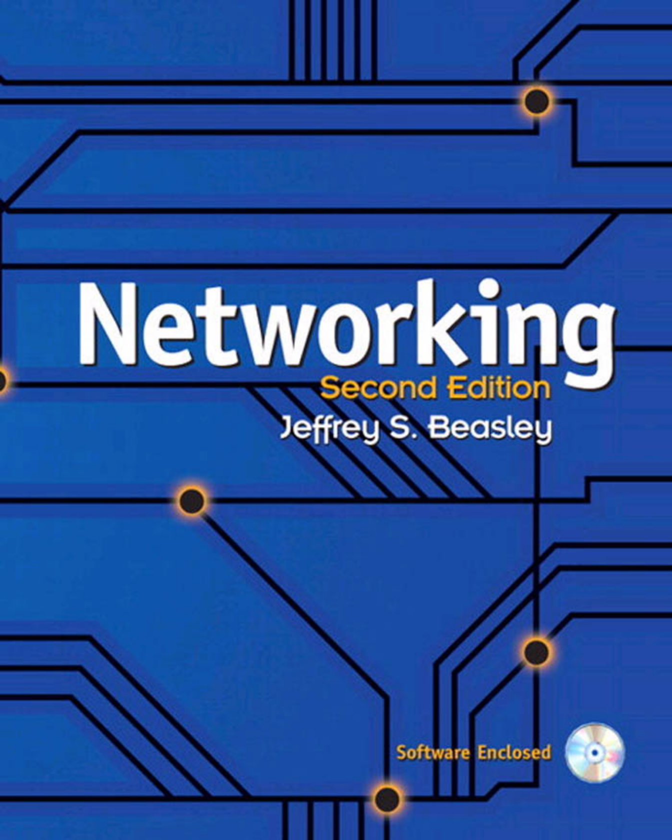


Networking

Second Edition

Jeffrey S. Beasley

Software Enclosed

Networking, Second Edition

Jeffrey S. Beasley

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

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.

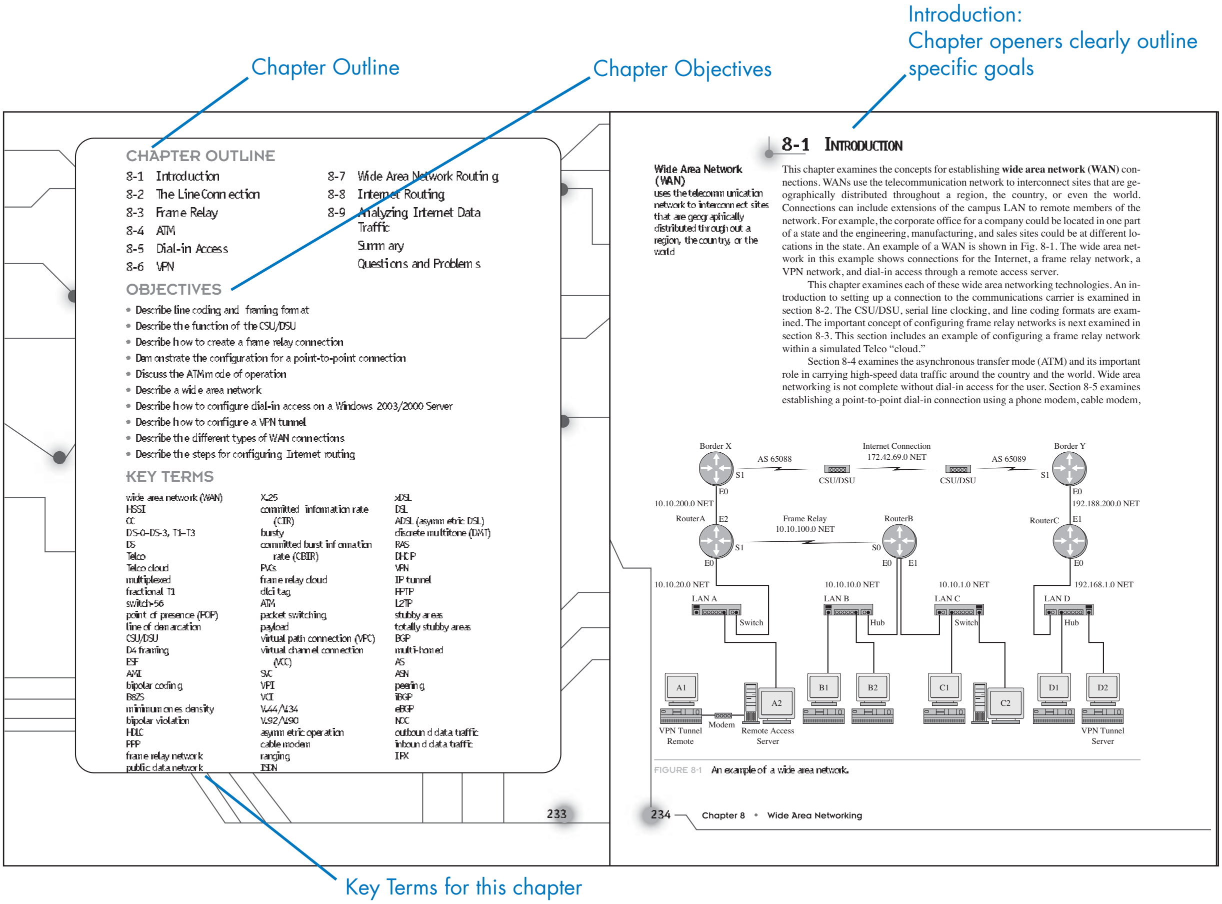
Organization of the Text

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 Objectives

Introduction:
Chapter openers clearly outline specific goals

Key Terms for this chapter

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
8-7 Wide Area Network Routing
8-8 Internet Routing
8-9 Analyzing Internet Data Traffic
Summary
Questions and Problems

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 mode 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)
HSSI
OC
DS-0–DS-3, T1–T3
DS
Telco
Telco cloud
multiplexed
fractional T1
switch-56
point of presence (POP)
line of demarcation
CSU/DSU
D4 framing
ESF
AMI
bipolar coding
B8ZS
minimum ones density
bipolar violation
HDLC
PPP
frame relay network
public data network
X.25
committed information rate (CIR)
bursty
committed burst information rate (CBIR)
PVCs
frame relay cloud
dlci tag
ATM
packet switching
payload
virtual path connection (VPC)
virtual channel connection (VCC)
SVC
VPI
VCI
V.44/V.34
V.92/V.90
asymmetric operation
cable modem
ranging
ISDN
xDSL
DSL
ADSL (asymmetric DSL)
discrete multitone (DMT)
RAS
DHCP
VPN
IP tunnel
PPTP
L2TP
stubby areas
totally stubby areas
BGP
multi-homed
AS
ASN
peering
iBGP
eBGP
NOC
outbound data traffic
inbound data traffic
IPX

233

8-1 Introduction

Wide Area Network (WAN)
uses the telecommunication network to interconnect sites that are geographically distributed throughout a region, the country, or the world

This chapter examines the concepts for establishing **wide area network (WAN)** connections. WANs use 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 Telco "cloud."

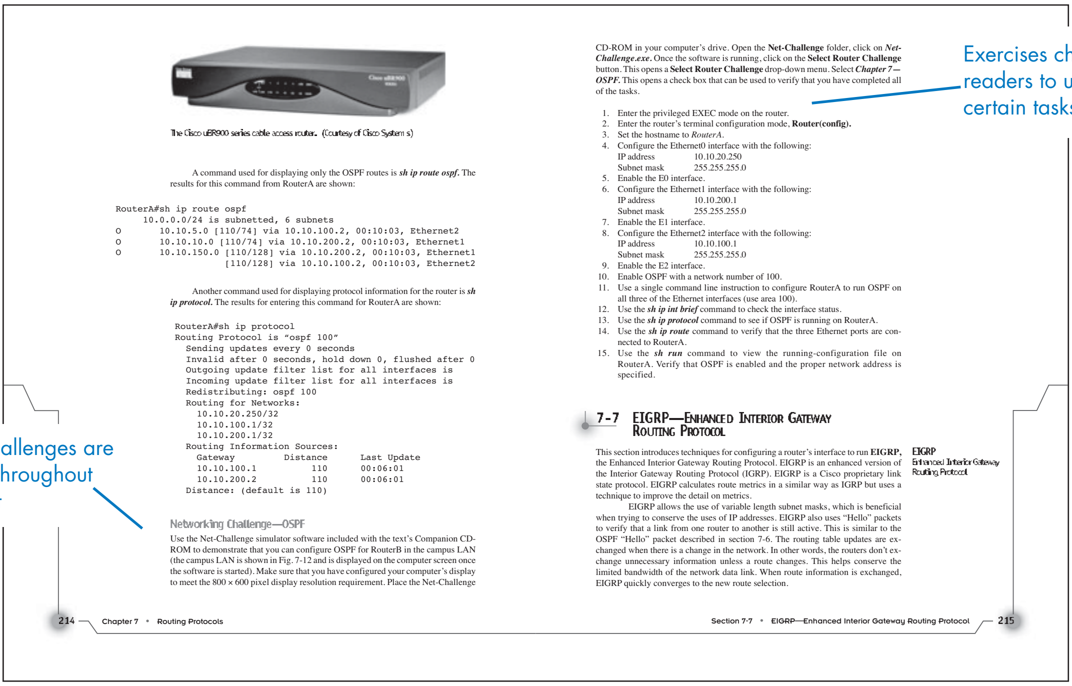
Section 8-4 examines the asynchronous transfer mode (ATM) and its important role in carrying high-speed data traffic around the country and the world. Wide area networking is not complete without dial-in access for the user. Section 8-5 examines establishing a point-to-point dial-in connection using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

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

234 Chapter 8 • Wide Area Networking

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 uBR900 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 0 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:
    10.10.20.250/32
    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)
```

Networking Challenge—OSPF

Use the Net-Challenge simulator software included with the text's Companion CD-ROM to demonstrate that you can configure OSPF for RouterB 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 10.10.200.1
   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 (use area 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
Enhanced Interior Gateway Routing Protocol

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

Net-Challenges are found throughout the text

FIGURE P-2

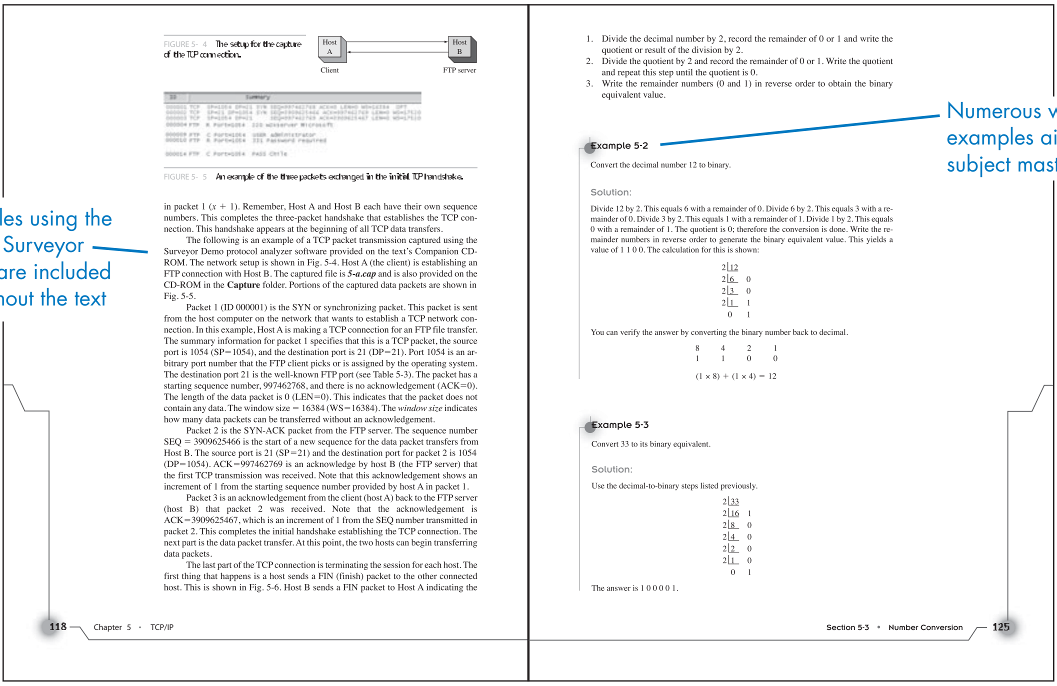


FIGURE 5-4 The setup for the capture of the TCP connection.

FIGURE 5-5 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-a.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 acknowledge 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

118 Chapter 5 • TCP/IP

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 1 1 0 0. The calculation for this is shown:

```
2|12
2|6   0
2|3   0
2|1   1
  0   1
```

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

8	4	2	1
1	1	0	0

$$(1 \times 8) + (1 \times 4) = 12$$

Example 5-3

Convert 33 to its binary equivalent.

Solution:

Use the decimal-to-binary steps listed previously.

```
2|33
2|16  1
2|8   0
2|4   0
2|2   0
2|1   0
  0   1
```

The answer is 1 0 0 0 0 1.

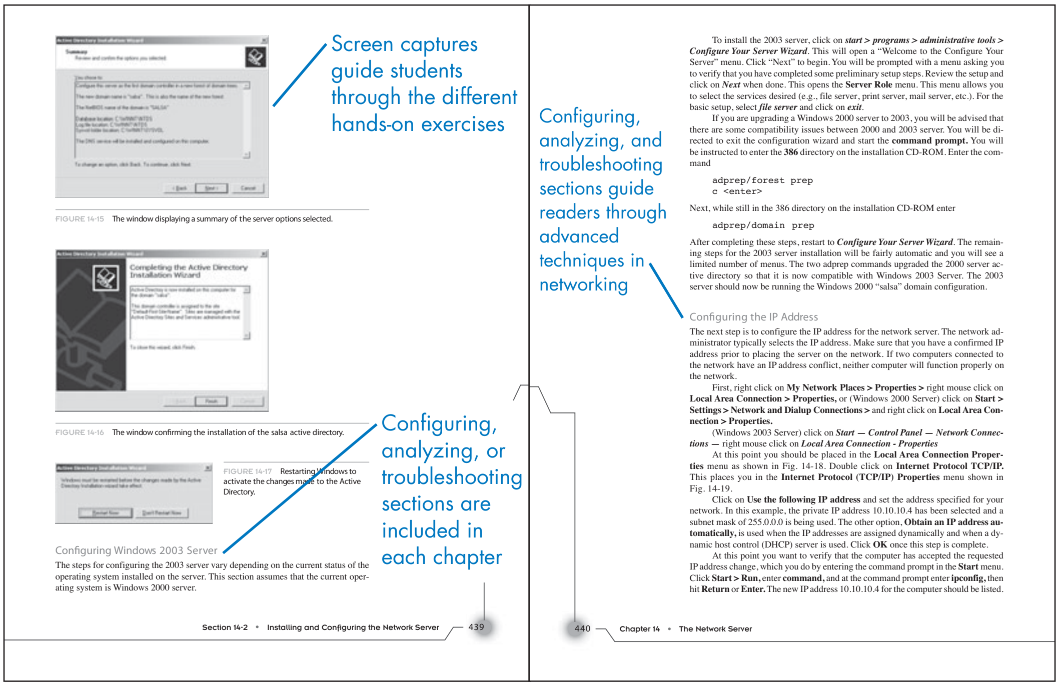
Section 5-3 • Number Conversion 125

Numerous worked-out examples aid in subject mastery

Examples using the Finisar Surveyor Demo are included throughout the text

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 14-15 The window displaying a summary of the server options selected.

FIGURE 14-16 The window confirming the installation of the salsa active directory.

FIGURE 14-17 Restarting Windows to activate the changes made to the Active Directory.

Configuring, analyzing, or troubleshooting sections are included in each chapter

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.

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

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

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 ***exit***.

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 configuration 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.

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 >** and 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.

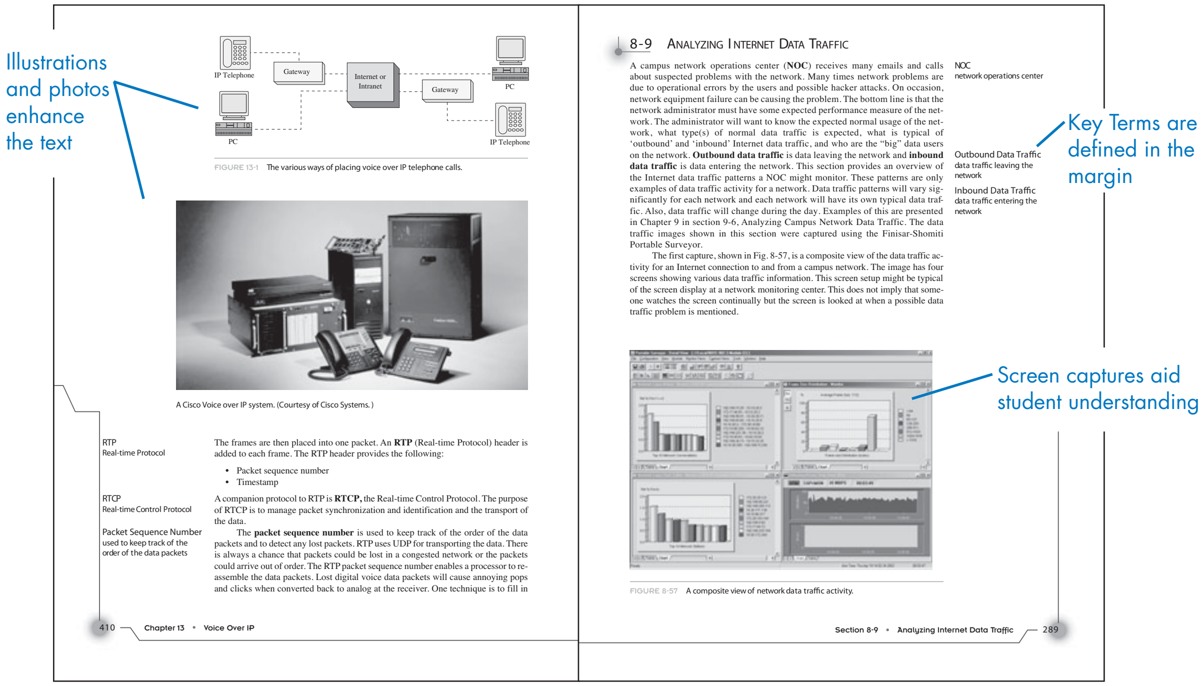
Click on **Use the following IP address** and set the address specified for your network. In this example, the private IP address 10.10.10.4 has been selected and a subnet mask of 255.0.0.0 is being used. The other option, **Obtain an IP address automatically,** is used when the IP addresses are assigned 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.

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

Key Terms are defined in the margin

Screen captures aid student understanding

FIGURE 13-1 The various ways of placing voice over IP telephone calls.

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

RTP
Real-time Protocol

RTCP
Real-time Control Protocol

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

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

- Packet sequence number
- Timestamp

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.

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

410 Chapter 13 • Voice Over IP

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.

NOC
network operations center

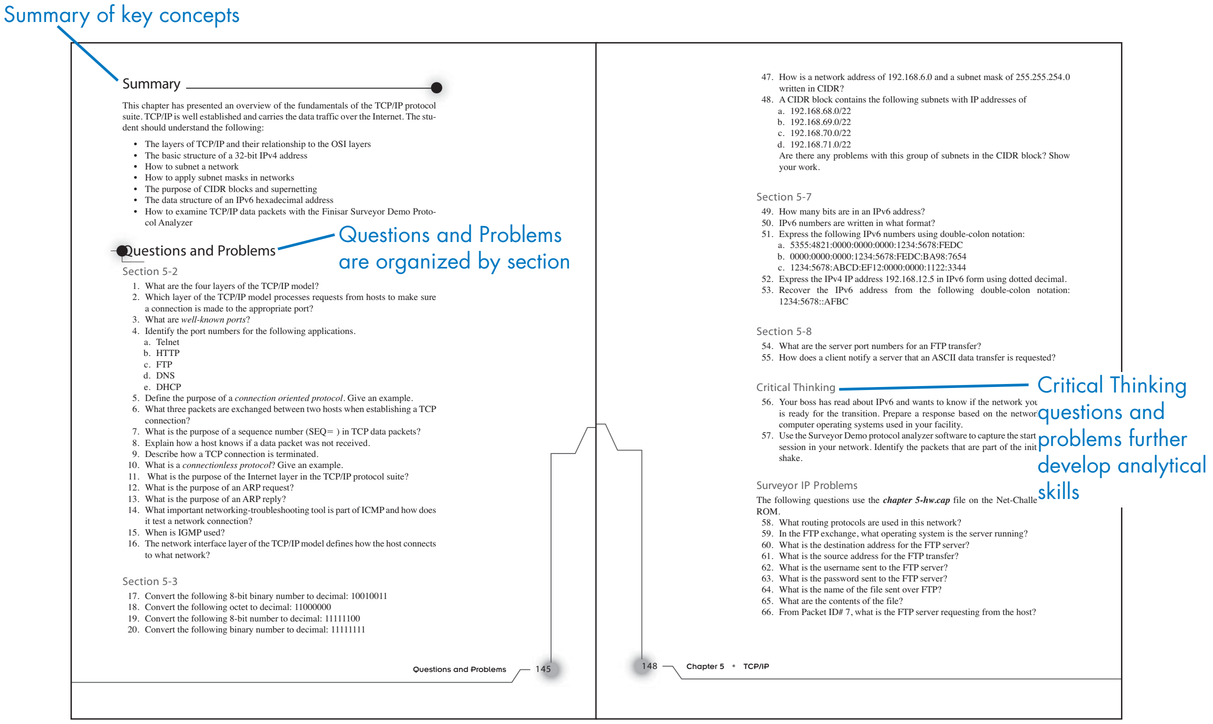
Outbound Data Traffic
data traffic leaving the network

Inbound Data Traffic
data traffic entering the network

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

Section 8-9 • Analyzing Internet Data Traffic 289

FIGURE P-5



Summary of key concepts

Questions and Problems are organized by section

Critical Thinking questions and problems further develop analytical skills

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

Questions and Problems 145

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. 192.168.68.0/22
    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:EF12:0000:0000:1122:3344
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 networ 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 init shake.

Surveyor IP Problems

The following questions use the ***chapter 5-hw.cap*** file on the Net-Challe 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?

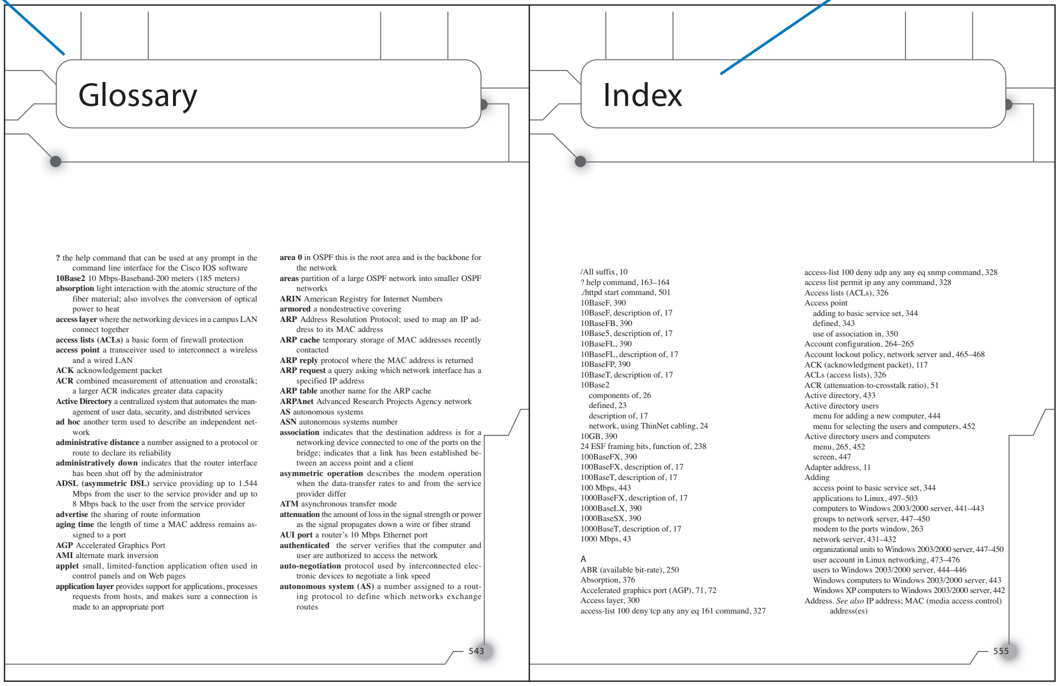
148 Chapter 5 • TCP/IP

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



Glossary

? the help command that can be used at any prompt in the command line interface for the Cisco IOS software
10Base2 10 Mbps-Baseband-200 meters (185 meters)
absorption light interaction with the atomic structure of the fiber material; also involves the conversion of optical power to heat
access layer where the networking devices in a campus LAN connect together
access lists (ACLs) a basic form of firewall protection
access point a transceiver used to interconnect a wireless and a wired LAN
ACK acknowledgement packet
ACR combined measurement of attenuation and crosstalk; a larger ACR indicates greater data capacity
Active Directory a centralized system that automates the management of user data, security, and distributed services
ad hoc another term used to describe an independent network
administrative distance a number assigned to a protocol or route to declare its reliability
administratively down indicates that the router interface has been shut off by the administrator
ADSL (asymmetric DSL) service providing up to 1.544 Mbps from the user to the service provider and up to 8 Mbps back to the user from the service provider
advertise the sharing of route information
aging time the length of time a MAC address remains assigned to a port
AGP Accelerated Graphics Port
AMI alternate mark inversion
applet small, limited-function application often used in control panels and on Web pages
application layer provides support for applications, processes requests from hosts, and makes sure a connection is made to an appropriate port
area 0 in OSPF this is the root area and is the backbone for the network
areas partition of a large OSPF network into smaller OSPF networks
ARIN American Registry for Internet Numbers
armored a nondestructive covering
ARP Address Resolution Protocol; used to map an IP address to its MAC address
ARP cache temporary storage of MAC addresses recently contacted
ARP reply protocol where the MAC address is returned
ARP request a query asking which network interface has a specified IP address
ARP table another name for the ARP cache
ARPAnet Advanced Research Projects Agency network
AS autonomous systems
ASN autonomous systems number
association indicates that the destination address is for a networking device connected to one of the ports on the bridge; indicates that a link has been established between an access point and a client
asymmetric operation describes the modem operation when the data-transfer rates to and from the service provider differ
ATM asynchronous transfer mode
attenuation the amount of loss in the signal strength or power as the signal propagates down a wire or fiber strand
AUI port a router's 10 Mbps Ethernet port
authenticated the server verifies that the computer and user are authorized to access the network
auto-negotiation protocol used by interconnected electronic devices to negotiate a link speed
autonomous system (AS) a number assigned to a routing protocol to define which networks exchange routes

543

Index

/All suffix, 10
? help command, 163–164
./httpd start command, 501
10BaseF, 390
10BaseF, description of, 17
10BaseFB, 390
10Base5, description of, 17
10BaseFL, 390
10BaseFL, description of, 17
10BaseFP, 390
10BaseT, description of, 17
10Base2
  components of, 26
  defined, 23
  description of, 17
  network, using ThinNet cabling, 24
10GB, 390
24 ESF framing bits, function of, 238
100BaseFX, 390
100BaseFX, description of, 17
100BaseT, description of, 17
100 Mbps, 443
1000BaseFX, description of, 17
1000BaseLX, 390
1000BaseSX, 390
1000BaseT, description of, 17
1000 Mbps, 43

A
ABR (available bit-rate), 250
Absorption, 376
Accelerated graphics port (AGP), 71, 72
Access layer, 300
access-list 100 deny tcp any any eq 161 command, 327
access-list 100 deny udp any any eq snmp command, 328
access list permit ip any any command, 328
Access lists (ACLs), 326
Access point
  adding to basic service set, 344
  defined, 343
  use of association in, 350
Account configuration, 264–265
Account lockout policy, network server and, 465–468
ACK (acknowledgment packet), 117
ACLs (access lists), 326
ACR (attenuation-to-crosstalk ratio), 51
Active directory, 433
Active directory users
  menu for adding a new computer, 444
  menu for selecting the users and computers, 452
Active directory users and computers
  menu, 265, 452
  screen, 447
Adapter address, 11
Adding
  access point to basic service set, 344
  applications to Linux, 497–503
  computers to Windows 2003/2000 server, 441–443
  groups to network server, 447–450
  modem to the ports window, 263
  network server, 431–432
  organizational units to Windows 2003/2000 server, 447–450
  user account in Linux networking, 473–476
  users to Windows 2003/2000 server, 444–446
  Windows computers to Windows 2003/2000 server, 443
  Windows XP computers to Windows 2003/2000 server, 442
Address. *See also* IP address; MAC (media access control) address(es)

555

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

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

11-1 INTRODUCTION

WLAN
Wireless local area network

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

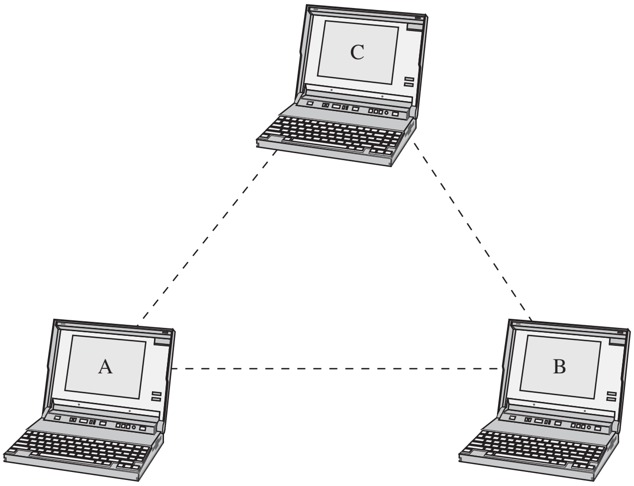


FIGURE 11-1 An example of the independent Basic Service Set or "ad hoc" network.

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

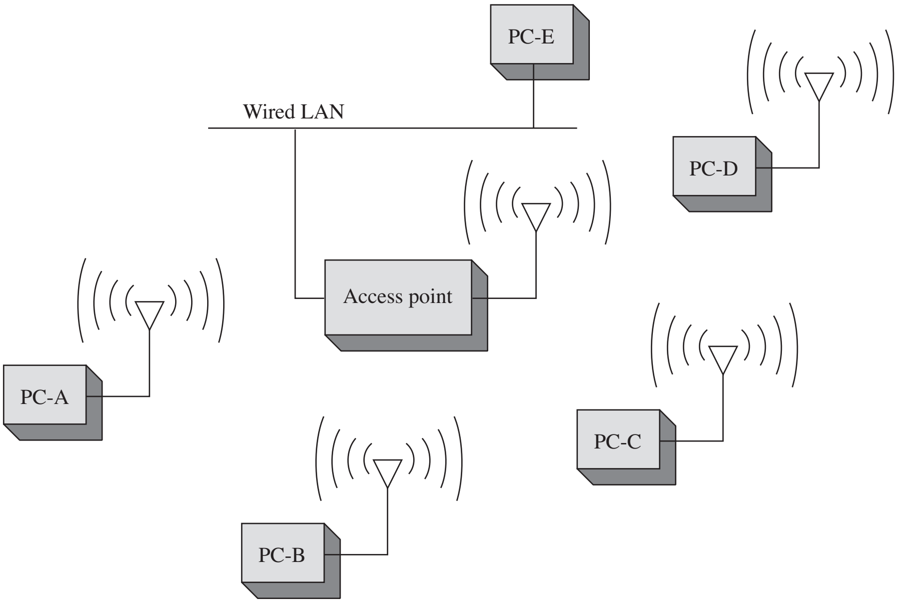


FIGURE 11-2 Adding an access point to the Basic Service Set.

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.

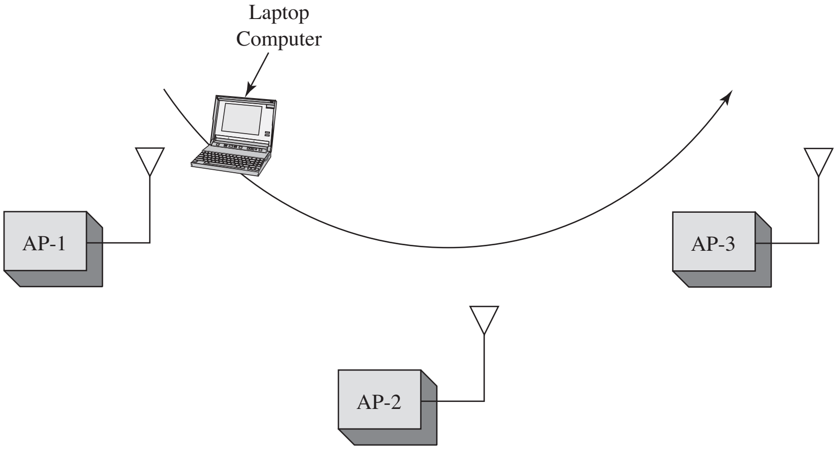


FIGURE 11-3 An example of an Extended Service Set used for increased user mobility.

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

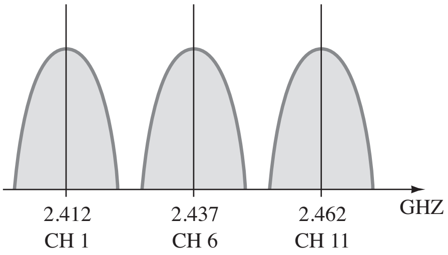


FIGURE 11-4 An example of the three channels in the DSSS spectrum.

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.

OFDM
Orthogonal frequency division multiplexing

U-NII
Unlicensed National Information Infrastructure

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.

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.

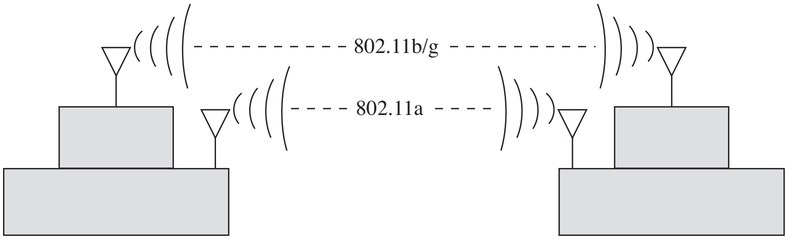


FIGURE 11-5 An example of an 802.11a installation and an 802.11b link running alongside each other.

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.

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

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.

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

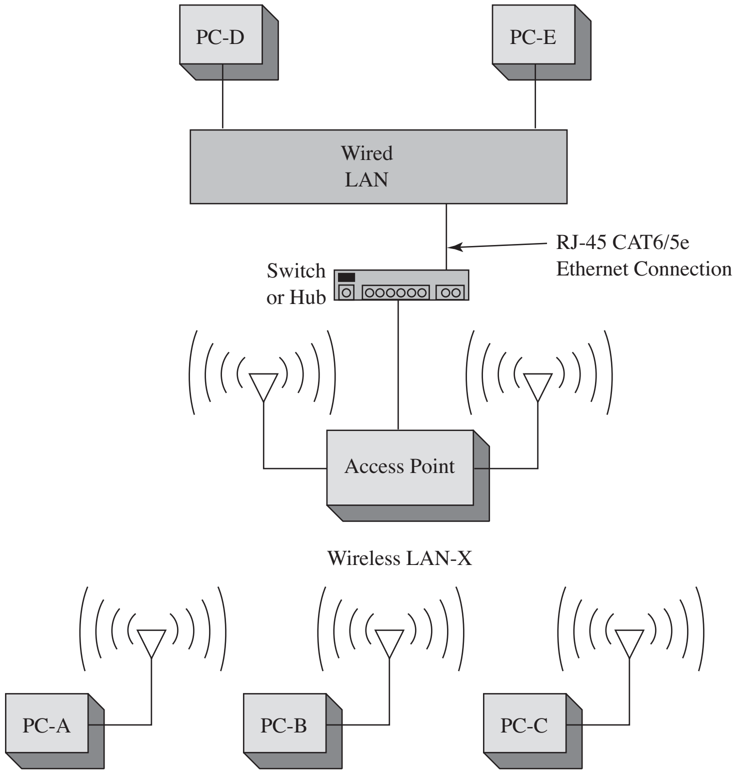


FIGURE 11-6 The setup for a basic wireless LAN.

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?"

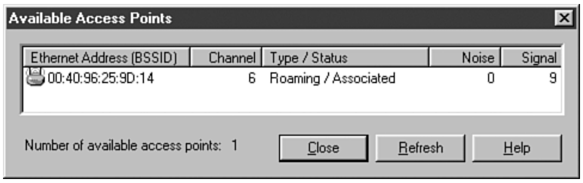
SSID
Service set identifier

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.



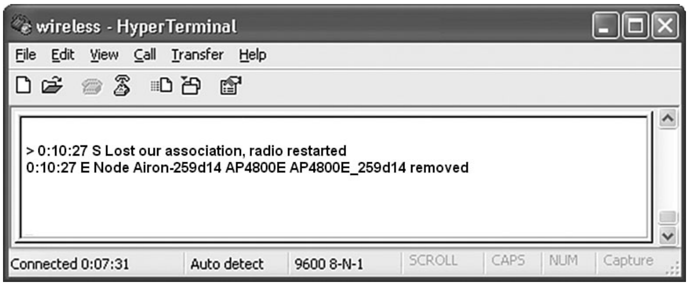
Ethernet Address (BSSID)	Channel	Type / Status	Noise	Signal
00:40:96:25:9D:14	6	Roaming / Associated	0	9

Number of available access points: 1

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.



```
> 0:10:27 S Lost our association, radio restarted
0:10:27 E Node Airon-259d14 AP4800E AP4800E_259d14 removed
```

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).

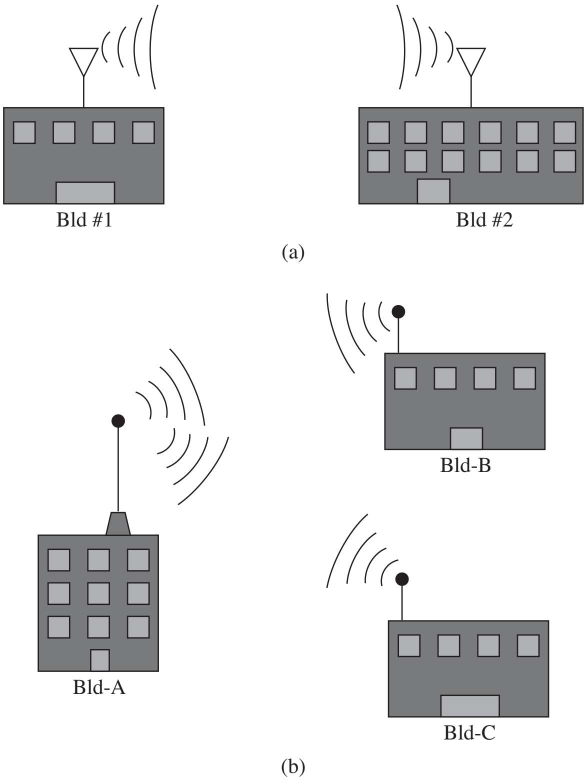


FIGURE 11-9 Examples of (a) point-to-point and (b) point-to-multipoint wireless bridge configurations.

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.

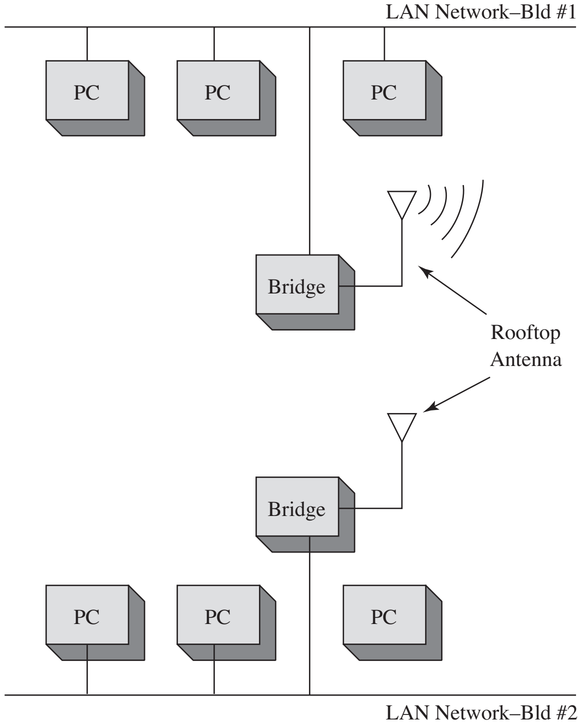


FIGURE 11-10 The wireless bridge connection to the wired network inside the building.

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

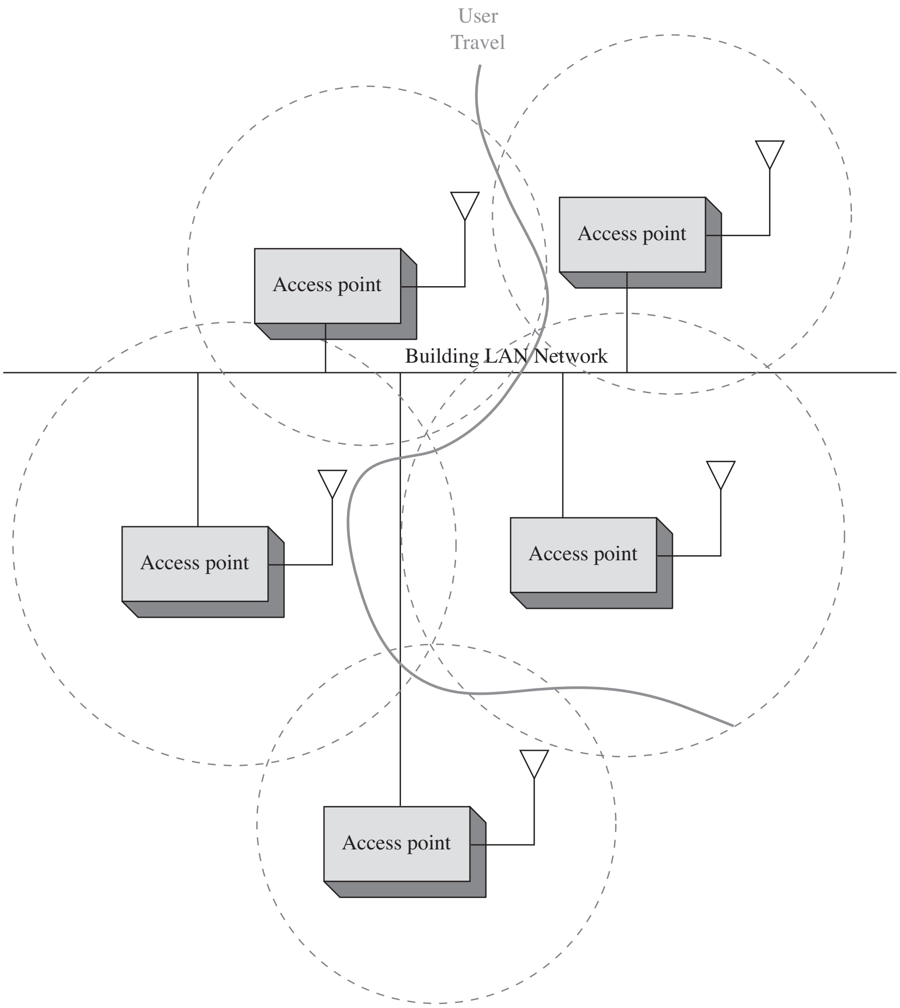


FIGURE 11-11 An example of configuring multiple access points to extend the range for wireless connectivity.

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.

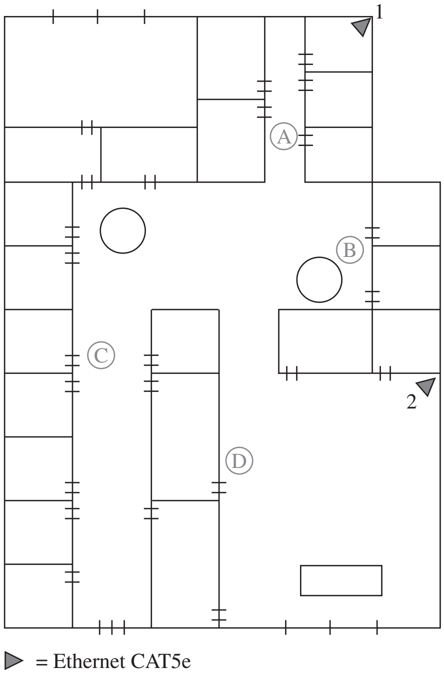
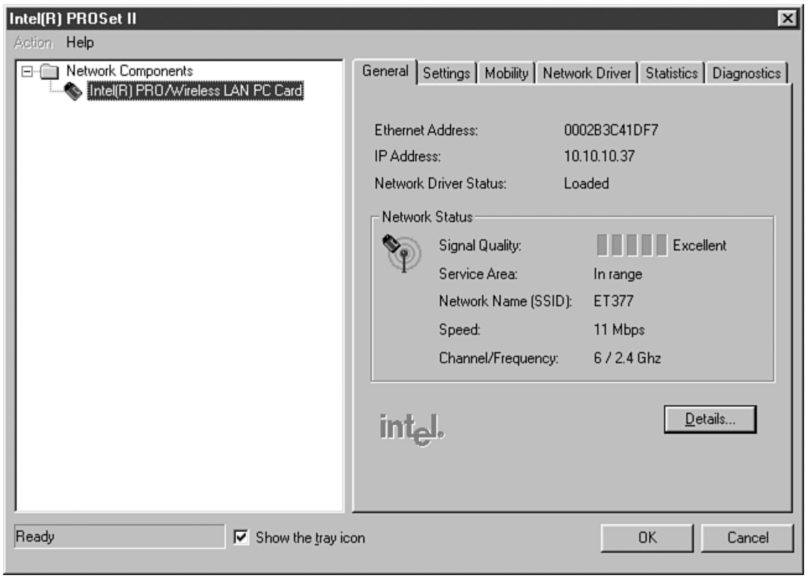


FIGURE 11-12 The floor plan of the building being surveyed for a wireless LAN.

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.

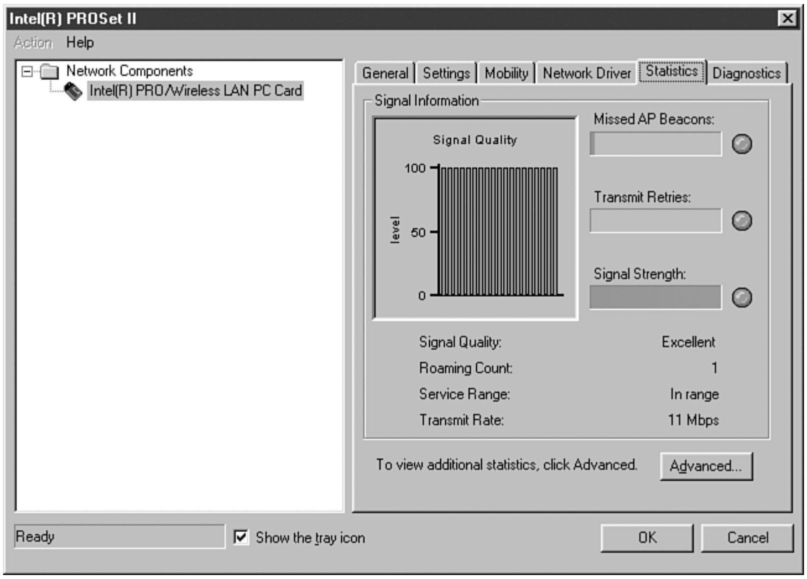


Ethernet Address: 0002B3C41DF7
IP Address: 10.10.10.37
Network Driver Status: Loaded

Network Status

Signal Quality: Excellent
Service Area: In range
Network Name (SSID): ET377
Speed: 11 Mbps
Channel/Frequency: 6 / 2.4 Ghz

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



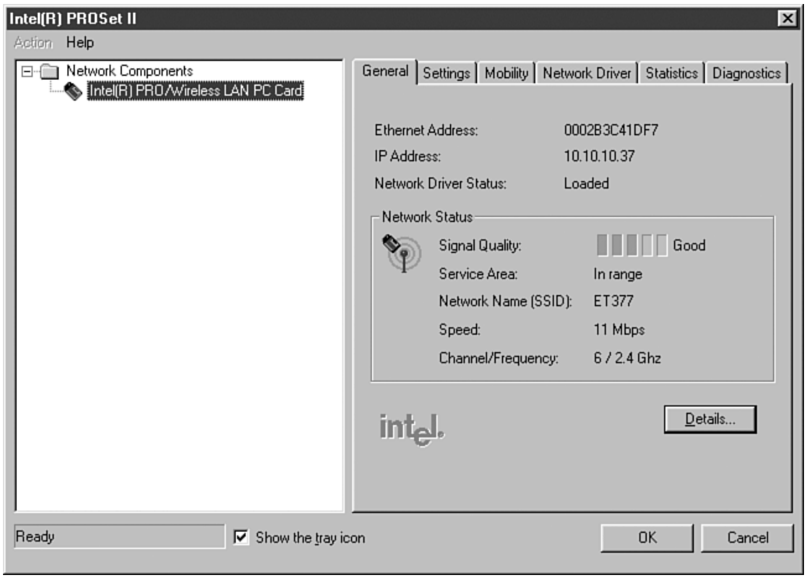
Signal Quality: Excellent
Roaming Count: 1
Service Range: In range
Transmit Rate: 11 Mbps

To view additional statistics, click Advanced.

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.

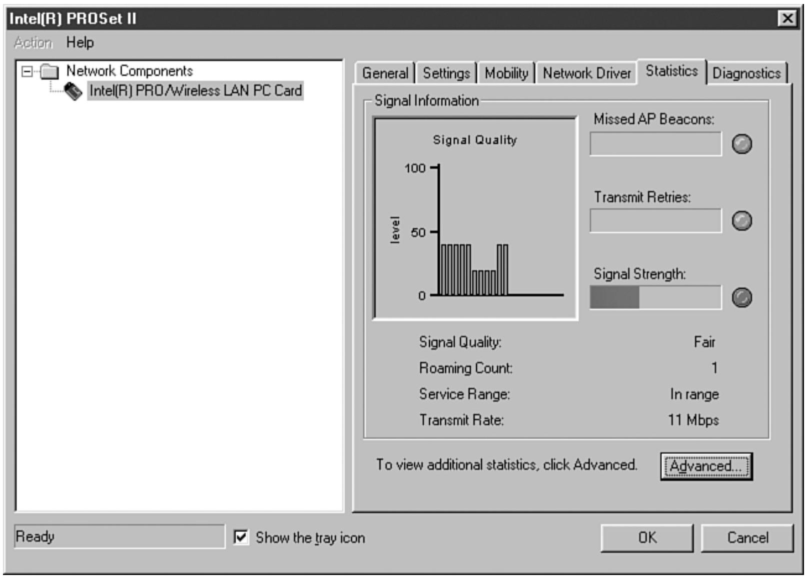


Ethernet Address: 0002B3C41DF7
IP Address: 10.10.10.37
Network Driver Status: Loaded

Signal Quality: Good
Service Area: In range
Network Name (SSID): ET377
Speed: 11 Mbps
Channel/Frequency: 6 / 2.4 Ghz

Ready
☑ Show the tray icon

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

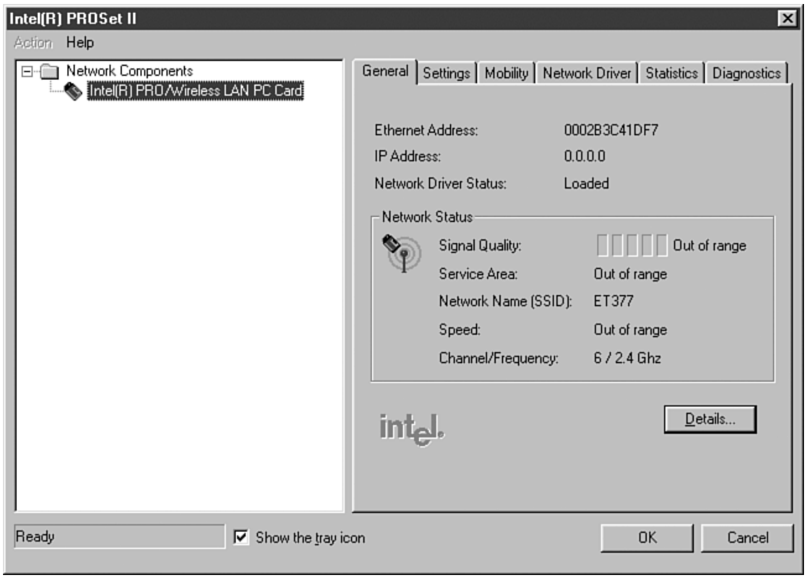


Signal Quality: Fair
Roaming Count: 1
Service Range: In range
Transmit Rate: 11 Mbps

To view additional statistics, click Advanced.

Ready
☑ Show the tray icon

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



Ethernet Address: 0002B3C41DF7
IP Address: 0.0.0.0
Network Driver Status: Loaded

Network Status

Signal Quality: Out of range
Service Area: Out of range
Network Name (SSID): ET377
Speed: Out of range
Channel/Frequency: 6 / 2.4 Ghz

Ready

☑ Show the tray icon

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

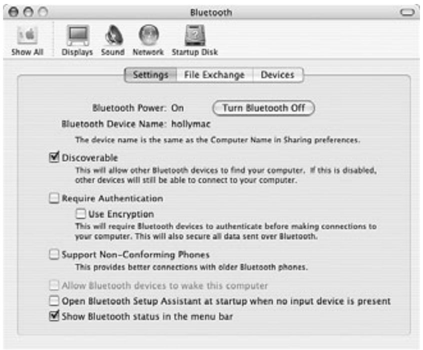
Paging Procedure
Used to establish and synchronize a connection between two Bluetooth devices

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.



Bluetooth Power: On

Bluetooth Device Name: hollymac

The device name is the same as the Computer Name in Sharing preferences.

☑ Discoverable

This will allow other Bluetooth devices to find your computer. If this is disabled, other devices will still be able to connect to your computer.

□ Require Authentication

□ Use Encryption

This will require Bluetooth devices to authenticate before making connections to your computer. This will also secure all data sent over Bluetooth.

□ Support Non-Conforming Phones

This provides better connections with older Bluetooth phones.

□ Allow Bluetooth devices to wake this computer

□ Open Bluetooth Setup Assistant at startup when no input device is present

☑ Show Bluetooth status in the menu bar

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

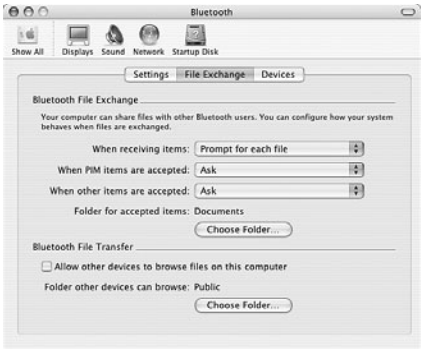
Pairing
When a Bluetooth device is set up to connect to another Bluetooth device.

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 allows files to come in. An example of the setup for the file transfer is shown in Figure 11-19.



Bluetooth File Exchange

Your computer can share files with other Bluetooth users. You can configure how your system behaves when files are exchanged.

When receiving items: Prompt for each file

When PIM items are accepted: Ask

When other items are accepted: Ask

Folder for accepted items: Documents

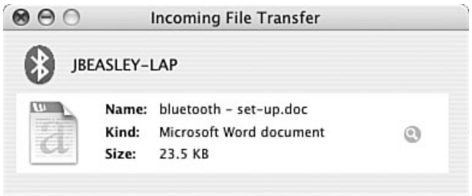
Bluetooth File Transfer

□ Allow other devices to browse files on this computer

Folder other devices can browse: Public

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.



JBEASLEY-LAP

Name: bluetooth – set-up.doc

Kind: Microsoft Word document

Size: 23.5 KB

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

WiMAX
A broadband wireless system based on the IEEE 802.16e standard

BWA
Broadband wireless access

WiMAX (**W**orldwide **I**nteroperability for **M**icrowave **Acc**ess) 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.

NLOS
Non line-of-sight

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.

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

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.

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

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 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.

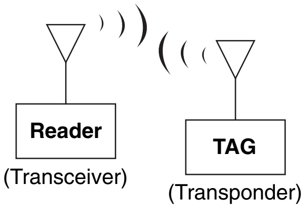


FIGURE 11-21 Basic block diagram of an RFID system.

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 10μA 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.

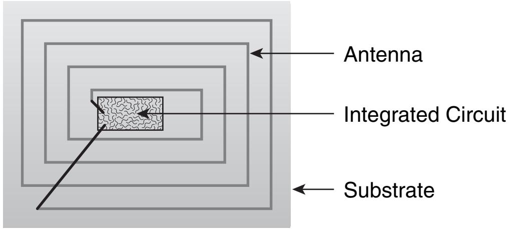


FIGURE 11-22 Examples of an RFID inlay.

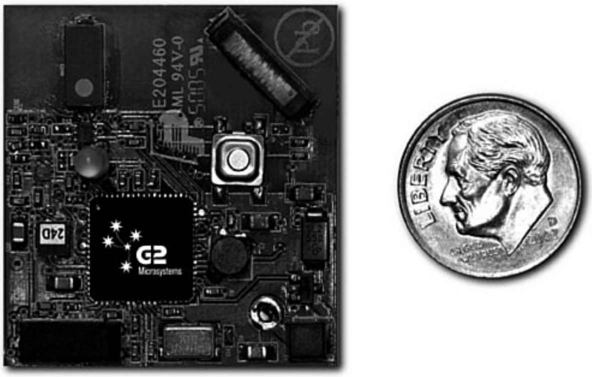


FIGURE 11-23 The G2C501 Active RFID tag from G2Microsystems (courtesy of G2Microsystems).

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!!!!!

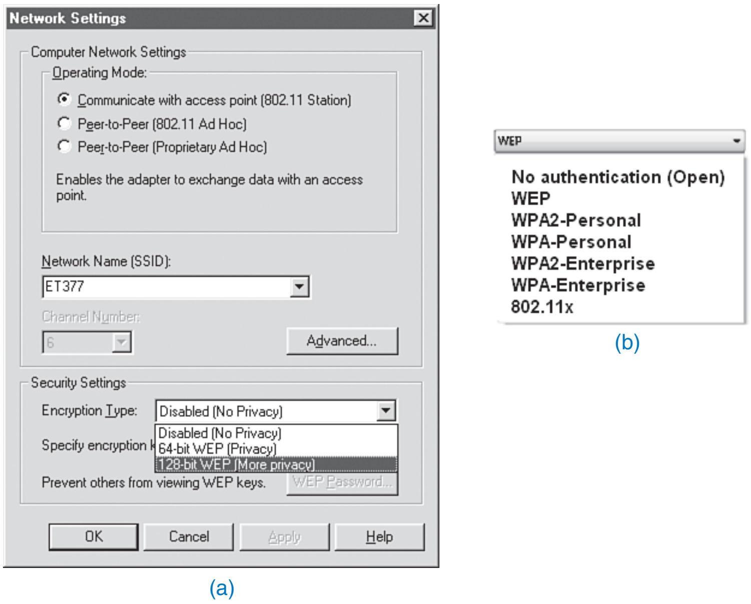
This might seem to be a bold statement, but surprisingly enough, many WLANs are placed on a network without turning on available wireless security features. Many times the user in the WLAN assumes that no one would break into his or her computer because nothing important exists on the system. This may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

Beacon
Used to verify the integrity of a wireless link

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.



Network Settings

Computer Network Settings

Operating Mode:

● Communicate with access point (802.11 Station)
○ Peer-to-Peer (802.11 Ad Hoc)
○ Peer-to-Peer (Proprietary Ad Hoc)

Enables the adapter to exchange data with an access point.

Network Name (SSID): ET377

Channel Number: 6

Security Settings

Encryption Type: Disabled (No Privacy)

Specify encryption k

Prevent others from viewing WEP keys.

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
Wi-Fi Protected Access

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 rouge of unauthorized access points.

EAP
Extensible Authentication Protocol

RADIUS
Remote Authentication Dial-In Service

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.

- 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.

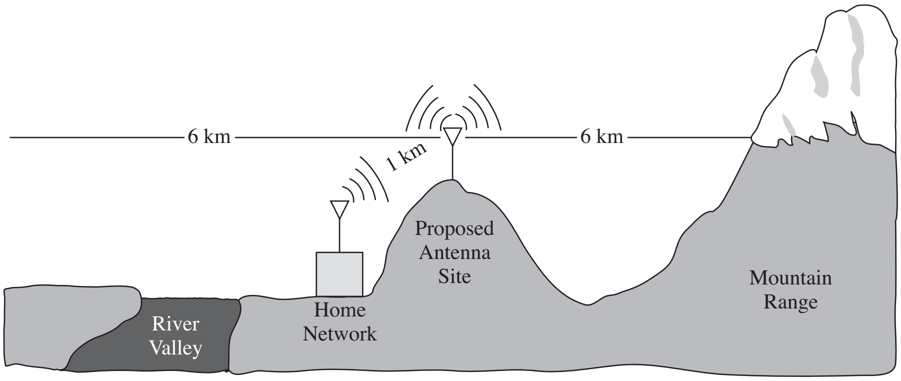


FIGURE 11-26 The terrain profile of the area to be supported by the proposed point-to-multipoint wireless network.

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.

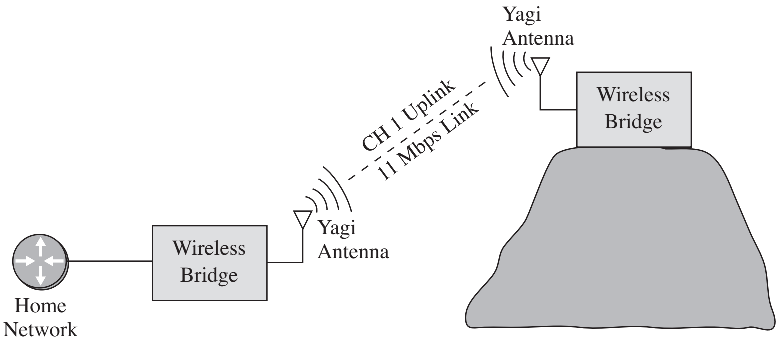


FIGURE 11-27 The proposed point-to-point wireless link from the home network to the antenna site.

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.

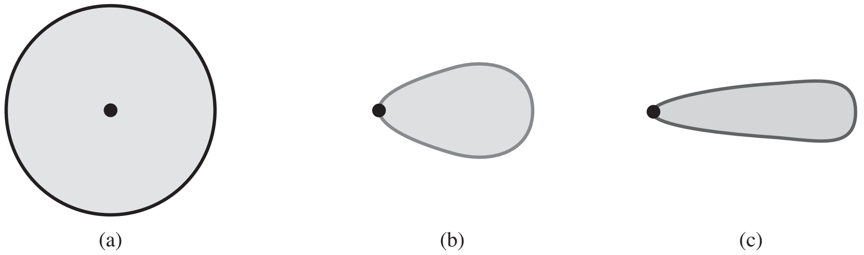


FIGURE 11-28 Antenna radiation patterns for (a) omnidirectional, (b) Yagi, and (c) dish [parabolic reflector] antenna, and supports 11 Mbps up to 7.5 km from the antenna. The cost of the Yagi antenna is comparable to the omnidirectional antenna.

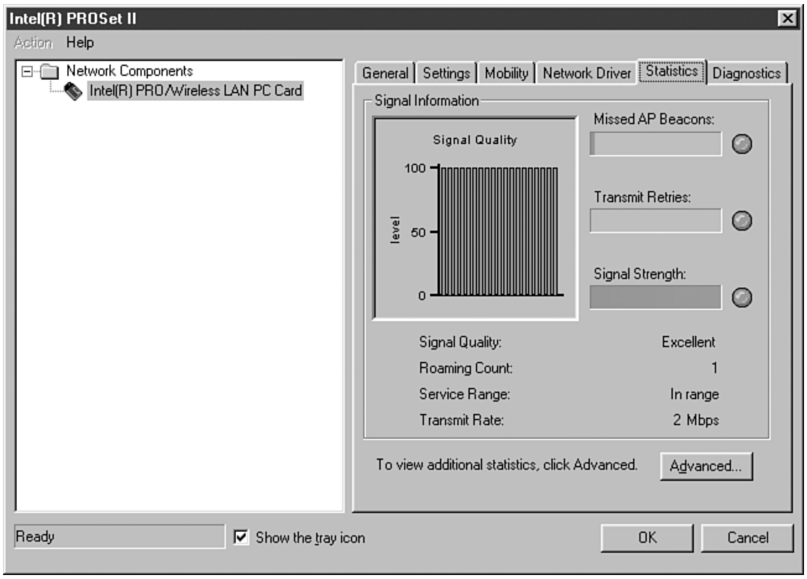
Antenna B, the directional Yagi, is selected for the point-to-point link. The antenna meets the distance requirement and also meets the 11 Mbps data rate requirement. Antennas A and C were not selected for the following reasons:

- 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.



Signal Quality: Excellent
Roaming Count: 1
Service Range: In range
Transmit Rate: 2 Mbps

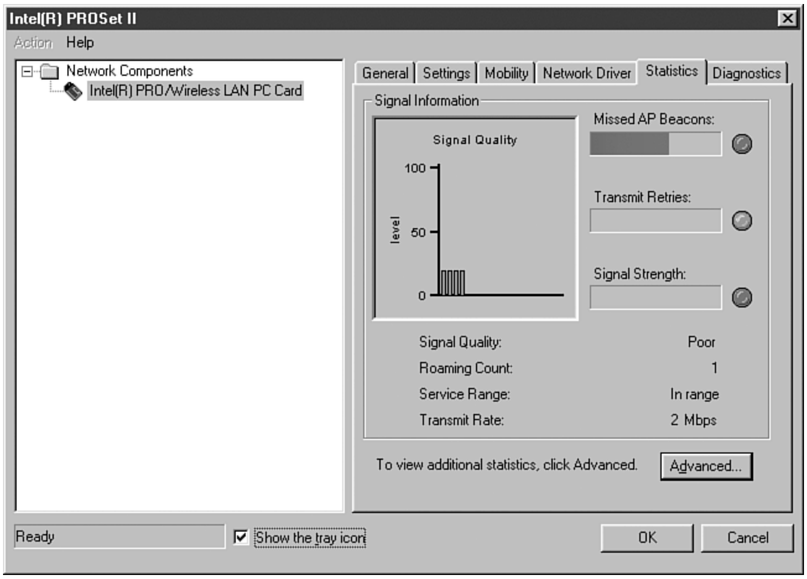
To view additional statistics, click Advanced.

Ready

☑ Show the tray icon

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.



Signal Quality: Poor
Roaming Count: 1
Service Range: In range
Transmit Rate: 2 Mbps

To view additional statistics, click Advanced.

☑ Show the tray icon

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.

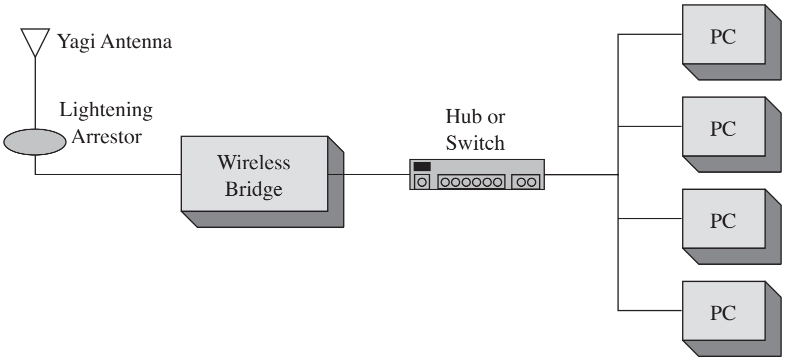


FIGURE 11-31 The setup for the remote user in the proposed point-to-multipoint wireless network.

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