*
 - segments, 199*
 - privileged EXEC mode
 - entering, 211*
 - Fast Ethernet interface configuration, 214*
 - hostname, 212*
 - line console passwords, 213*
 - Net-Challenge software, 216-217*
 - password protection, 213*
 - serial interface configuration, 214-216*
 - segments, 145
 - terminal configuration mode, 212
 - troubleshooting, 217-220
 - uptime, 208
 - User EXEC mode
 - console connection confirmation, 206*
 - entering, 206*
 - help command, 207*
 - Net-Challenge software, 209-211*
 - show command options, 207*
 - show flash command, 208*
 - show version command, 208*
 - wireless, 17, 21
- routing**
 - Internet, 338
 - autonomous systems, 339*
 - BGP, configuring, 339-343*
 - Net-Challenge BGP configuration, 343-344*
 - static, Juniper routers, 268
 - WANs, 337
- Routing and Remote Access Server Setup Wizard, 315**
- Routing and Remote Access window, 315**
- Routing Information Protocol. See RIP**
- routing loops, 239**
- routing protocols**
 - dynamic, 236
 - convergence, 237*
 - distance vector, 238-239*
 - features, 237*
 - link state, 239*
 - load balancing, 237*
 - metrics, 237*
 - path determination, 237*

EIGRP

- DUAL finite state machine*, 257
- neighbor discovery recovery*, 257
- Network Challenge software*, 262
- protocol dependent modules*, 257
- reliable transport protocol*, 257
- routes, configuring*, 257-261

IGRP

- administrative distance*, 245
- autonomous systems*, 246
- classful networks*, 246
- enabling*, 246
- enhanced*. *See EIGRP*
- holddowns*, 245
- metrics*, 245
- Network Challenge software*, 250
- OSPF, compared*, 251
- routes, configuring*, 246-249
- split horizons*, 245

OSFPIGP, 277

OSPF, 250

- advantages/disadvantages*, 252
- area 0*, 254
- areas*, 251
- “Hello” packets*, 251, 275-277
- Juniper router configuration*, 270-271
- LSAs*, 251
- Network Challenge software*, 256-257
- RIP/IGRP, compared*, 251
- routes, configuring*, 252-256
- VLSMs*, 251
- wild card bits*, 253

RIP

- classful addressing*, 240
- enabling*, 240
- initializing*, 241
- Juniper router configuration*, 269-270
- network advertising*, 240
- Networking Challenge software*, 244-245
- OSPF, compared*, 251
- route configuration*, 242-244
- routing loops*, 239

static, 227

- configuring*, 234-235
- data packet flow between LANs*, 231
- default gateways*, 227

- gateway of last resort*, 233
- host PC routing tables*, 228
- loopbacks*, 228
- Network Challenge software*, 236
- next hop IP addresses*, 231
- routing table codes*, 232
- three-router campus network*, 228, 232
- two-router network*, 229
- variable length subnet masking*, 231

TFTP

- configuring*, 271-273
- Network Challenge software*, 274-275
- viewing*, 242

routing tables, 144, 228

RPM (Red Hat Package Manager), application management

- Apache Web service installation*, 588-589
- file searches*, 585-586
- installed applications, viewing*, 584
- installing Red Hat applications*, 586-587
- man page*, 584
- Mozilla*, 588
- uninstalling telnet applications*, 586

rpm -e command (Linux), 586

rpm -i command (Linux), 586-587

rpm -qa command (Linux), 584

rpm -qf command (Linux), 585-586

RS-232 serial communications ports, 201

RSLs (received signal levels), 463

RTCP (Real-Time Control Protocol), 490

RTP (Real-Time Protocol), 490

RTPS (Real-Time Publish-Subscribe Protocol), 630

RX (receive), 62

S

safety, optical networking, 479-480

SATA (Serial Advanced Technology Attachment), 106

sbin directory (Linux), 570

SC fiber connectors, 466

scattering, 457

SCSI (Small Computer System Interface), 105-106

SDH (Synchronous Digital Hierarchy), 468

SDRAM (Synchronous DRAM), 113

secure MAC address assignments, 134

secure session initiation protocol. *See* SSIP

Secure Shell. *See* SSH

security

ACLs, 396-398

blocking host IP addresses example, 403

blocking SMB data packets example, 400-401

extended, 399

named access list example, 401-402

routers, applying to, 399-400

standard, 399

DDoS attacks, 396

DoS attacks, 395-396

firewalls, 396

ACLs, 398-403

attack prevention, 398

home networks, 28

Linux, 605

packet filtering, 397

proxy servers, 397

stateful, 397

home networks, 27-28

intrusions

detecting, 404

packet sniffing, 390

password cracking, 389-390

social engineering, 389

viruses, 393

vulnerable software, 391-393

wireless vulnerabilities, 394

worms, 393

IPsec, 334, 390

Linux, troubleshooting, 601

passwords

cracking, 389-390

line console, 372-373

switches, 372

unsecured data packets

captured packets, 407

capturing packets setup, 405

protecting, 408

router connections, 406

telnet session packets, 407

telnetting to routers, 405

user verification, 406

VoIP, 497

WLANs, 435-438

segments

defined, 124, 145

layer 3 networks, 199

Serial Advanced Technology Attachment. *See* SATA

serial ports, naming, 143

server message block. *See* SMB

servers

application, 512

DHCP, 513

DNS, 513

email, 512

fax, 513

FTP, 513, 596

information, 512

network. *See* network servers

print, 513

proxy, 397, 513

remote access

client configuration, 323-325

Windows 2003 server configuration, 315-322

root, DNS, 362

types, 512-513

VPN configuration, 331

Web, 512

service set identifiers. *See* SSIDs

Session Initiation Protocol. *See* SIP

session layer (OSI model), 123

set protocols command, 270

sh ip int brief command, 218-220

sh ip route command, 232

sh run command, 303

shadowing, 623

sharekey authentication, 436

shielded twisted-pair. *See* STP

shortcuts (Linux administration commands), 583

show access-list command, 402

show atm vc command, 308

show command, options, 207

show controllers command, 216

show controllers serial command, 216

show flash command, 208

show frame-relay PVC command, 304

- show interfaces brief command, Juniper routers, 267
- show ip interface brief (sh ip int brief) command, 214, 218-220, 242
- show ip protocol (sh ip protocol) command, 242
- show ip route (sh ip route) command, 231
- show ip route igrp (sh ip route igrp) command, 249
- show ip route static (sh ip route static) command, 234
- show running config (sh run) command, 235
- show startup config (sh start) command, 235
- show version command, 208
- shutdown command (Linux), 583
- shutdown -h now command (Linux), 583
- signal transmission, 10GBASE-T, 85-86
- signal transport (VoIP), 489
- signaling, VoIP, 488-489
- signatures, 404
- Simple Network Management Protocol. *See* SNMP
- single mode (sm) fibers, 455-457, 473
- single points-of-failure, 623
- SIP (Session Initiation Protocol), 489
- site surveys, WLANs, 424, 426, 428
- Slotted Aloha protocol, 435
- slowdowns, 126
- sm (single mode) fibers, 473
- Small Computer System Interface. *See* SCSI
- smart devices, 621
- SMB (server message block), 398
- Smurf attacks, 395
- SNMP (Simple Network Management Protocol)
 - campus networks, 365-367
 - configuring, 365-367
 - MIB, 364
- snmp community public ro command, 365
- social engineering, 389
- SONETs (Synchronous Optical Networks), 468
- spam over Internet telephony. *See* spit
- Spanning-Tree Protocol. *See* STP
- spatial streams, 419
- spectrum notation, 451
- SPI (Stateful Packet Inspection), 28
- spit (spam over Internet telephony), 497
- split horizons, 245
- splitters, 463
- spoofs, 396
- SS7, 488
- SSH (Secure Shell), 408, 594-595
- SSIDs (service set identifiers)
 - 802.11 WLAN configuration, 421
 - home networks, 28
- SSIP (secure session initiation protocol), 489
- ST fiber connectors, 466
- standard ACLs, 399
- star topologies
 - defined, 8
 - LANs, 8
 - office-type LANs, 32
- stateful firewalls, 397
- Stateful Packet Inspection. *See* SPI
- static, 134
- static MAC address assignments, 134
- static routing
 - defined, 227
 - Juniper routers, 268
 - protocols
 - configuring, 234-235
 - data packet flow between LANs, 231
 - default gateways, 227
 - gateway of last resort, 233
 - host PC routing tables, 228
 - loopbacks, 228
 - Network Challenge software, 236
 - next hop IP addresses, 231
 - routing table codes, 232
 - three-router campus network, 228, 232
 - two-router network, 229
 - variable length subnet masking, 231
 - WANs, 337
- static VLANs
 - configuring, 373-377
 - defined, 370
 - Network Challenge software, 376-377
- statistical data, 620
- step-index fibers, 455
- store-and-forward switching, 137
- STP (shielded-twisted pair) cables, 51, 60
- STP (Spanning-Tree Protocol)
 - BPDU, 377
 - states, 378

straight-through cables, CAT5/5e patch cable configuration, 64

jacket stripping, 69

RJ-45 plugs

crimping, 71

inserting wires into, 70

wire pairs, separating, 70

straight-through ports, 33

streaming data, 164

stretching cables, 87

structured cabling

campus hierarchical topology, 53

EIA/TIA 568-B, defined, 51

horizontal cabling, 54

patch cables, 56

terminated, 55

standards, 51

subsystems, 52

telecommunications architecture, 52-53

TIA/EIA 568-A, 51

STS (Synchronous Transport Signals), 469

stubby areas, 337

su command (Linux), 580

subinterfaces

ATM routers, configuring, 307

Frame Relay networks, 300

subnet masks

8 subnet division example, 177-178

binary/decimal equivalents, 176

CIDR notation, 180

creating, 173-175

destination networks, finding, 198

prefix length notation, 180

router-to-router link example, 179-180

VLSM, 231, 251

subsystems, structured cabling, 52

supernetting, 180. *See also* CIDR blocks

SVCs (switched virtual circuits), 306

Switch(config)# prompt, 372

Switch(config-line)# prompt, 372

switch-56 connections, 293

switches

configuring

campus networks, 370-371

hostnames, 371

line console, 372-373

password protection, 372

privileged mode, 371

STP, 377-378

defined, 8

home networks, 19

industrial Ethernet, 627

LANs, interconnecting, 128

hosts, 129

hub comparison, 130-132

isolating the collision domains, 136

managed switches, 133-137

multilayer switches, 137-138

networking devices, 129

latency, 137

layer 2, 128

link lights, 33

managed

aging time, 134

benefits, 136

broadcast domains, 137

CAM, 136

Cisco Catalyst 2960, 133

flooding, 137

frames, forwarding, 137

IP addresses, configuring, 136

isolating the collision domains, 136

MAC address assignments, 134

multilayer, 137-138

star topologies, 8

SYN attacks, 395

Synchronous Digital Hierarchy. *See* SDH

Synchronous DRAM. *See* SDRAM

Synchronous Optical Networks. *See* SONETs

Synchronous Transport Signals. *See* STS

system config tools (Linux)

date/time, 605

firewalls, 605

network menu, 607

printers, 607

services, 609

software management, 607

users, 609

viewing, 604

System Properties menu (Vista), 108

system-config commands (Linux)

- date/time, 605
- firewalls, 605
- network menu, 607
- printers, 607
- services, 609
- software management, 607
- tools, viewing, 604
- users, 609

T

T1 framing, 294-295

T1 to T3 data rates, 292

T568A wiring guideline, 60

T568B wiring guideline, 60

tables

- bridging, defined, 124
- routing, 144, 228

tag-based VLANs, 370

tags

- dlci, 300
- RFID, powering, 434

TCA (Topology Change Notification Acknowledgement), 377

TCL (Transverse Conversion Loss), 84

TCN (Topology Change Notification), 377

TCOs (telecommunications outlets), 52

TCP (Transport Control Protocol), 158, 360-361

TCP/IP (Transmission Control Protocol/Internet Protocol), 16

- development, 156
- layers, 156
 - application, 157-158
 - Internet, 162-164
 - network interface, 164
 - transport, 158-162

TCTL (Transverse Conversion Transfer Loss), 84

TDM (time division multiplexing), 492

TE (telecommunications enclosure). See telecommunications closet structured cabling subsystem

Telco clouds, 293

telecommunications cabling architecture, 52-53

telecommunications closet structured cabling subsystem, 52

Telecommunications Industry Association. See TIA

telecommunications outlets. See TCOs

telecommunications room (TR). See telecommunications closet structured cabling subsystem

Telnet, defined, 584

terminal configuration mode (routers), 212

terminated cables, 55

terminating

- CAT6 horizontal link cables
 - bend-limiting strain relief boot, 65, 68
 - jacket stripping, 66
 - lacing tool, 66
 - RJ-45 jack and lacing tool alignment, 67
- high-performance UTP, 60-61

testing

- cables, 71
 - ACR, 74
 - attenuation, 72
 - CAT6 links, 75-82
 - channel specifications, 72
 - delay skew, 74
 - ELFEXT, 74
 - NEXT, 72
 - propagation delay, 74
 - PSACR, 74
 - PSELFEXT, 74
 - PSNEXT, 73
 - return loss, 74
 - LANs, 35-36
 - router interface configurations, 242
- TFTP (Trivial File Transfer Protocol)**
- configuring, 271
 - data transfer, 273
 - port 69 write request, 273
 - port assignment write request, 273
 - Network Challenge software, 274-275

ThinNet, 6

TIA (Telecommunications Industry Association), 51

TIA/EIA 568-A, 51

tie lines, defined, 492

time division multiplexing. See TDM

timestamps, 490

timing considerations, industrial networks, 622

TLDs (top level domains), 362
tmp directory (Linux), 570
token passing, 6
token-ring hubs, 6
token-ring topologies, 6
top level domains, 362
topologies
 bus topologies, 6, 8
 defined, 5
 industrial Ethernet, 626-627
 LANs, 5-9
 mesh topologies, 9
 ring topologies (industrial networks), 623
 star topologies, 8, 32
 token-ring topologies, 6
Topology Change Notification. See TCN
Topology Change Notification Acknowledgement. See TCA
totally stubby areas, 337
TR (telecommunications room). See telecommunications closet structured cabling subsystem
traffic (Internet)
 analyzing, 344
 frame size distribution, 347
 network layer host tables, 346
 network layer matrix, 345-346
 utilization/errors strip chart, 344
 data traffic, campus networks
 daily, 379
 hourly, 379
 weekly, 380
 filtering, 354
transceivers, 415
transient interfaces, 267
translation bridges, 127
Transmission Control Protocol/Internet Protocol. See TCP/IP
transmit (TX), 62
transmit cable pairs, aligning, 62-63
transparent bridges, 127
Transport Control Protocol. See TCP
transport layer (OSI model), 123
transport layer protocols
 data packet sequence, 159
 TCP, 158

TCP handshake, 160
terminating the TCP, 160-161
UDP, 161-162
Transverse Conversion Loss. See TCL
Transverse Conversion Transfer Loss. See TCTL
trees, defined, 515
Trivial File Transfer Protocol. See TFTP
troubleshooting
 cables
 CAT5e test examples, 88, 92-93
 failing to meet manufacturer specifications, 87
 installation, 86
 stretching, 87
 home networks, 26
 Linux
 boot processes, 598-600
 boot services, 602-603
 security, 601
 users, 600-601
 optical networking, 481
 routers, 217-220
 VPN tunnels, 331
tunable lasers, 462
TX (transmit), 62

U

U-NII (Unlicensed National Information Infrastructure), 418
UDP (User Datagram Protocol), 161-162
UDP/IP (User Datagram Protocol/Internet Protocol), 629
UHF (ultra-high frequency), 435
unicast addresses, 184
unicast packets, 360
Universal Serial Bus 1.1. See USB 1.1
Universal Serial Bus 2.0. See USB 2.0
unmount command (Linux), 583
unsecured data packets
 captured packets, 407
 capturing packets setup, 405
 protecting, 408
 router connections, 406
 telnet session packets, 407

- telnetting to routers, 405
- user verification, 406
- unshielded twisted-pair.** *See* UTP cables
- unspecified bit-rate class,** 306
- up arrow (Linux),** 583
- upgrading PBXs,** 493-494
- uplink ports,** 33
- uptime, routers,** 208
- USB 1.1 (Universal Serial Bus 1.1),** 104
- USB 2.0 (Universal Serial Bus 2.0),** 104
- USB connections,** 105
- user accounts, RAS configuration,** 322
- User Datagram Protocol.** *See* UDP
- User Datagram Protocol/Internet Protocol.** *See* UDP/IP
- User EXEC mode (routers)**
 - entering, 206
 - help command, 207
 - Net-Challenge software, 209-211
 - show command options, 207
 - show flash command, 208
 - show version command, 208

users

- Linux
 - adding to,* 561-563
 - managing,* 609
 - troubleshooting,* 600-601
- multi-homed, 338
- Windows 2003/2008 server domains, adding to, 526-527

usr directory (Linux), 570

UTP (unshielded twisted-pair) cables, 51

- balanced mode, 58
- bottlenecking, 59
- categories, 58-59
- F/UTP, 84
- full duplex gigabit Ethernet support, 59
- high-performance, terminating, 60-61
- RJ-45 modular plug example, 57
- standards, 57

V

- V.44/V.34 analog modem connection standard,** 309
- V.92/V.90 analog modem connection standard,** 309

- var directory (Linux),** 570
- var/log directory (Linux),** 600
- variable bit-rate real time class,** 306
- variable bit-rate/non-real time class,** 306
- variable length subnet masks.** *See* VLSMs
- VCCs (virtual channel connections),** 306
- VCIs (virtual channel identifiers),** 306
- VCs (virtual channels),** 308
- VCSELs (vertical cavity surface emitting lasers),** 462
- vendor support, industrial networks,** 625

verifying

- device drivers
 - Mac OS X,* 110-111
 - Windows Vista/XP,* 108-109
- memory amounts installed, 113
- My Network Places connection
 - Windows 2000,* 550-551
 - Windows XP,* 546-549
- Network connection (Windows Vista), 546
- Network Neighborhood connection (Windows NT/98), 552

vertical cavity surface emitting lasers. *See* VCSELs

VFLs (Visual Fault Locators), 481

viewing

- ATM interfaces, 308
- ATM virtual channels, 308
- file contents commands (Linux), 569
 - cat,* 568
 - more,* 567
- “Hello” packets, 277
- installed applications (Linux), 584
- Juniper router
 - configuring,* 265
 - interfaces,* 267-268
- Linux system-config tools, ls system-config, 604
- MAC addresses, 12
- routing protocols, 242

virtual channel connections. *See* VCCs

virtual channel identifiers. *See* VCIs

virtual channels. *See* VCs

Virtual LANs. *See* VLANs

virtual path connections. *See* VPCs

virtual path identifiers. *See* VPIs

Virtual Private Networks. *See* VPNs

virtual tie lines, 489

viruses, 393

Visual Fault Locators (VFLs), 481

VLANs (Virtual LANs), 369

dynamic, 370

membership assignments, 370

static

configuring, 373-377

defined, 370

Network Challenge software, 376-377

types, 369

VoIP, 497

VLSMs (variable length subnet masks), 231, 251

VoIP (Voice over IP)

data packet analyzation, 497

acknowledgement, 499, 502

call processor call plans, 502

call processor messages, 499

collecting data packets, 498

IP network handshaking, 504

NBX call processor codes, 498

PCM voice data, 499

test setup, 502

gateways, 488, 492

implementing

replacing PBX tie lines, 491-493

switching to IP telephony solutions, 494

upgrading PBXs, 493-494

overview, 488

packet sequence numbers, 490

PBX, 488

QoS

jitter, 495-496

network latency, 496

queuing, 496-497

security, 497

signal transport, 489

signaling, 488-489

SIP, 489

SSIP, 489

timestamps, 490

virtual tie lines, 489

VLANs, 497

VPCs (virtual path connections), 306

VPIs (virtual path identifiers), 306

VPNs (virtual private networks), 28, 325

remote client configurations

Cisco VPN Client software, 334-337

Mac OS X, 333

Windows Vista, 332

Windows XP, 332-333

router-to-router connections, 326-331

server configuration, 331

tunnel connections, 326

tunnels, troubleshooting, 331

vulnerable software attacks, 391-393

W

WANs (wide area networks), 5, 291

ATM, 305

classes, 306

connections, creating, 308

interfaces, viewing, 308

PVC interface, 306

router configuration, 307

router subinterface configuration, 307

VCI, 306

virtual channels, viewing, 308

VPI, 306

dial-in access

analog modem technologies, 309-310

cable modems, 310

ISDN, 310-312

remote access servers. See RAS

xDSL modems, 312-314

Frame Relay networks, 298

configuring, 299, 305

creating connections, 301-302

point-to-point connections, 300

point-to-point router connections, 302-304

PVCs, 300

subinterfaces, 300

Internet data traffic analyzation

frame size distribution, 347

network layer host tables, 346

network layer matrix, 345-346

utilization/errors strip chart, 344

- Internet routing, 338
 - autonomous systems*, 339
 - BGP, configuring*, 339-343
 - Net-Challenge BGP configuration*, 343-344
- line connections
 - data channels*, 292-293
 - encoding formats*, 295-298
 - POP*, 294
 - T1 framing*, 294-295
- routing, 337
- VPNs, 325
 - Cisco VPN Client software*, 334-337
 - Mac OS X clients*, 333
 - router-to-router connections*, 326-331
 - server configuration*, 331
 - tunnel connections*, 326
 - troubleshooting tunnels*, 331
 - Windows Vista clients*, 332
 - Windows XP clients*, 332-333
- war driving**, 394
- wavelengths (optical networking)**, 452
- WDM (wavelength division multiplexing)**, 451, 464
- Web servers**, 512
- websites**
 - ARIN, 173
 - IANA, 15
 - IEEE OUI and company ID assignment database, 14
 - JUNOS CLI User Guide*, 271
 - Linux, 565
 - port assignments, 158
- weighted fair queueing**. *See* WFQ
- weighted random early discard**. *See* WRED
- well-known ports**, 157
- WEP (wired equivalent privacy)**, 28, 394
- WFQ (weighted fair queuing)**, 496
- who command (Linux)**, 601
- Wi-Fi**. *See* wireless networks; WLANs
- Wi-Fi Alliance**, 17
- Wi-Fi Protected Access**. *See* WPA
- wide area networks**. *See* WANs
- wild card bits**, 253
- WiMAX (Worldwide Interoperability for Microwave Access)**, 432
- Windows 2000, verifying My Network Places connection**, 550-551

- Windows 2003 servers**
 - domains
 - adding computers, to*, 522-526
 - adding groups to*, 528-532
 - adding organization units to*, 528-532
 - adding users to*, 526-527
 - creating*, 514-519
 - policy configuration*, 539, 542-544
 - RAS configuration
 - enabling RAS*, 315
 - IP configuration*, 321
 - managing multiple servers*, 318
 - modem configuration*, 318, 320
 - protocol selection*, 317
 - Routing and Remote Access Server Setup Wizard menu*, 315
 - Routing and Remote Access window*, 315
 - user accounts*, 322
 - VPN server configuration, 331
- Windows 2008 servers**
 - configuring, 521
 - domains
 - adding computer to*, 522-526
 - adding groups to*, 528-532
 - adding organizational units*, 528-532
 - adding users*, 526-527
 - domain policy configuration*, 534-536, 539
- Windows NT/98, verifying Network Neighborhood connection**, 552
- Windows Vista**
 - device drivers, 108-109
 - Network connection, verifying, 546
 - RAS client configuration, 324
 - VPN client configuration, 332
- Windows XP**
 - device drivers, 108-109
 - My Network Places connection, verifying, 546-549
 - RAS client configuration, 324
 - VPN client configuration, 332-333
- winipcfg command, MAC addresses**, 13
- wire maps**, 64
- wire speed routing**, 138
- wired equivalent privacy**. *See* WEP
- wired networks**
 - advantages, 17
 - defined, 16

- disadvantages, 17
- troubleshooting, 26
- wireless bridges, 127**
- wireless local area networks. *See* WLANs**
- wireless networks**
 - advantages, 17
 - configuring, 27
 - connections, 27
 - defined, 16
 - hotspots, 27
 - range extenders, 27
 - routers, 17
 - security, 27-28
 - standards, 17
 - troubleshooting, 26
 - vulnerabilities, 394
 - Wi-Fi Alliance, 17
- wireless routers, 17, 21**
- Wireless-N adapters, 20**
- wiring guidelines, EIA/TIA 568B, 60**
- WLANs (wireless local area networks)**
 - 802.11 configuration, 420
 - access points, 422*
 - bridges, 422*
 - lost associations, 422*
 - range, extending, 424*
 - signals, 423*
 - site survey, 424-428*
 - SSIDs, 421*
 - 802.11 standard, 414
 - MAC layer, 415*
 - OFDM, 418-419*
 - physical layer, 415*
 - 802.11a standard, 420
 - 802.11b standard, 419-420
 - 802.11g standard, 419-420
 - 802.11i standard, 420
 - 802.11n standard, 419-420
 - 802.11r standard, 420
 - access points, 415
 - benefits, 414
 - Bluetooth, 429
 - configuring, 430-431*
 - inquiry procedure, 430*
 - paging procedure, 430*
 - piconets, 430*

- BSS, 415-416
- CSMA/CA, 416
- DSSS, 417
- ESS, 416
- FHSS, 417
- hand-offs, 416
- point-to-multipoint configuration, 438
 - antenna site survey, 439*
 - multipoint distribution, 440*
 - point-to-point wireless links, 439-440*
 - remote installations, 442*
- RFID, 433
 - air interface protocol, 435*
 - backscatter, 432*
 - frequency of operation, 435*
 - tags, powering, 434*
- roaming, 416
- security, 435-438
- security vulnerabilities, 394
- standard, 415
- WiMAX, 432
- Work Area Outlets. *See* WOs**
- work area structured cabling subsystem, 52**
- workstation, defined, 523**
- Worldwide Interoperability for Microwave Access. *See* WiMAX**
- worms, 393**
- WOs (Work Area Outlets), 53**
- WPA (Wi-Fi Protected Access), 28, 394, 437**
- WPA2, 394**
- WRED (weighted random early discard), 496**
- write memory (wr m) command, 235**
- wuftp (Washington University ftp server), 596**

X - Y - Z

- X.25 protocol, 298**
- xDSL modems, 312-314**
- XENPAKs (10 Gigabit Interface Adapters), 471**

- Z-Term serial communications software, configuring, 205**
- zero-dispersion wavelength, 459**