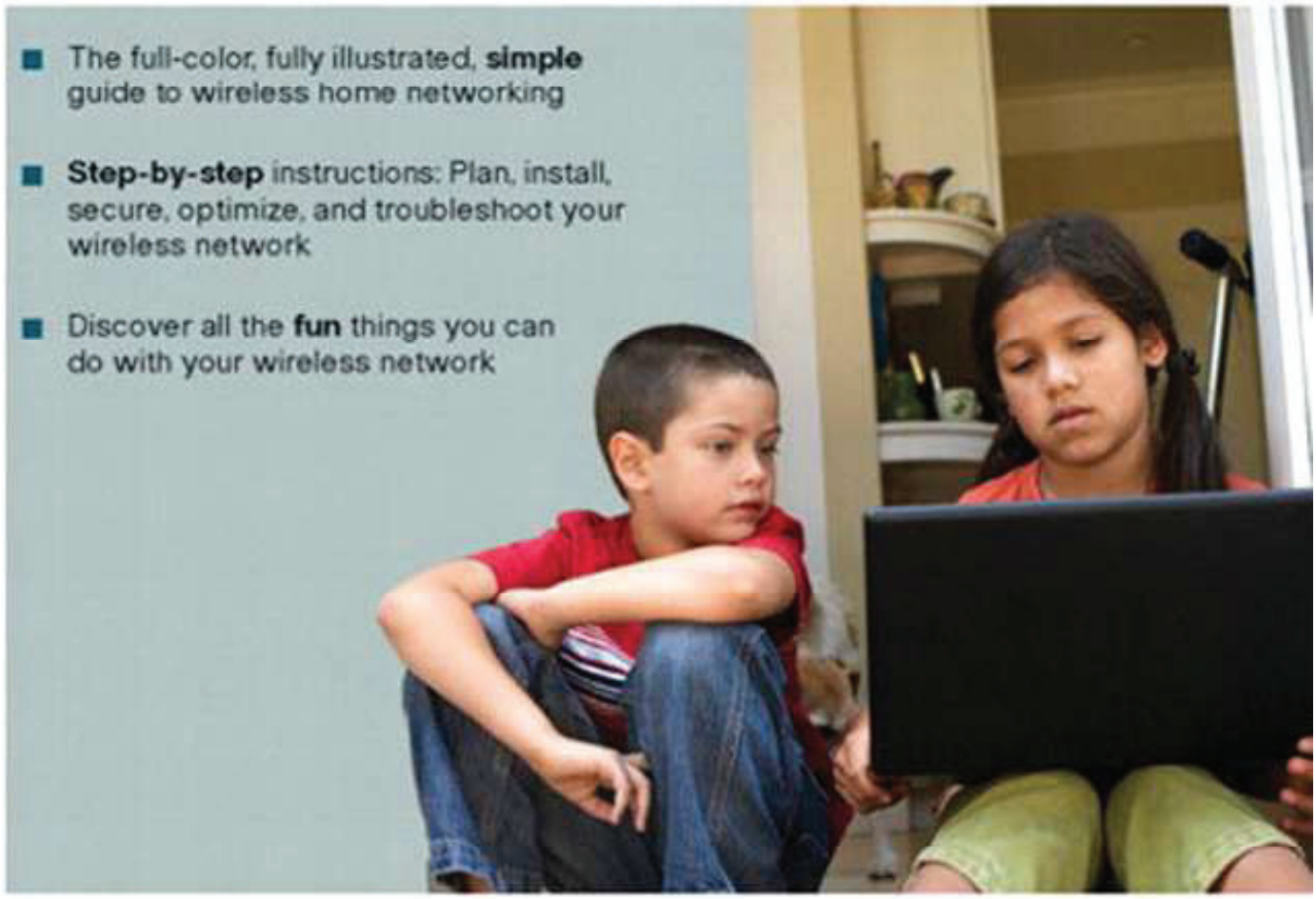
Wireless Home Networking Simplified

- The full-color, fully illustrated, **simple** guide to wireless home networking
- **Step-by-step** instructions: Plan, install, secure, optimize, and troubleshoot your wireless network
- Discover all the **fun** things you can do with your wireless network

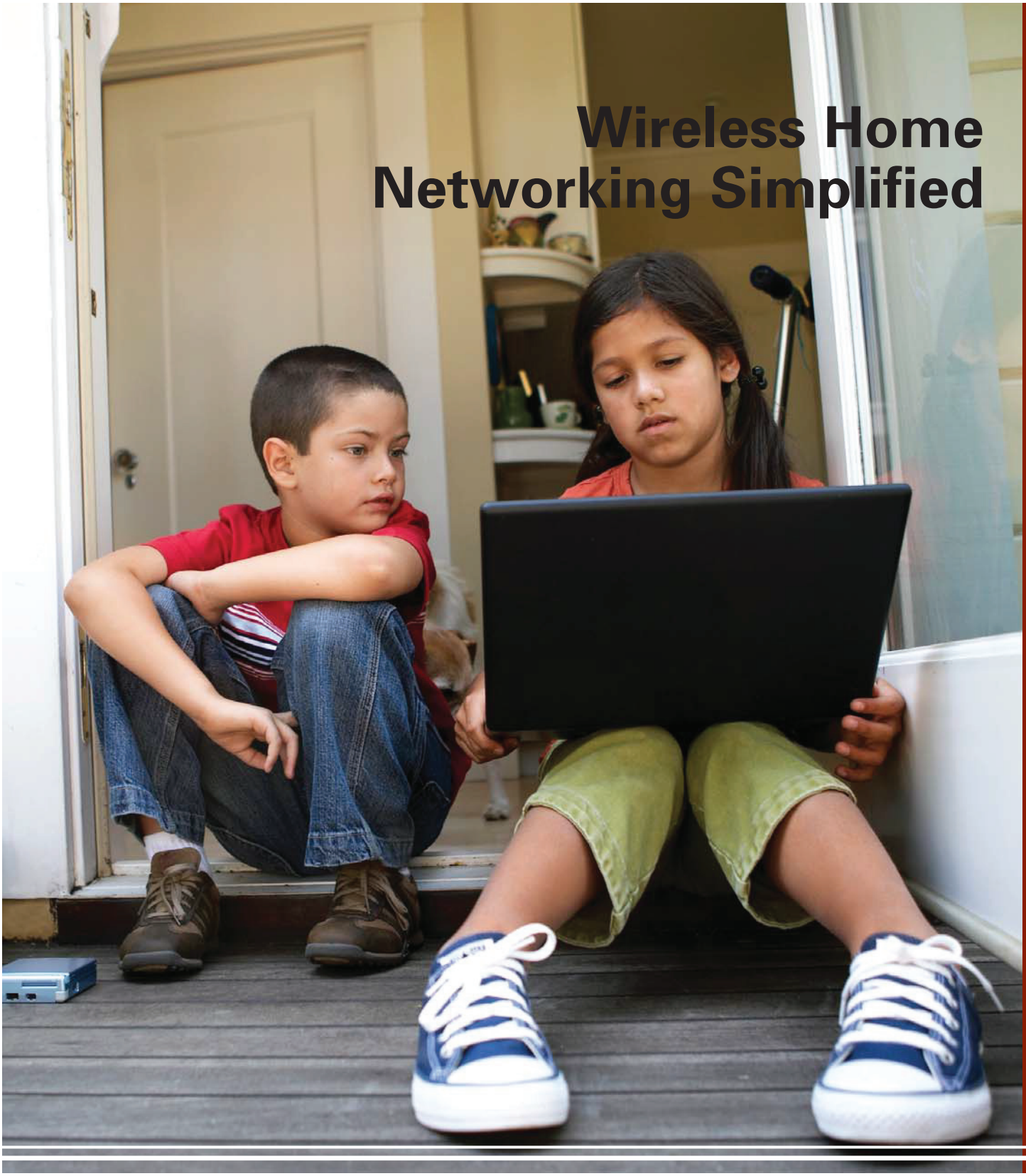


Jim Doherty
Neil Anderson

ciscopress.com

Amazon EX1013 Page 1

Wireless Home Networking Simplified



Jim Doherty
Neil Anderson
Illustrations by Nathan Clement

Cisco Press
800 East 96th Street
Indianapolis, IN 46240

Amazon EX1013 Page 2

Wireless Home Networking Simplified

Jim Doherty and Neil Anderson

Copyright© 2007 Cisco Systems, Inc.

Published by:
Cisco Press
800 East 96th Street
Indianapolis, IN 46240 USA

All rights reserved. No part of this book may be reproduced or transmitted in any form or by any means, electronic or mechanical, including photocopying, recording, or by any information storage and retrieval system, without written permission from the publisher, except for the inclusion of brief quotations in a review.

Printed in the United States of America 1 2 3 4 5 6 7 8 9 0

First Printing: December 2006

ISBN: 1-58720-161-5

Library of Congress Cataloging-in-Publication Data

Doherty, Jim, CCNA.
Wireless home networking simplified / Jim Doherty, Neil Anderson.
p. cm.
ISBN 1-58720-161-5 (pbk.)
1. Home computer networks. 2. Wireless LANs. I. Anderson, Neil, 1965- II. Title.
TK5105.75.D66 2006
004.6'8--dc22
2006036500

Warning and Disclaimer

This book is designed to provide information about building, using, and living with wireless home networks. Every effort has been made to make this book as complete and as accurate as possible, but no warranty or fitness is implied.

The information is provided on an “as is” basis. The authors, Cisco Press, and Cisco Systems, Inc. shall have neither liability nor responsibility to any person or entity with respect to any loss or damages arising from the information contained in this book or from the use of the discs or programs that may accompany it.

The opinions expressed in this book belong to the authors and are not necessarily those of Cisco Systems, Inc.

Feedback Information

At Cisco Press, our goal is to create in-depth technical books of the highest quality and value. Each book is crafted with care and precision, undergoing rigorous development that involves the unique expertise of members from the professional technical community.

Readers' feedback is a natural continuation of this process. If you have any comments regarding how we could improve the quality of this book, or otherwise alter it to better suit your needs, you can contact us through e-mail at feedback@ciscopress.com. Please make sure to include the book title and ISBN in your message.

We greatly appreciate your assistance.

Trademark Acknowledgments

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

Publisher
Paul Boger

Cisco Representative
Anthony Wolfenden

Cisco Press Program Manager
Jeff Brady

Executive Editor
Kristin Weinberger

Managing Editor
Patrick Kanouse

Development Editor
Dayna Isley

Senior Project Editor
San Dee Phillips

Copy Editor
Bill McManus

Technical Editors
Doug Foster
Bradley Mitchell

Team Coordinator
Vanessa Evans

Cover Designer
Louisa Adair

Interior Design and Composition
Mark Shirar

Indexer
WordWise Publishing Services, LLC

Proofreader
Katherin Bidwell

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

Asia Pacific Headquarters
Cisco Systems, Inc.
168 Robinson Road
#28-01 Capital Tower
Singapore 068912
www.cisco.com
Tel: +65 6317 7777
Fax: +65 6317 7799

Europe Headquarters
Cisco Systems International BV
Haarlerbergpark
Haarlerbergweg 13-19
1101 CH Amsterdam
The Netherlands
www-europe.cisco.com
Tel: +31 0 800 020 0791
Fax: +31 0 20 357 1100

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at www.cisco.com/go/offices.

©2006 Cisco Systems, Inc. All rights reserved. CCVP, the Cisco logo, and the Cisco Square Bridge logo are trademarks of Cisco Systems, Inc.; Changing the Way We Work, Live, Play, and Learn is a service mark of Cisco Systems, Inc.; and Access Registrar, Aironet, BPX, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Enterprise/Solver, EtherChannel, EtherFast, EtherSwitch, Fast Step, Follow Me Browsing, FormShare, GigaDrive, GigaStack, HomeLink, Internet Quotient, IOS, IP/TV, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, iQuick Study, LightStream, Linksys, MeetingPlace, MGX, Networking Academy, Network Registrar, Packet, PIX, ProConnect, RateMUX, ScriptShare, SlideCast, SMARTnet, StackWise, The Fastest Way to Increase Your Internet Quotient, and TransPath are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or Website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0609R)

About the Authors

Jim Doherty is the vice president of marketing at CipherOptics, where he leads the outbound marketing teams. Prior to joining the CipherOptics team Jim held leadership positions with Symbol Technologies and Cisco. Jim has more than 15 years of technical marketing and engineering experience and has led various marketing campaigns for IP telephony, routing and switching, and network security solutions. Jim is the coauthor of the *Networking Simplified* series of books published by Cisco Press. Jim is a former Marine Corps sergeant; he holds a B.S. degree in electrical engineering from N.C. State University and an M.B.A. degree from Duke University.

Neil Anderson is the senior manager of enterprise systems engineering with Cisco. Neil has more than 20 years of broad engineering experience including public telephone systems, mobile phone systems, Internet, and home networking. At Cisco, Neil's focus is on large corporate customers in the areas of routing and switching, wireless, security, and IP communications. Neil is the coauthor of the *Networking Simplified* series of books including *Home Networking Simplified*, *Home Network Security Simplified*, and *Internet Phone Services Simplified*. Neil holds a B.S. degree in computer science.

About the Technical Reviewers

Doug Foster works in the area of packet voice, video, and data convergence. With 30 years of experience for companies such as Cisco, John Deere, and Alcatel and for private business, Doug has some interesting firsthand stories to tell about the evolution of the Internet. He has architected and helped install international networks, such as the migration of John Deere's worldwide SNA business network into a multiprotocol intranet in the mid-1980s. As a result of that work, Doug was asked by the U.S. Department of Defense to speak at Interop '88 on "How John Deere builds tractors using TCP/IP." This was nearly a decade before most businesses began to leverage the value of the Internet and eCommerce applications. Most recently, Doug worked for Cisco as one of its first enterprise voice consultants. Doug has a bachelor of science in mechanical engineering from Iowa State University and lives in Cary, North Carolina, with his wife, Cindy. When not busy with family—daughters, Erin and Amber; son-in-law, Jeremy; and grandson, Jake—or business (Convinsys, Performance Podcasts, and Idea Mechanics), Doug devotes his free time to writing his first book (*Convince Me!*) and to sea kayaking.

Bradley Mitchell works as a freelance writer on the About.com wireless/networking site. He has produced online content at About.com on home computer networking, wireless, and related topics for six years. Bradley is also a senior engineer at Intel Corporation. Over the past 12 years at Intel, he has served in various capacities for research and development of software and network systems. Bradley obtained his master's degree in computer science from the University of Illinois and his bachelor's degree from M.I.T.

About the Illustrator

Nathan Clement declared himself an illustrator four years ago. Nathan holds a bachelor of fine arts degree in art and writing, which launched a surprise career in publishing, design, and art direction. His major roles have been owning a printing company, designing books in-house at Macmillan Computer Publishing, and serving as art director for an ad agency. Through these little adventures, he decided to get back to his art roots and keep both feet planted firmly in both the publishing and design worlds as an illustrator. He has been pleased to illustrate four previous books in the Cisco Press *Networking Simplified* series and has done work for Que Publishing, Macromedia Press, Peachpit Press, Prentice Hall, and *ESPN The Magazine*. He lives with his wife, Greta, a nurse practitioner, in Indianapolis and also pursues children's book illustration with paint and brushes. Contact Nathan at nathan@stickmanstudio.com.

Dedications

From Jim Doherty:

I would like to dedicate this to my good friend and coauthor Neil Anderson. Working together across ten years, two companies, and six books has been both fun and rewarding, and I'm better off for having been a part of it.

From Neil Anderson:

I would like to dedicate this book to my great and talented coauthor Jim Doherty. I could not ask for a more creative and humorous friend and coauthor. It's been a kick to work with you Jim on our common passion.

Acknowledgments

Jim and Neil would like to thank the following people:

Our families, for putting up with yet another book, and our extended families and friends whose phones calls and e-mails about wireless convinced us that this book was still needed.

Our publisher and the fine team at Cisco Press and Pearson Education. We would especially like to thank our editor, Dayna Isley, who we lied to about our schedule at every turn; our production manager, Patrick Kanouse, the team's sole survivor from our first book; our project manager, handler, and den mother, Kristin Weinberger; San Dee Phillips, our project editor (who we just tortured with our poor grammar); and the entire editorial and production team.

As always we want to thank our illustrator, Nathan Clement at Stickman Studios (www.stickman-studio.com/). What can we say, you did it again.

A special thanks to our technical reviewers, Bradley Mitchell and Doug Foster, who work hard on our reader's behalf to keep us honest and accurate.

Another special thanks to some kind folks at Linksys: Stuart Hamilton, Uzi Entin, and Brenton Elmore.

And last but not least, the following people who helped us with technical questions along the way: Brian Cox, Lou Ronnau, Jason Frazier, Steve Ochmanski, and Bruce McMurdo.

Contents at a Glance

Part I How Does It Work

Chapter 1 How Wireless LANs Work 3

Chapter 2 Wireless Standards: What the Letters Mean 15

Chapter 3 Selecting the Right Wireless Standard for Your Network 23

Part II What You Should Know

Chapter 4 Planning Your Wireless Network 35

Chapter 5 Wireless Security: What You Need to Know 47

Chapter 6 What to Buy 57

Part III How Do I Set It Up?

Chapter 7 Wireless Router Setup 73

Chapter 8 Wireless NIC Setup 99

Chapter 9 Wireless Security Setup 123

Part IV "Honey, This Stupid Wireless Thing Is Not Working"

Chapter 10 Troubleshooting: I Can't Connect at All 173

Chapter 11 Troubleshooting: I Can Connect Sometimes 219

Chapter 12 Troubleshooting: I Can Connect, but It's Slow 239

Part V Bells and Whistles

Chapter 13 Wireless Video and Entertainment 259

Chapter 14 Wireless to Go 295

Chapter 15 The Future of Wireless Networking 317

Appendixes

Appendix A MAC Address Filtering 325

Appendix B 802.11n Wireless Channels 331

Appendix C 802.11 Additional Revisions 333

Glossary 335

Index 345

Contents

Part I How Does It Work

Chapter 1 How Wireless LANs Work 3

Why Wireless? 4

Before We Get to the Wireless Bit, What the Heck Is a LAN? 5

Okay, Now the Wireless Part 9

Challenges for Wireless Communication 9

The Solution 10

Putting It All Together 11

Summary 12

Where to Go for More Information 13

Chapter 2 Wireless Standards: What the Letters Mean 15

The Standard 802.11 and the IEEE 16

802.11a 17

802.11b 18

802.11g 19

802.11n 20

Combinations 21

What Happened to the Other Letters? 21

Summary 22

Where to Go for More Information 22

Chapter 3 Selecting the Right Wireless Standard for Your Network 23

What to Consider When Choosing Your Wireless Standard 24

Compatibility 24

Relationships Among Wireless Standards 25

Dual-Band Products 26

Proprietary Extensions 27

Speed 27

Range 28

Security 28

Cost 29

Additional Considerations 29

Comparing the IEEE WLAN Standards 30

Recommendations 31

Summary 32

Where to Go for More Information 32

Part II What You Should Know

Chapter 4 Planning Your Wireless Network 35
Wireless Network Topologies 35
Sketching a Network Layout 37
Thinking Your Network Plan Through 39
Determining the Networking Capabilities of Your Computers 40
Looking for a Wired NIC 40
Looking for a Wireless NIC 40
Determining Your Immediate Needs to Create a Wireless Network 43
Completing Your Plan 44
Summary 45

Chapter 5 Wireless Security: What You Need to Know 47
Why Should I Worry About Wireless Network Security? 47
What Do I Do to Secure My Wireless Network? 50
Don't Advertise Your Wireless Network 51
Scramble Your Signal 52
What Is Encryption? 52
Choosing an Encryption Key 53
Disable Ad Hoc Networking 54
Other Tips to Consider 55
Summary 55
Where to Go for More Information 55

Chapter 6 What to Buy 57
Determining Network Readiness 57
Making Your List, Checking It Twice 61
Wireless Router Options 62
Wireless NIC Options 63
Gear for Travel Bugs and Road Warriors 65
Extra Stuff 66
Where to Buy Your Gear 67
Summary 69
Where to Go for More Information 69

Part III How Do I Set It Up?

Chapter 7 Wireless Router Setup 73
Connecting the Wireless Router 74
Configuring the Wireless Router 75
Using the Linksys Setup Wizard 77
Using an Internet Browser 84
Using Linksys EasyLink Advisor 91

Summary 98
Where to Go for More Information 98

Chapter 8 Wireless NIC Setup 99
Installing the Wireless NIC 99
Installing a PCI Wireless Card in a Desktop Computer 101
Installing a PCMCIA Wireless Card in a Laptop Computer 102
Installing a USB Wireless NIC in a Computer 103
Associating the Wireless NIC to the Wireless Router 105
Wireless Profiles 106
Wireless Connection Managers 108
Using the Windows Wireless Network Connection Utility 109
Using Linksys WLAN Monitor 111
Using Linksys EasyLink Advisor 113
Summary 121
Where to Go for More Information 122

Chapter 9 Wireless Security Setup 123
Setting Up Wireless Encryption 123
Tips Before We Start 125
If Only It Were That Easy 126
Manually Setting Up Wireless Encryption 127
Enabling WEP Encryption on the Wireless Router 128
Enabling WEP Encryption on the Wireless NIC 130
WPA Encryption Example 137
Setting Up Wireless Encryption with Linksys SecureEasySetup 142
Linksys SecureEasySetup on the Wireless Router 144
Linksys SecureEasySetup on the Wireless NIC 148
Setting Up Wireless Encryption with Linksys EasyLink Advisor 150
Linksys EasyLink Advisor on the Wireless Router 151
Using EasyLink Advisor to Add Encryption to Wireless NICs 156
More Wireless Security Steps 162
Stop Advertising Your Wireless Network 163
Turn On the Firewall 164
Prevent Unintentional Roaming 164
MAC Address Locking 166
Top Troubleshooting Tips for Wireless Encryption 167
Summary 167
Where to Go for More Information 168

Part IV "Honey, This Stupid Wireless Thing Is Not Working"

Chapter 10 Troubleshooting: I Can't Connect at All 173

Steps to Connecting 174
- Scanning 176
- Matching 176
- Associating 176
- Securing the Connection 176
- Obtaining an IP Address 177
- Sending and Receiving 177

What Can Go Wrong 177
- Problems During Scanning 178
- Problems During Matching 179
- Problems During Association 180
- Problems Securing the Connection 180
- Problems Obtaining an IP Address 180
- Problems Sending and Receiving 180

Five Things to Look At First 181

How to Tell if You Do Not Have a Connection 181

Figuring Out Why It Will Not Connect 183
- Scanning-Related Issues 184
  - Incompatible Wireless Standards 184
  - Wireless Turned Off 185
  - Poor Signal Strength 187
- Matching-Related Issues 189
  - SSID Mismatch 189
  - SSID Broadcast 192
- Association-Related Issues 193
- Security- and Encryption-Related Issues 196
  - Encryption Type Mismatch 196
  - Encryption Key Mismatch 197
  - Windows XP Authentication Setting Mismatch 209
- IP Address Assignment–Related Issues 210
  - Determining if an IP Address Is Assigned 211
  - Determining if IP Address Assignment Is Failing 212
  - Trying the Windows XP Repair Function 214
  - Checking the Router's DHCP Client Pool 215

Wireless Connection Made 216

Oops, How Embarrassing! 218
The 10-Minute Miracle 218
Summary 218
Where to Go for More Information 218

Chapter 11 Troubleshooting: I Can Connect Sometimes 219
How Wireless Coverage Works 219
Tuning Your Wireless Coverage 221
Performing a Wireless Survey 221
Wireless Survey Using Windows XP 223
Wireless Survey Using Linksys WLAN Monitor 224
What to Conclude from Your Wireless Survey 226
What You Can Do to Improve Coverage 227
Improving the Location of the Wireless Router 227
Trying Different Channels 229
Trying Different Antenna Positions 234
Upgrading the Antenna 236
Using Wireless Range Extenders and Additional Access Points 236
Upgrading the Wireless Router 237
Summary 237
Where to Go for More Information 237

Chapter 12 Troubleshooting: I Can Connect, but It's Slow 239
Is the Broadband Internet Connection the Bottleneck? 239
Checking the Broadband Connection 241
Testing Your Broadband Speed 243
Is the Wireless Network Too Slow? 244
Understanding Wireless Standards and Speeds 244
Verifying Wireless Network Speed 245
Is the Wireless Network Signal Getting Degraded? 248
Interference from Other Wireless Routers 248
Checking for Conflicting Wireless Routers 248
Determining Whether the Conflicting Wireless Router Is Causing an Issue 250
Correcting a Conflicting Wireless Router Situation 251
Interference from Cordless Phones and Other Devices 252
Determining Whether the Conflicting Cordless Phone Is Causing an Issue 252
Correcting a Conflicting Cordless Phone Issue 254
Summary 255
Where to Go for More Information 255

Part V Bells and Whistles

Chapter 13 Wireless Video and Entertainment 259

Wireless Video Cameras 259
- Finding Uses for Wireless Video Cameras 261
- Connecting the Video Camera to Your Wireless Network 263
- Determining Who Can Access the Video Camera 268
- Viewing Video from Within Your House 271
- Viewing Video over the Internet 273
  - Setting Up the Wireless Router for Internet Camera Viewing 274
  - How to View the Camera over the Internet 276
  - Problems with Viewing Video over the Internet 277
- Using the Video Camera as a Motion Detector 277

Wireless Online Gaming 279
- Gaming Servers 280
- Options for Online Gaming 280
- How to Connect Video Game Consoles to Your Wireless Network 281
  - Setting Up the Wireless Game Adapter 282
  - Connecting a Video Game Console 284
  - Connecting to an Online Game Provider 285

Networking Your DVR 288
- Typical DVR Setups Today 289
- Reasons to Network Your DVR 289
- Networking Your DVR 290
- Using TiVoToGo 291

Summary 293

Where to Go for More Information 293

Chapter 14 Wireless to Go 295

What Is a Wireless Hotspot? 295

How to Find Wireless Hotspots 297

Wireless Hotspot Options and Costs 298

Discovering and Connecting to Wireless Hotspots 299
- Connecting to Hotspots Using Linksys WLAN Monitor 300
- Connecting to Hotspots Using Windows XP 302
- Connecting to Hotspots Using Boingo 305
- Passing the Membership Test 305
  - Example: Connecting to a Free Service at Bear Rock Cafe 306
  - Example: Connecting to T-Mobile Service at Borders Book Stores 307

What Not to Do When Using a Wireless Hotspot 308
Setting Up Your Own Portable Hotspot 310
How Wireless Travel Routers Work 310
Setting Up a Wireless Travel Router 311
Setting Up Your Laptop to See the Travel Router 314
How to Use a Wireless Travel Router 315
Summary 316
Where to Go for More Information 316

Chapter 15 The Future of Wireless Networking 317
Wireless Networks Will Be Faster 317
Wireless Networks Will Go Farther 319
Wireless Networks Will Be in More Places 319
Wireless Networks Will Move with You 320
More Devices Will Connect to Wireless Networks 321
Summary 321
Where to Go for More Information 321

Appendixes

Appendix A MAC Address Filtering 325

Appendix B 802.11n Wireless Channels 331

Appendix C 802.11 Additional Revisions 333

Glossary 335

Index 345

Introduction

We assume that if you read the front cover you know what this book is about, but there's a bit more to it than that. With the explosion of popularity in wireless networking, there is a proportional number of people who do not understand the technology, and a similar number of people who think they understand it (but don't) and are all too willing to dispense advice. Usually it ends poorly, and you get stuck with a network that does not work.

This book is written for all of you out there who want to get the benefits of wireless networking but don't feel like you have the technical background to set it up yourselves. We are confident that if you read this book and follow the steps we lay out, you will have a much better understanding of the technology and, most importantly, a working wireless network. We will try to do this without you having to get a technical degree just to deploy your home network.

What to Expect

We've divided this book into five parts, each of which describes a major part of the process of building and using a wireless network. These sections describe

- How wireless works
- What you need to know
- How to set it all up
- What to do if it doesn't work
- What other cool things you can do with it

Each section is described in greater detail in the following sections.

Part I, "How Does It Work?"

Part I starts by explaining the basics in Chapter 1, "How Wireless LANs Work." We think it's worth mentioning that a basic working knowledge of wireless networking should be of interest to you if you are about to set up your own wireless network, and at a minimum it will help you make some better-informed decisions. In Chapter 2, "Wireless Standards: What the Letters Mean," we cover the main wireless standards. There are a number of choices with regard to the frequency, speed, range, and costs of each of the main standards, and we cover all of them here. We finish this section with Chapter 3, "Selecting the Right Wireless Standard for Your Network." There are a lot of choices out there. This chapter will help you cut through the confusion.

Part II, "What You Should Know"

In Part II we focus on what you should know before setting up your wireless network. This is where we put all the information in Part I to good use.

Chapter 4, "Planning Your Wireless Network," covers how to plan your network to meet the needs of today and bridge the gap to tomorrow. Chapter 5, "Wireless Security: What You Need to Know," covers the very important topic of wireless security. Don't skip this chapter.

Finally, in Chapter 6, "What to Buy," we explain how to figure out what equipment you need to buy. It's important to wait until this point in the book to actually buy gear, especially if you are starting from scratch. Trust us, this will save you money in the long run.

Part III, "How Do I Set It Up?"

In Part III we get to work and build your network. Chapter 7, "Wireless Router Setup," covers setting up your wireless router. This is the heart and soul of your network. In Chapter 8, "Wireless NIC Setup," we help you set up your wireless network interface card (called a NIC). This is the piece that allows your computer to be "wireless." Once everything is up and running, Chapter 9, "Wireless Security Setup," covers the implementation of wireless security in a step-by-step manner, because we need to keep the bad guys off our network.

Part IV, "Honey, This Stupid Wireless Thing Is Not Working"

Into every life a little rain must fall. Part IV covers how to troubleshoot a network that does not want to work the way it ought to. Chapter 10, "Troubleshooting: I Can't Connect at All," focuses on what to do when you can't get a computer to connect to the wireless network. Sometimes you can connect but the coverage is lousy. Chapter 11, "Troubleshooting: I Can Connect Sometimes," covers what to do in these cases. Chapter 12, "Troubleshooting: I Can Connect, but It's Slow," wraps up the section with steps to take when your connection seems slower than it ought to be.

Part V, "Bells and Whistles"

For those of you who want to take a step beyond a basic wireless network, Part V covers some bells and whistles you can add. Chapter 13, "Wireless Video and Entertainment," provides information on how to set up wireless-based entertainment options on your network. Chapter 14, "Wireless to Go," shows you how to take your wireless on the road and connect to hotspots. We close the section and the book with a summary in Chapter 15, "The Future of Wireless Networking," on what we think the future holds for wireless networking.

Housekeeping Stuff

This book focuses on the Windows operating systems and all screenshots were taken from computers running Windows XP. If you are not running Windows XP, you can still follow the recommendations and tips for the chapters where changes or setups are made, or where directory paths are followed. The general steps still hold true, but the directory paths and filenames may change. Your user manual or help files should help get you where you need to go for operating systems other than Windows XP.

We also had to make some decisions regarding what type of gear and programs to install as examples. Most of the gear we recommend here is from Linksys. In the spirit of full disclosure, our current (Neil) and former (Jim) employer is the parent company of Linksys. That said, we believe that Linksys has the most complete and easy-to-use wireless portfolio.

We hope you find this book useful, usable, and entertaining. Good luck, and happy networking.

Amazon EX1013 Page 19



PART I

PART

How Does It Work

Chapter 1 How Wireless LANs Work

Chapter 2 Wireless Standards: What the Letters Mean

Chapter 3 Selecting the Right Wireless Standard for Your Network

We'll start the book with a few chapters on how wireless works. Nothing too deep or complicated; just a high level overview to provide some information that we think will help you to decide which type of wireless home network you want, where you want to use it, and how you put it together.

Chapter 1, "How Wireless LANs Work," is a primer on how wireless networking works. We'll cover how the pieces talk to each other and how the network sends and receives data to and from the Internet.

Chapter 2, "Wireless Standards: What the Letters Mean," untangles all the different wireless standards. We cover what the letters mean, how they are different from each other, and what the pros and cons of each are. We also tell you what happened to the "missing" letters.

We wrap up Part I with Chapter 3, "Selecting the Right Wireless Standard for Your Network," which provides some guidance on how to determine which wireless standard you should choose. A lot depends on your circumstances, but we will give you our recommendations to at least help narrow down the choices.

CHAPTER 1

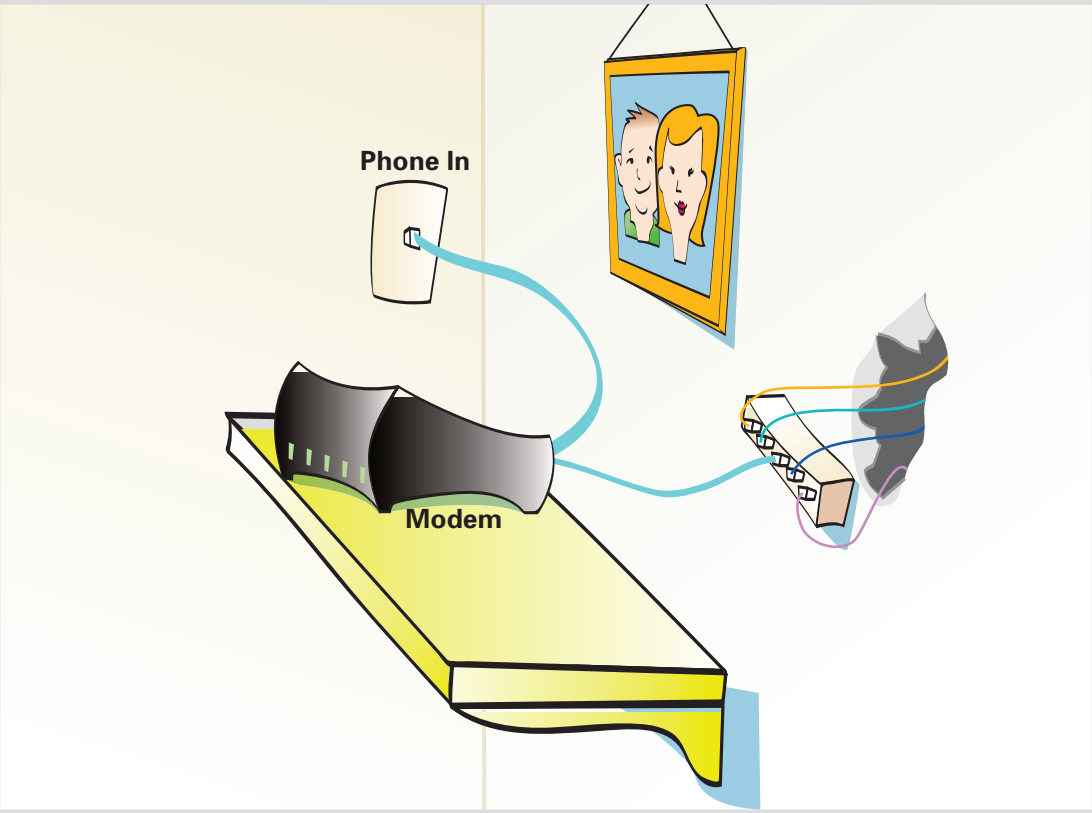
How Wireless LANs Work

Albert Einstein was quoted as saying "You see, wire telegraph is a kind of a very, very long cat. You pull his tail in New York and his head is meowing in Los Angeles. Do you understand this? And radio operates exactly the same way: you send signals here, they receive them there. The only difference is that there is no cat."

That, in a nutshell, is how a wireless computer network works. In a wired network, data is sent and received between computers and routers using pieces of cable called *Ethernet*.

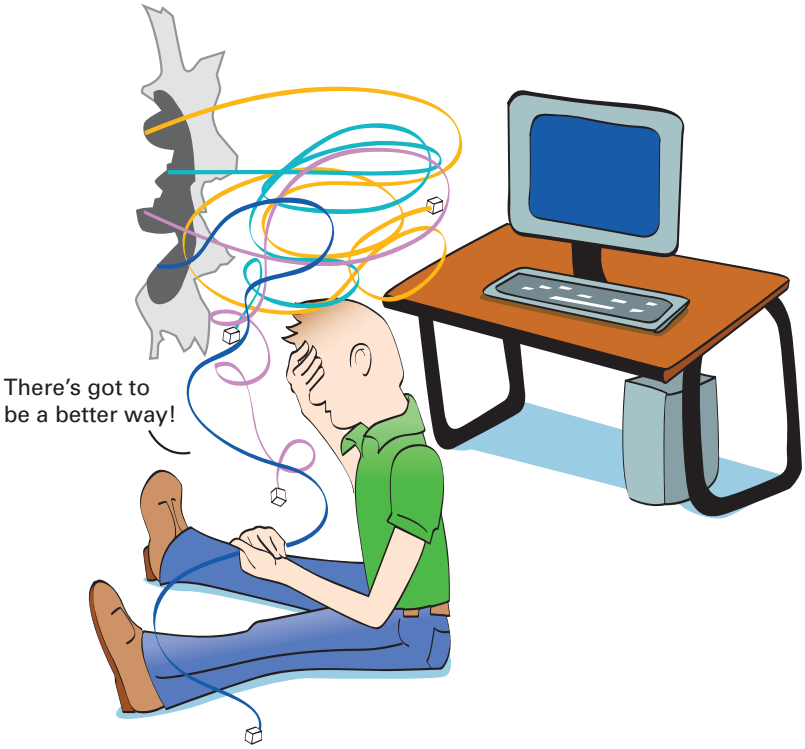
In a wireless network, air replaces the cables, and the same computer-to-computer communications are transmitted and received over the air using radio waves, very similar actually to how your mobile phone communicates.

This chapter discusses how wireless networks work and some of the challenges that had to be overcome to make them operate. If it gets too technical, just remember one thing: wireless networking is just a way to send stuff like web pages to and from your computer without a cable.



Why Wireless?

For those of you still on the fence about going wireless, we start this chapter off by trying to convince you that it is worth the time, effort, and money to go wireless, especially because it only takes a little of each to get started. The biggest reason for making the switch to wireless boils down to a single word: flexibility.



Wireless technology provides us with a great deal of flexibility when it comes to what devices we put on the network, how many devices we use, and where we put those devices. Let's look at an example. Suppose a family wants to connect to the Internet using broadband cable (this example works with any type of broadband). This family has three computers in the home, one for each parent and one for their teenager, and all family members want to connect to the Internet at the same time. First, they must determine where the cable jacks are located in the home and decide which one they want to connect to the cable modem. Is a cable jack close to where one of the computers will be used? If not, that's a problem. They have to either put a computer where they don't want one or string a long cable across a room.

After they decide which cable jack to use, they have to figure out how multiple computers can get access to it, because there is only a single cable modem. This means they either need to have a single device connected to the Internet at a time or need to buy a device (such as a router) that allows multiple computers to connect to the Internet simultaneously. They also have to decide how to connect all the computers in the house to the router.

At this point, the family has some options:

- Run cables through the walls. If the family were building a new house, they could have it wired throughout for Internet access, but this can be expensive. If they live in an existing home, they could hire an electrician to run cables, but that is really expensive and messy. If they rent, neither of these is an option.
- String cables all through the house. This is cheap, but it's messy and the family members will be tripping over cables all the time.
- Move all the computers to where the router is. This is not a very practical option.
- Go wireless.

Now, some folks may be a little dubious about using a "new" technology, but the ability to provide wireless networking actually has been around for a long time. The reason you have heard about it only recently is that its use was never really necessary previously. The need to provide high-speed network access to multiple, somewhat mobile, computers only emerged with the widespread availability of broadband Internet and inexpensive computers.

The bottom line is that wireless networking is reasonably affordable and easy to install. If you were to build a wired network, by the time you purchased wired network adapters for all your computers, a router to connect them, and all the cables, the price would be close to what a wireless system would cost. Considering the convenience and the absence of clutter, the wireless network is a bargain. Keep in mind that with most wireless routers, you also get four ports for wired access, so with a wireless network you get the best of both worlds.

Before We Get to the Wireless Bit, What the Heck Is a LAN?

The chapter title says we will teach you how wireless LANs work, so it is probably a good idea to start off with a brief description of what a LAN is—nothing overly technical, just some background information that may come in handy later.

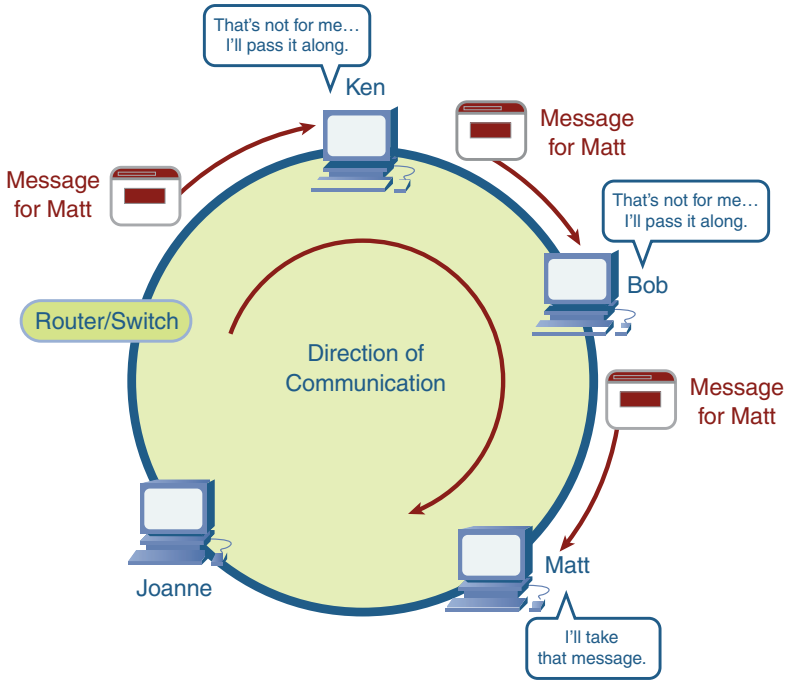
A local-area network, or LAN, is just what you think it might be, based on the name: a network connecting computers in a small or localized area. This area can be a house, a small office, or a floor of a building in a big office.

LANs form the basic building blocks of large-scale computer networks. LANs connect to other LANs to form larger corporate or institutional networks. These networks connect to larger networks that span large geographic areas. In some cases the larger networks cover a metropolitan area, called MANs. Still larger are networks covering multiple cities, states, countries, or even spanning the globe. Networks of this size are called WANs, or wide-area networks.

This structure provides a connection hierarchy that is very scalable. In fact, the Internet is the result of multiple WANs connected to each other, which in effect connects hundreds of thousands of LANs together along with the computers associated with those LANs. Think of your home network as one of those many networks.

When people first started connecting computers for networking, they used many different configurations and communication methods (or protocols). Some LANs were connected using a ring topology, where each computer is connected in a line, as shown in Figure 1-1. Communication from one computer to another is passed along the ring until it reaches the intended recipient.

Figure 1-1 Ring Topology



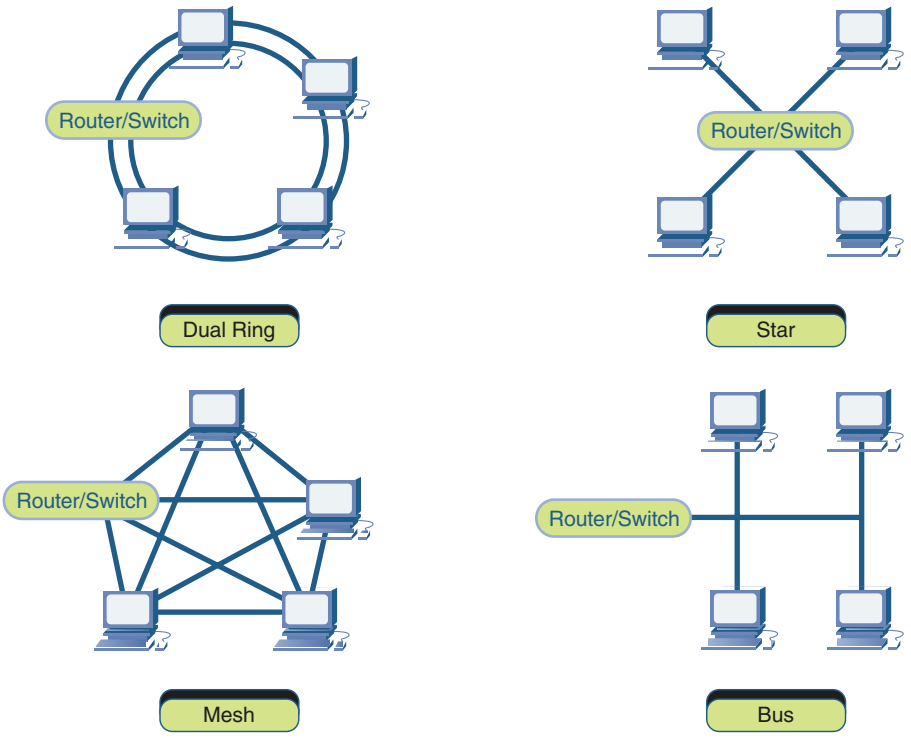
Other topologies included stars, meshes, dual rings, and buses. These configurations are illustrated in Figure 1-2.

Eventually, the topology that was (primarily) settled on was the bus topology. A bus topologoy has all the computers connected to a common cable, which is referred to as the bus. The common "cable" connecting all the computers today is located inside the router or switch, but it works the same way. Other topologies are still in use but most of the time LANs are connected using a bus topology.



Note: Routers and switches are similar in that they both provide a way to connect multiple computers together. The main difference is that switches typically connect only computers together, whereas routers additionally connect the home network to another network, such as the Internet. For a more thorough discussion on routers, switches, and other types of home networking equipment, pick up a copy of *Home Networking Simplified* (Cisco Press, 2005).

Figure 1-2 Common Network Topologies



Using the bus topology, one computer communicates with another computer by putting its message out on the bus. What is interesting here is that all the computers on the LAN receive the message. Contained in the message, however, is information about who the intended recipient is. Each computer receiving the message looks to see whether or not it is the intended recipient. If it is, it processes the message. The set of rules governing this type of communication is called the *Ethernet protocol*. If it is not, it ignores the message.

Figure 1-3 shows how this process works. When a message comes in from the WAN (for example, let's assume an e-mail comes in for Bob), all the computers on the LAN are notified of an incoming message. Matt's, Ken's, and Joanne's computers ignore the message because it is not intended for them. Bob's computer sees that it is the intended recipient and processes the message.

The same thing happens when a message is sent out. Let's say Ken wants to look at a web page. His computer sends out a request to view the contents of a web page (this is what happens when you type a URL or click a web link). In this case all the computers, including the switch or router, receive the request. Matt's, Joanne's, and Bob's computers see that the request is not intended for them so they discard it. The switch or router sees the requests and determines that the request is for a computer that is not on the LAN, so it passes the request over to the Internet service provider (ISP). This is illustrated in Figure 1-4.

Figure 1-3 LAN Communication: Incoming Message

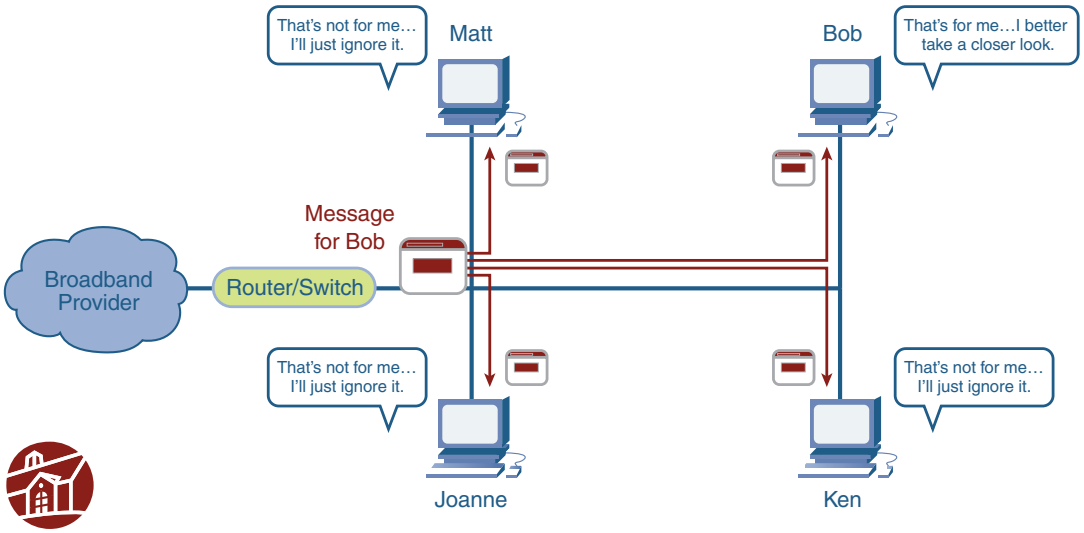
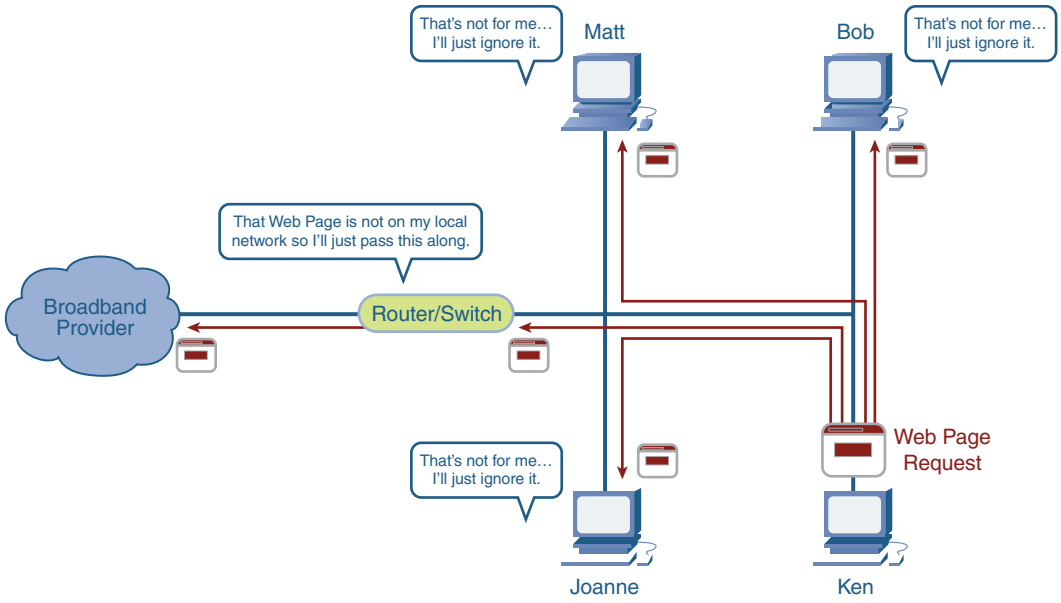


Figure 1-4 LAN Communication: Outgoing Message



While we have simplified this quite a bit, this is pretty much how communication works on a LAN. There are some pretty complex addressing (identification) schemes that are used and there are different protocols, or rules, for different types of communication, but most of them are beyond the scope of this book. The important point is this: Any communication to or from a computer on the LAN is seen by all other computers on that LAN, but is ignored by all but the intended recipient.

This means that if someone wants to "snoop" and monitor someone else's communication, all they have to do is physically connect to the wired LAN and make it so that their computer processes all

the traffic rather than just the traffic meant for that computer. The good news is that it is pretty easy to see if someone who does not belong is connected to the LAN. In an office you just have to follow the wires, since they need a cable to connect. In your house, it's the strange guy on the couch with a computer that you did not invite in.



Note: Chapter 5, "Wireless Security: What You Need to Know," and Chapter 9, "Wireless Security Setup," provide a good discussion about wireless network security and the steps you need to take to make your wireless network pretty secure. For an additional source of information about more general home network security, pick up a copy of *Home Network Security Simplified* (Cisco Press, 2006), which covers ten easy things you can do to make your home network more secure.

Okay, Now the Wireless Part

The wired Ethernet protocol and LANs had been around for a long time before wireless networking became practical. In fact, the world had pretty much standardized on wired Ethernet long before any of the wireless networking companies were even formed (the technology was there, but, as we mentioned earlier, there was no commercial need). In addition, the number of computers using wired Ethernet had exploded, and other devices were being connected to the network as well.

This meant that if someone wanted to have computers communicate over a wireless connection, they were going to have to create a standard that worked with, or at least be compatible with, the wired Ethernet standard. The millions of existing computers were not going to change the way that they communicated just because some nerds wanted to check their e-mail while sitting on the toilet. (Okay, we can't prove it, but we suspect this was one of the driving forces behind the whole wireless thing.)



Note: Other types of cableless connections include, infrared, Bluetooth, and powerline. Just to be clear, these are not what we refer to as a "wireless network." Most of these technologies are point-to-point, meaning computer to printer, or mobile phone to headset. They have very limited capabilities for multidevice networks. When we say "wireless networking" throughout the rest of this book, we are referring to Wi-Fi.

Challenges for Wireless Communication

To make wireless communication practical, the engineers had some problems to overcome, despite the fact that the basic technology had been around for a long time. Some of the key problems to overcome were the following:

- **RF signaling**—RF stands for radio frequency. Transmission of radio signals is tightly regulated in pretty much every country. There are open ranges of frequencies where you can transmit without a license so long as the power is low, and restricted bands which require a license and carry

heavy fines for unauthorized transmissions. Because of this, wireless networks work on the "open" frequency bands, but this leads to a few other issues.

- **Interference**—Because many other devices use the open frequency bands (including cordless phones and baby monitors), anything using these bands is prone to interference from other devices.
- **Power and range**—The rules for the open frequency band limit the power of transmissions. The problem here is that the lower the power, the shorter the range. Engineers had to develop a way to make sure the range was wide enough to cover your house, to make going wireless worth the cost.
- **Data rates**—Data rate is another way of saying speed. People had become accustomed to the speed of broadband Internet. If switching to wireless meant that it would take an hour to download a single e-mail attachment again (as with dial-up), then no one was ever going to use it. So wireless had to be about as fast as wired.
- **Interoperability**—If seven different companies solve these problems in seven different ways, the technology will not be very usable or commercially viable. To ensure that everyone can make some money, standards are needed to make sure that stuff from different manufacturers works together.

The Solution

The solution for wireless communication was something called 802.11, also known as Wi-Fi (pronounced "why fie"). We go into some detail about 802.11 in Chapter 2, "Wireless Standards: What the Letters Mean?" but for now just look at it as the name of the solution that some smart folks came up with that enables computers to communicate with each other over a wireless connection, without messing up the way computers were already talking to each other. We'll look at this in two parts: first the wireless part, and second how it works with the wired Ethernet protocol.

For all its magic, the technology that drives wireless communication is no more than a fancy walkie-talkie in a really small package. The wireless device—whether it is a card you plug in or electronics that are built right into the computer—is a transmitter and receiver, sending and receiving radio signals. Unlike the kids' walkie-talkies, however, these radios are capable of sending and receiving data at very high rates, from 10 Mbps at the low end to over 100 Mbps at the high end. Just a few years ago, these kinds of speeds were only possible using a cable to connect computers. The really good news is that the range of these wireless devices is good enough that you can put the wireless router in your home and provide access throughout most of your home and probably into areas of your yard. This is all done with minimal power consumption so that the battery on your wireless laptop does not drain too fast.

So now that we have computers that are capable of communicating over a radio link instead of a cable, let's look at how the smart folks made it compatible with the existing wired Ethernet protocol. As it turns out, there was really no way to make wired Ethernet wireless without changing every existing network in the world. To overcome this, the 802.11 team (comprised of engineers from many companies, universities, and other organizations) figured out that the best way to solve the problem

was to take the bits of information being sent via Ethernet and stuff them into the wireless signal, which was then transmitted and received using the radio technology mentioned earlier. On the receiving end, the Ethernet packet was then pulled out of the wireless signal and passed onto the computer, at which point all the normal rules for Ethernet applied.

Let's look at this a different way. Imagine that you and your friend have developed a system for passing notes back and forth to each other during a class in which you sit next to each other. You have developed a shorthand system so that the notes are small but still contain all the information you need to communicate. Now imagine that you find yourselves in another class but you are now seated on opposite sides of the room. You still want to communicate with each other, but you really don't want to develop a new system with which to communicate (such as sign language) because using two methods would really be a pain. Your friend gets a great idea and cuts a hole into a tennis ball and stuffs the note into it. She then throws the ball to you. You catch the ball, pull the note out, and write a response. You then take your note and stuff it into the ball, which you then throw back.

This is basically what the wireless LAN (802.11) protocol does with Ethernet communication. 802.11 wireless LANs act as a way to carry the same wired Ethernet conversations that computers are used to, but over the air instead of over a cable. Pretty neat.

Putting It All Together

Now, back to the network discussion. When computers are connected to a LAN, they are physically connected to each other, which is the basis for their association to that LAN.

With a wireless LAN, the computers have to find a way to connect, or associate, themselves to the LAN, because they are not physically connected. The way they do this is by tuning themselves to the wireless router using the name of the router (the wireless router's name is called the Service Set Identification number, or SSID). When you tell your computer to connect to an access point, the computer tunes to the access point's frequency and asks permission to join the LAN. If the access point is open, any computer asking to join the LAN will be allowed to do so. If the LAN has encryption security enabled, the computer needs to know the encryption key to even ask permission to join.

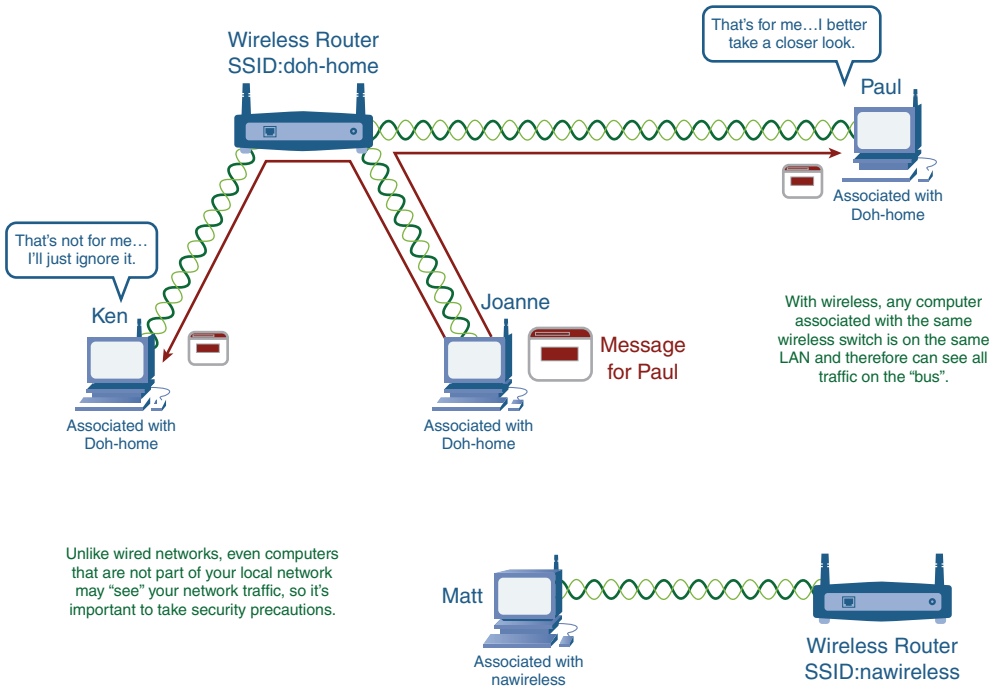


Note: In addition to *wireless router,* you may also see the terms *base station* or *wireless access point,* and all three pretty much mean the same thing in home networks. Well stick with *wireless router* for the rest of this discussion.

Once a computer has connected, or associated, itself to the access point, it becomes part of the LAN. And, as we mentioned before, if a computer is on a LAN, it then has access to every bit of communication that takes place on that LAN. Now the computer can send and receive information to and from other computers on the LAN or to and from the Internet by transmitting over wireless to the wireless router (or access point). The wireless router acts as the central communication routing point, much like the wired cable in the LAN example earlier.

Unlike a wired LAN, you cannot tell who is on your wireless LAN by following wires or casually looking around, as illustrated in Figure 1-5.

Figure 1-5 Wireless Network Environment



This is really the big risk with wireless: Someone can connect to your network without being in your house or being physically near your router. Now, it's not all bad, because there are some really simple actions you can take to prevent people from connecting to your LAN and your network, and we will show you how to take those actions in Chapter 9.

Summary

In a nutshell, all the computers on a LAN see all the network traffic regardless of who the intended receiver is. The computers just ignore all the stuff that's not intended for them.

In a wireless network, the same protocols or communication rules are used, the packets are just "stuffed" into a wireless carrier and then "unpacked" on the receiver end, and everything works the same way it does in a wired network. The big difference here is that any wireless computer in the range of the wireless signals can "see" the traffic even if it is not part of the LAN. This makes wireless very convenient, but it also makes the need for security very, very important.

The rest of this book takes you through all the considerations for wireless networking, including the standards, what equipment you need, how to apply security, and how to put it all together.

Where to Go for More Information

One of the best places on the web to learn about networking, wireless, and pretty much anything else you can think of is HowStuffWorks: www.howstuffworks.com.

Linksys also provides on its site some good information about wireless networking and how it works: www.linksys.com.

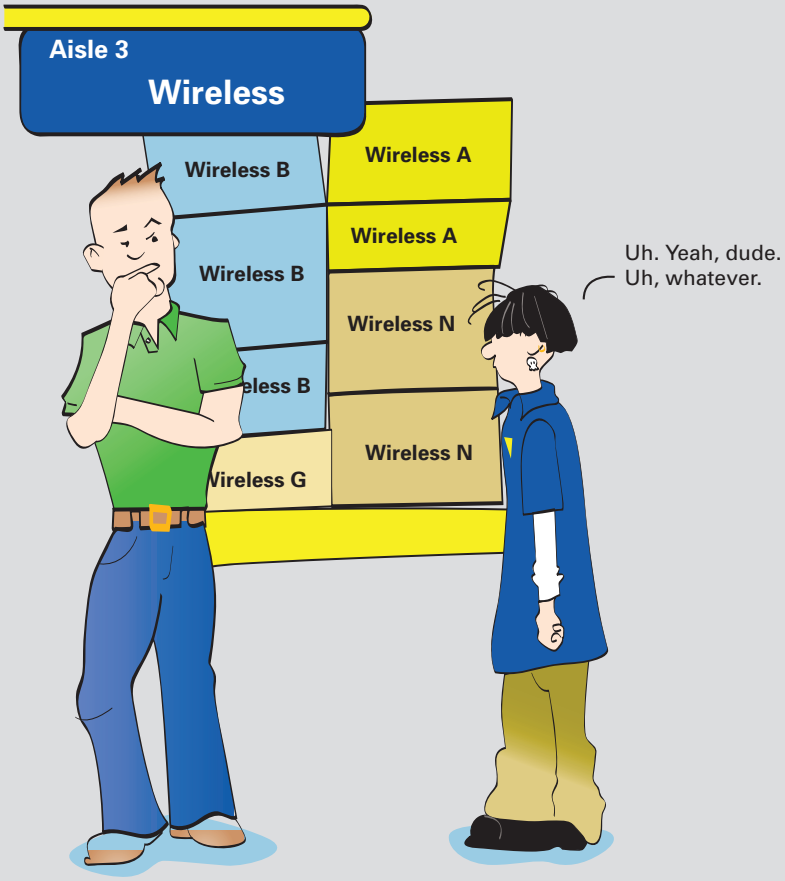
This page intentionally left blank

CHAPTER 2

Wireless Standards: What the Letters Mean

If you have already done some research about, or gone window shopping for, wireless networking stuff, you probably noticed that each piece of wireless gear has a letter (or letters) associated with it. The letters are usually A, B, G, N, or some combination such as A+G. In addition, the letters are usually prefaced by the words "wireless," "wireless standard," or "802.11." So it is possible that while shopping for a router, you could see boxes that say any of the following:

- Wireless B
- 802.11g
- Wireless A+G
- Wireless Standard N



You might also see boxes that include each manufacturer's own terminology, such as "SRX Technology," "MIMO," "Range Extension," "Speed Booster," "pre-N," or any number of other descriptions or marketing ploys.

You may have scanned the products on the shelves and left the store without purchasing anything because you had absolutely no idea what in the world you needed. This chapter helps you cut through all the confusion and explains what the letters mean, where they come from, and which ones work together.

The Standard 802.11 and the IEEE

Regardless of how the letters on the wireless equipment are presented, they all fall under a standard referred to as *IEEE 802.11*.

IEEE stands for the Institute of Electrical and Electronic Engineers. While this may not sound like a very exciting group of people, the IEEE is the worldwide standards body for all sorts of technologies, and it has greatly contributed to advancement of technologies ranging from the Internet, to the phone system, to DVDs, and much, much more. The IEEE standards ensure that nearly all devices, technologies, and parts (within the realm of electronics anyway) are standardized and agreed upon. Without such a standards body, it would be extremely difficult for all vendors to make gear that works together. Just think about how much of a pain it would be, for instance, if every stereo speaker manufacturer used different types of cables and connectors. This type of standardization also allows for very rapid innovations and price reductions because everyone with an interest in a technology works to further a single standard instead of multiple competing ones.

When a new technology comes along, the IEEE puts a workgroup together made up of engineers from multiple companies (often competing ones), government bodies, and universities to develop the standards for that technology. These workgroups are each given an identifier based on the nature of the technology. The workgroup that determines the standards for wireless networking is workgroup 802.11, which is also the name of the standard.

Once the workgroup develops the base standard, all subsequent additions, variations, or modifications are given a letter designation off the base standard. This is where 802.11a, 802.11b, and so forth come from. Because most people would not have a clue about what 802.11 is, most people just say "wireless standard," which is really the same thing.

The IEEE developed and approved the original wireless standard (802.11, without any other identifiers) in 1997. This standard was limited in that it had a maximum throughput of about 2 megabits per second (Mbps), which was pretty slow. There were other issues as well that impacted wide adoption, such as price and the fact that most people were still on dial-up access, which does not support the need for a wireless network with multiple computers behind it. 802.11 did get the whole wireless networking thing going, though, and was followed by a number of improvements.

802.11a

In 1999, two years after the original standard was developed, the IEEE published the standards for revisions A and B, both of which were different "flavors" of the original wireless standard. Wireless standard A was the faster of the two revised wireless types. It was a bit more costly to develop and therefore had much slower adoption than the B standard, which was used by most of the companies making wireless devices for home networking. Because of this, many people think that standard B came out before standard A. Given the fact that engineers develop these standards, that assumption is just silly. (If you are wondering, the convention is to use lowercase letters with 802.11 and uppercase letters when alone, for example, 802.11a and the A standard.)



Note: In the spirit of full disclosure, the authors made the statement that B came out before A in one of our previous books. It has also come to our attention that during the review of that book, one of our technical reviewers did in fact catch this error, and we ignored him. Sorry Bradley.

The A standard provides up to 54 Mbps, which is plenty fast for most home networking applications, including Voice over IP (VoIP) programs, such as Skype, running on your PC. In fact, if you have high-speed Internet access (which you really ought to if you are considering any type of wireless networking), even the slowest of the modern wireless standards provides more throughput (bandwidth) than the fastest home networking connection (cable, satellite, or even small business data service). The type of wireless standard you use generally does not affect the performance of your Internet access.

The 802.11a standard operates in an unregulated frequency range (5 GHz). *Unregulated* means that any product can use the range so long as the transmission power is not too strong. Because of this, your 802.11a-based router may get some interference from cordless telephones, baby monitors, and other electronics; however, we have found that there does seem to be less interference from these types of devices in the 5-GHz band than in the 2.4-GHz band, where 802.11b and 802.11g wireless networks operate. This will change as time goes on and more and more devices are made for the 5-GHz band.

The bad news is the equipment for the A standard tends to be a bit more expensive than the equipment for the other standards, and because the system uses a higher frequency range, the signal does not pass through walls or other obstacles as easily as the signals from the standards using lower frequencies (trust us, it's a physics thing). This means that in general the range of an 802.11a router will not be as good as other standards such as 802.11b and 802.11g, all other factors being equal. Table 2-1 provides a summary of the wireless A standard.

Table 2-1 802.11a Summary

Feature	Description
Frequency	5-GHz range
Throughput	54 Mbps
Pros	Fast Less interference from other electronic devices such as cordless phones (for now)
Cons	Range is limited More expensive than B or G Difficult to find compatible hotspots
Compatibility	Not compatible with 802.11b, 802.11g, or 802.11n

802.11b

802.11b was developed at the same time as the A standard. Because it was less expensive to develop, 802.11b is the standard that most vendors first developed for home networking. As a result, 802.11b is also the first standard that enjoyed widespread adoption and is still widely used in home networking and Internet hotspots (Internet cafés and public wireless locations) today. This standard operates at 2.4 GHz and offers up to 11 Mbps of performance.

802.11b is the slowest of the main wireless standards but it is also the least expensive and most widely deployed. Keep in mind, though, that the speed of the B standard (11 Mbps) is still faster than most forms of high-speed Internet access, so the only limitation will be the applications you run within your network. So, although this standard would not work well for sending high-definition video over your wireless network within your home, it should be just fine for downloading video clips from YouTube (www.youtube.com).

802.11b has a range of about 150 feet (maximum) in open air before signal degradation becomes noticeable. The frequency used by the B standard is also unregulated, and you will find that many devices that use radio transmission (baby monitors, cordless phones, Bluetooth, and others) also use this frequency band and may interfere with your wireless router signal. We'll talk about this a bit more in Chapter 3, "Selecting the Right Wireless Standard for Your Network."

Table 2-2 provides a summary of the wireless B standard.

Table 2-2 802.11b Summary

Feature	Description
Frequency	2.4 GHz
Throughput	11 Mbps
Pros	Least expensive of the wireless standards Most widely deployed Range is good Used by most hotspots
Cons	Slowest of the wireless standards Prone to interference from other devices
Compatibility	Compatible with 802.11g and 802.11n Not compatible with 802.11a

802.11g

The 802.11g standard was developed in 2003 and borrowed from the best of the two previous standards (A and B). Wireless G offers the speed of the A standard (54 Mbps) but still operates on the unregulated 2.4-GHz frequency band, which provides the cost and range benefits of the B standard. Since its inception, the G standard has proven to be very popular and is very quickly replacing the B standard. The equipment cost for this standard is a bit more than for the B standard but less than for the A standard. The G standard is starting to become widely available in hotspots, and many computers that come with built-in wireless capabilities (which is most of them these days) come with G capability. This standard is also backward compatible with the B standard, so if you find yourself near a router using the B standard, your G-capable computer can communicate with it (the opposite is also true).

Some additional proprietary upgrades to the G standard make it even faster (up to 108 Mbps). Linksys has two flavors of speed enhancement. The first is called *Speed Booster*, which, as you might have guessed, boosts the speed (although Linksys only claims 54 Mbps+). The other enhancement is called *SRX*, which stands for Speed and Range eXpansion. Linksys claims that its top-of-the-line version of SRX provides 10x speed and 3x range enhancement. We have not done laboratory tests to measure this but the SRX routers do provide a noticeable improvement in both speed and range.



Note: We do not recommend buying and deploying such proprietary extensions of the 802.11g or other standards. They have several limitations, including two important ones:

- You do not get the additional performance unless your wireless router and wireless NICs are both using the proprietary scheme. Buying an SRX router, for example, and using plain old 802.11g wireless NICs means you get 802.11g performance and no SRX enhanced performance.
- Proprietary extensions can lead to incompatibilities with standard equipment.

Therefore, we recommend you stick with one of the standards and be wary of proprietary manufacturer extensions.

Table 2-3 summarizes the wireless G standard.

Table 2-3 802.11g Summary

Feature	Description
Frequency	2.4 GHz
Throughput	54 Mbps
Pros	Very good speed Available at most hotspots Good range Less expensive than A
Cons	More expensive than B Prone to interference from cordless phones and other electronics
Compatibility	Compatible with 802.11b and 802.11n Not compatible with 802.11a

802.11n

The newest standard is designated as wireless standard N, scheduled to have final approval by the IEEE in 2007 (originally it was 2006, but it was not ratified). Prior to the final approval, several vendors have begun to offer products for this standard based on the initially released specifications. Users who buy the products now should be OK even if there are changes to the standard in the mean time (which, if there are any, are likely to be minor and would only require an additional software or firmware download).

The N standard achieves much higher speeds than the G standard using a technology called multiple inputs, multiple outputs (MIMO). MIMO does exactly what you might expect: It uses several radio-based connections (in both directions) to achieve very high (100 Mbps+) speeds (also called bandwidth, throughput, or capacity) and extended ranges. In addition to using multiple radio streams, MIMO also takes advantage of reflected signals (radio signals that "bounce" off of walls, ceilings, or other obstructions) to enhance the strength of the signal and, therefore, improve the transfer rates and range. This feature also greatly reduces "dead spots" within the operating range of the router, meaning that it can cover more of your house with fewer signal problems.

Wireless standard N provides the bandwidth necessary to run applications such as streaming high-definition video signals, digital music or interactive multiplayer video games, within your home over your wireless network.

The N standard is also backward compatible with the G and B standards, so you will not have to replace the wireless cards in all your PCs in the event that you buy an 802.11n router to stream high-definition video from a single computer or device. Table 2-4 provides a summary of the wireless N standard.

Table 2-4 802.11n Summary

Feature	Description
Frequency	2.4 GHz
Throughput	100 Mbps+
Pros	Very high data-transfer speeds Greater coverage range No dead spots in coverage
Cons	Still new so you may not find many hotpots that offer it (although if you have N on your computer, it will work with an 802.11g system) The most expensive of the wireless standards (at the time of this writing, but eventually it will be as cheap as the others)
Compatibility	Compatible with 802.11b and 802.11g Not compatible with 802.11a

Combinations

You may see some wireless routers or devices that offer multiple wireless standards such as A+B. These devices work on only one standard at a time with any given device. In other words, if you have a computer that uses the G standard, it can use only that standard. You will not get the benefits of both standards on any single device. Chapter 3 covers how to choose a standard in detail.

What Happened to the Other Letters?

At this point you may be wondering what happened to the other revisions. As it turns out, the revisions to the 802.11 standard do not always involve new wireless standards. In many cases the revisions are updates to the communication protocols, which, by themselves, do not warrant a new wireless standard. For a complete list of the other revisions, check out Appendix C, “802.11 Additional Revisions,” which is provided for information purposes only. These updates have limited relevance for the home networking crowd.

Summary

The 802.11 standard specifies how wireless works and communicates with both devices and the network. Although there are many 802.11 specifications, only four have any relevance to the purchasing decisions of the home user (standards A, B, G, and N). How you choose the right standard for your situation is the subject of Chapter 3.

It is also important to note that we most likely have not seen the last of new wireless standards. Because wireless is such a relatively new technology, there are bound to be more improvements.

Finally, because wireless networks use radio transmitters at particular frequencies that are authorized by governments, do not assume that the wireless router you purchased in your country can safely be used in another country. Research the standards for the country you wish to visit to make sure it uses the same frequencies as the wireless equipment you purchased.

Where to Go for More Information

Wi-Fi Planet is a good site for general information about wireless networking, providing a plethora of articles and tutorials. For this chapter, we referenced the tutorial "802.11 Alphabet Soup" by Jim Geier at www.wi-fiplanet.com/tutorials/article.php/1439551.

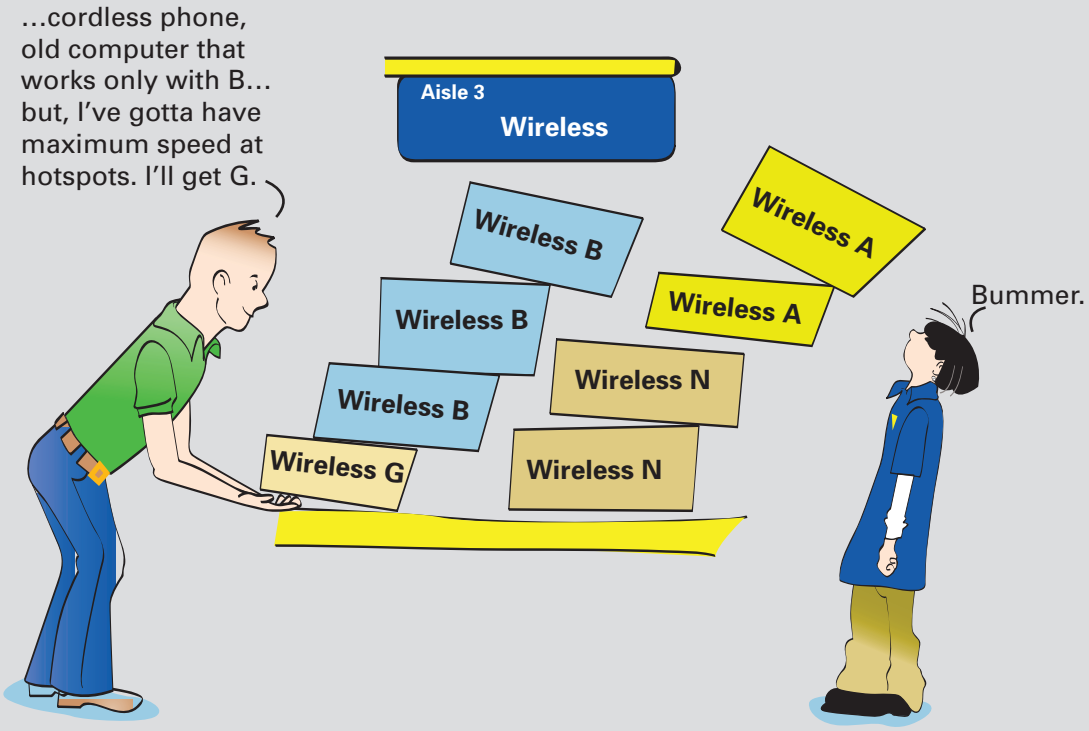
Linksys also provides a great deal of information about the various wireless standards at www.linksys.com. Click **Network Basics** on the Learning Center drop-down menu and then click the **Wireless Standards** tab on the left side of the page to access the information.

CHAPTER 3

Selecting the Right Wireless Standard for Your Network

If you have looked around at your local technology store for wireless networking equipment, you probably noticed the array of wireless designations. With several broad-based standards available and even more vendor extensions, it's no wonder people leave the store confused and probably empty handed.

This chapter helps you choose which wireless standard is right for you. The decision does not have to be difficult at all. We try to boil the facts down and make it easy.



What to Consider When Choosing Your Wireless Standard

So how do you sort through the many wireless options that are available to you and decide what's best for your home network? First, you must keep in mind that there are two sides to this decision process:

- What to choose for the wireless access point/router that will "host" your wireless network
- What to choose for wireless network interface cards (NICs) that will allow the computers on your home network to "join" the network wirelessly

The previous chapters covered the various wireless standards that exist and the advantages and disadvantages of each. Knowing the frequencies and other facts about the various standards is all well and good, but you still need to make a decision that will work well for you not only now, but also for at least a couple of years so that you can recoup the investment you made. In our opinion, you need to weigh the following six primary factors:

- **Compatibility**—How well will all your wirelessly connected stuff work together?
- **Speed**—How fast is fast enough?
- **Range**—How far from the router can I get a wireless signal?
- **Security**—What level of security is supported?
- **Cost**—How much?
- **Future proofing**—Will the technology be obsolete the day after I buy it?

As it turns out, compatibility and speed are intimately related. The following sections explore all six factors, followed by our bottom-line recommendations.

Compatibility

Whatever wireless standard you choose, it's very important that the wireless router and wireless NICs are compatible. Otherwise, your wireless network will not work at all or, at best, will work rather poorly.

There are three primary factors to consider for compatibility:

- What are the relationships between the standards, and which standards are compatible with each other?
- How does multi-standard, or dual-band, equipment fit into the picture?
- Are the proprietary extensions offered by manufacturers, like SRX, something you should consider?

We examine these questions in the following sections.

Relationships Among Wireless Standards

The first really important point to understand is the relationships among the wireless A, B, G, and N standards, introduced in Chapter 2, "Wireless Standards: What the Letters Mean." As previously mentioned, NICs need to be compatible with the wireless router you purchase or your router won't be of much use to anyone. Fortunately, the relationships are pretty straightforward:

- A NICs are compatible *only* with A routers.
- B NICs are compatible with B, G, and N routers.
- G NICs are compatible with B, G, and N routers.
- N NICs are compatible with B, G, and N routers.

Likewise, the relationships work in both directions such that a G router is compatible with B, G, and N NICs.

The key point to remember is that the lowest standard (in terms of speed) shared by the router and the NIC dictates the performance of the interaction between the two devices. This means that N and B devices work together, but only at the B level of performance. Figure 3-1 and Figure 3-2 illustrate this concept.

Figure 3-1 B NIC on Different Routers

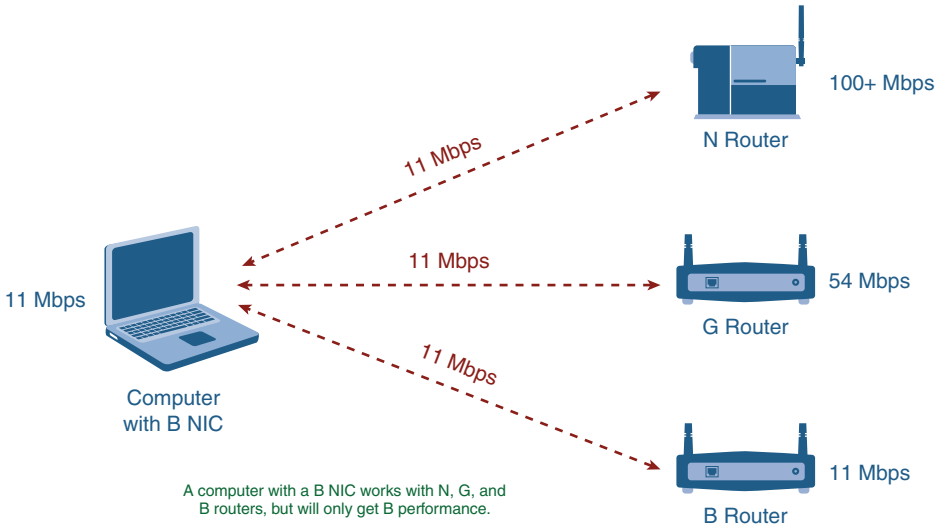


Figure 3-2 G Routers with Different NICs

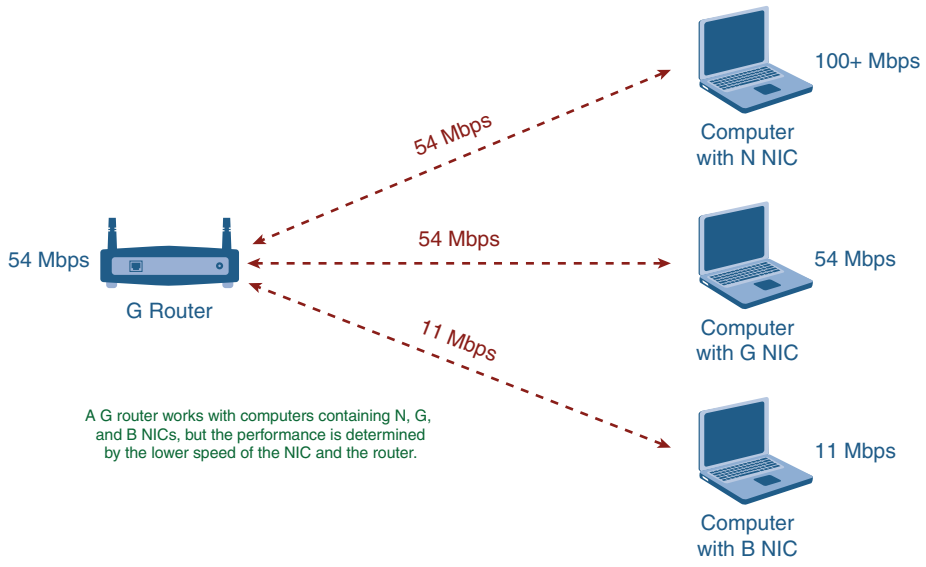


Table 3-1 summarizes the compatibility between standards and the performance you will have when combining NICs and wireless routers.

Table 3-1 Wireless Standards Compatibility Summary

	A Router	B Router	G Router	N Router
A NIC	A performance	Not compatible	Not compatible	Not compatible
B NIC	Not compatible	B performance	B performance	B performance
G NIC	Not compatible	B performance	G performance	G performance
N NIC	Not compatible	B performance	G performance	N performance

Dual-Band Products

Another point to consider is that some manufacturers provide *dual-band* (also known as *dual-standard*) wireless NICs and routers, meaning that the product supports two bands. As discussed in Chapter 2, 802.11a operates in the 5-GHz band, while 802.11b, 802.11g, and 802.11n all operate in the 2.4-GHz band. The designation of a router or NIC as *dual-band* means that it supports at least one wireless standard in each band, meaning 2.4 GHz and 5 GHz.

By definition, G routers and NICs are dual-standard, because they are backward compatible with the B standard. So, *dual-band* almost always refers to the wireless A standard, plus another standard like B, G, or N. Thus, you will see products labeled A+B and A+G. You will likely see some A+N routers as well. The same holds true for wireless NICs. You can have NICs that are single-band only, such as B or G, or dual-band, such as A+G.

Proprietary Extensions

The next complication is that some vendors provide proprietary extensions to their products to make them run even faster. For example, we mentioned in Chapter 2 that Linksys provides a Speed Booster version of its wireless G products that improves the transmission speed beyond the standard 54 Mbps. Linksys also provides an SRX series of wireless G products that doubles the speed to 108 Mbps. Other vendors have similar product extensions. You need to understand three things about such extensions:

- They are (or should be) backward compatible with the base standard.
- The extended speeds typically work only when you are using both that vendor's NICs and its routers with that particular extension. So, to get the benefits of SRX, you need to have both an SRX router and an SRX NIC.
- If you already own or intend to purchase a laptop with a built-in NIC, it most likely is not going to support such proprietary extensions.

Remember this when you are thinking of buying products with such extensions. Make sure they are compatible with the base standard, at a minimum. You should also make sure that you have the correct NIC for any manufacturer-based extensions. It would be a waste to pay the extra money for the Linksys SRX router, for example, if your NIC supports only the base G standard.

Speed

The second consideration when choosing your wireless standard is resulting speed. Later in the chapter, in the section "Comparing the IEEE WLAN Standards," Table 3-2 gives an indication of the performance you will receive when you use a type of wireless NIC with a type of wireless access point/router. In general, the maximum performance the different wireless standards offer follows:

- **802.11a**—54 Mbps
- **802.11b**—11 Mbps
- **802.11g**—54 Mbps (up to 108 Mbps with extensions)
- **802.11n**—100 Mbps+

However, these speeds are the "stated" numbers, which are often only achieved in a lab setting. Once you have a router in your house, any number of factors can come into play that impact the speed you actually get. These factors include the distance between the router and the computer, the building materials in your home, interference from cordless phones and other devices, and, in some cases, even sunspots. Okay, that last one is pretty rare, but it can happen, and the basic point is that many factors—most of which are out of your control—affect the actual speed of the router.

Also, at the risk of being redundant, remember that the lower of the NIC and router speeds dictates the speed. For example, a NIC for the 802.11b standard will certainly function with a wireless router for the 802.11g standard, but it will only operate at the 11-Mbps rate, not the higher 54-Mbps rate of the G standard. Similarly, a NIC for the 802.11g standard will work just fine with a wireless router for the 802.11b standard. It will just operate at the slower 11-Mbps rate of the B standard.



Note: It is important to realize that even the slowest of the wireless standards often provides greater bandwidth than even the fastest residential high-speed Internet connection at the time this book was written. Average broadband provides download speeds (from the Internet) between 1 and 2 Mbps, and upload speeds (to the Internet) between 256 kbps and 1 Mbps). Even very high-speed broadband provides download speeds up to 6 Mbps and maximum upload speeds of around 2 Mbps (and at a price premium).

Even the lowest-speed wireless standard, 802.11b, operates at 11 Mbps and, factoring in the wireless overhead, delivers about 6 Mbps. This can pretty easily keep up with most broadband connections.

The point is, before you go and spend a lot of money on the very fastest wireless router, be sure that you really need the speed you are paying for.

Range

In general, the range of most current wireless routers on the market is adequate for the average house or apartment, so it's not really something to be very concerned about.

If you do have a large house or area you want to cover with your wireless router (maybe you want to lie by the pool or mount your laptop to your John Deere riding mower), then you may want to consider range as a factor.

Wireless B and G offer about the same range. Wireless A operates in the 5-GHz range and therefore signals last a shorter distance. Wireless N is specifically designed to provide up to four times the range of wireless B and G, and therefore offers the longest range on the market today. Keep in mind, though, that the closer you get to the maximum range, the lower the speed will be and, in some cases (such as with B), the speed at the edge of the range will be quite slow.

Security

Most new wireless routers on the market support the full range (or nearly so) of wireless security options available. There are two primary security-related factors to look for:

- What types of encryption are supported?
- Does the wireless router also provide a firewall?

Encryption comes in a number of "flavors" including (from least to most secure) WEP-64, WEP-128, WPA, and WPA2. Similar to wireless standard and speed, encryption that can be used is determined by the lower of the encryption supported between the router and NIC. You want WEP-128 at a minimum, but WPA or WPA2 is preferred. See Chapter 5, "Wireless Security: What You Need to Know," and Chapter 9, "Wireless Security Setup," for a more thorough discussion on wireless security types and recommendations.



Note: Unlike the wireless standard performance, with encryption the lowest available standard determines the type of encryption for all devices on the network. In other words, if you have a NIC that is limited to WEP-64 on your network, all the devices on the network must be set to encrypt at the WEP-64 standard regardless of any higher encryption standard that they are capable of.

The other factor to consider is whether the wireless router you buy contains a built-in stateful packet inspection (SPI) firewall. *Stateful* means that the firewall looks inside the packet to make sure it is part of a valid communication session. Basically it keeps hackers from "tricking" your computers into talking with their computer. This provides a good level of security between your home network and the Internet, and we highly recommend it.

By the way, the type of encryption and whether or not a firewall is included are completely independent of the wireless standard supported by the router. In other words, all types of encryption are possible with all the wireless standards. It's just a matter of determining what types of encryption are supported by the wireless router and NIC you have or are considering buying.

Cost

Costs have come way down for wireless networking, to the point that it is almost the same cost to put up a wireless network as a wired one. Wireless NICs can be more expensive than wired NICs, but costs are falling rapidly. The latest (and fastest) wireless standard (at this time N) tends to be the most expensive option, followed by the next fastest speed (A and G at this time), and finally the slowest wireless standard (at this time B). The gap is rapidly closing as prices come down across the board; however, you pay a price premium for faster speed.

It is getting pretty difficult to find wireless B equipment still for sale because it has been replaced for the most part by wireless G equipment.

Additional Considerations

When making your decision, you need to consider a couple of other points, including

- What types of wireless NICs do you already own versus what you must go out and purchase? Many new laptops (and even some desktops) are sold with built-in wireless NICs.
- Do you want to be able to use wireless network access outside your home in a publicly provided wireless network (hotspot)?

The last thing you want to do is purchase a wireless router only to find out that you need to replace a wireless NIC that came with your laptop because it is not compatible. Similarly, you will be quite frustrated if you buy a wireless NIC for your laptop, intending to use it at hotspots, only to find out you bought the wrong standard.



Note: Wireless NICs come in various form factors, including PCI for installing in desktop computers, PCMCIA and Express Cards (plug-in cards) for installing in laptop computers, and USB for connecting to any computer or device with a USB port. Choose whichever makes sense for your network, computers, and budget.

Comparing the IEEE WLAN Standards

With the preceding considerations in mind, it's time to make a choice between wireless standards. Table 3-2 provides an easy-to-read, side-by-side comparison of the four standards. This table should help you figure out which standard is right for you.

Table 3-2 IEEE WLAN Standards Comparison

	A	B	G	N
Speed	Up to 54 Mbps	Up to 11 Mbps	Up to 54 Mbps (faster with proprietary extensions)	100 Mbps or faster
Cost	$$$	$ (Finding new equipment for sale is difficult. You may have to purchase via alternative channels such as eBay.)	$$	$$$$
Frequency	Uncrowded 5-GHz band. Can coexist with 2.4-GHz networks without interference.	More crowded 2.4-GHz band. Some conflict may occur with other 2.4-GHz devices, such as cordless phones, microwaves, and so on.	More crowded 2.4-GHz band. Some conflict may occur with other 2.4-GHz devices, such as cordless phones, microwaves, and so on.	More crowded 2.4-GHz band. Some conflict may occur with other 2.4-GHz devices, such as cordless phones, microwaves, and so on.
Range	Shorter range than 802.11b and 802.11g. Typically, 25 to 75 feet indoors.	Typically, up to 100–150 feet indoors, depending on construction, building material, and room layout.	Typically up to 100–150 feet indoors, depending on construction, building material, and room layout. Much farther with extensions such as Linksys SRX.	150–400 feet is claimed although this has not been widely verified on the high end.
Hotspots	Very few hotspots support the A standard.	Most hotspots support the B standard.	The number of public hotspots supporting the G standard is growing rapidly, allowing wireless connectivity in many airports, hotels, public areas, and restaurants.	Very few hotspots support the N standard, but your N NIC will work with G or B hotspots.

Table 3-2 IEEE WLAN Standards Comparison

	A	B	G	N
Key Benefits	Good alternative if the 2.4-GHz band has too much interference.	Widely supported.	Good mix of speed and broad support.	Blazing-fast speed for high-end networking applications.
Shared Internet Connection	✓	✓	✓	✓
Multiplayer Gaming over Internet	✓	✓	✓	✓
Multiplayer Wireless LAN Games			✓ (with speed extensions)	✓
VoIP	✓	✓ (Performance can be an issue in some cases.)	✓	✓ (over Wireless)
Streaming Audio			✓	✓
Streaming Video			✓ (with speed extensions)	✓
Large Homes		✓ (Keep in mind that speed greatly suffers at the edge of the usable range.)	✓ (with speed extensions)	✓

Recommendations

Based on the information in Table 3-2, here are our bottom-line recommendations:

- If you just want Internet access, are on a tight budget, or do not anticipate a large amount of internal traffic (from a wireless juke box, for example), either the B or G standard is a good choice. Choose B only if you already have B-only NICs for most of your computers.
- B equipment may be hard to find for sale in retail locations because it has been mainly replaced by G equipment in the market, so if you can't find B, go with G.
- If you plan on using hotspots or getting on other people's networks, G offers the best bet for compatibility and speed.
- If you anticipate a large amount of internal traffic, plan on setting up a wireless gaming system, or want a little bit of future-proofing, N is the best choice. Purchasing G with an extension such as SRX will give you similar performance, but as N begins to gain popularity (and it will), a proprietary G extension will limit your flexibility.

We do *not* recommend the A standard unless you happen to have a specific reason to avoid using B, G, or N. For example, if you are getting known interference from 2.4-GHz cordless phones, or if you live in an apartment and you are surrounded by G routers, A might be an option. Keep in mind, though, that cordless phones are now also being offered in the 5-GHz range, which can potentially interfere with wireless A networks.

For the purposes of helping the broadest group of readers, we will hedge our bet just a bit and show the setup and configurations for both an N and a G router throughout the remainder of this book.

Summary

There are several important factors to consider when choosing your wireless standard, including compatibility, security levels supported, and the performance you expect.

B, G, and N devices are compatible with each other and offer the most opportunity for compatibility outside your network as well, at wireless hotspots.

Standard A equipment works only with other A equipment. Unless you have an explicit need for wireless A, avoid building out an A network.

If you have typical requirements for speed and range, a G network usually is sufficient. If you need extra speed inside your home for streaming video, heavy gaming, or other wireless applications, or you need significant extra range, then an N network is probably a better bet.

Where to Go for More Information

To learn more about wireless A, B, and G standards, check out Bradley Mitchell's article on About.com titled "802.11 Standards—802.11b 802.11a 802.11g": http://compnetworking.about.com/cs/wireless80211/a/aa80211standard.htm.

Space.com has an interesting article about interference from sun spots: www.space.com/scienceastronomy/solarsystem/sunspot_detail_021113.html.



PART II

PART II

What You Should Know

Chapter 4 Planning Your Wireless Network

Chapter 5 Wireless Security: What You Need to Know

Chapter 6 What to Buy

Now that we have provided you with information on how this wireless networking stuff works, we provide the information you need to plan out your wireless network and get ready to set it up.

In Chapter 4, "Planning Your Wireless Network," we provide you with a method for figuring out how and where you will be using your wireless network. This is a pretty simple step but it is important because it could keep you from buying products you don't need, or at least keep you from making multiple trips to the electronics store.

Chapter 5, "Wireless Security: What You Need to Know," provides some critically important information regarding wireless security. If you are not yet convinced that you need wireless security, this chapter should change your mind. Even if you are a believer in security, you might want to give this a quick read through because there have been quite a few updates in this area in the last couple years.

Part II finishes with Chapter 6, "What to Buy." Lots of gadgets out there claim to improve your wireless networking experience. This chapter provides you some guidance on what is necessary, what is cool, and what should be avoided.

CHAPTER 4

Planning Your Wireless Network

The first step in building your wireless network is to sit down and do some planning. Sure, it's fun to run out and start buying stuff, but a little time spent up front will save you a lot of frustration and rework time later.

Wireless Network Topologies

Before laying out the wireless network, we need to discuss the basic concept of wireless network topologies. There are essentially two types of wireless networks:

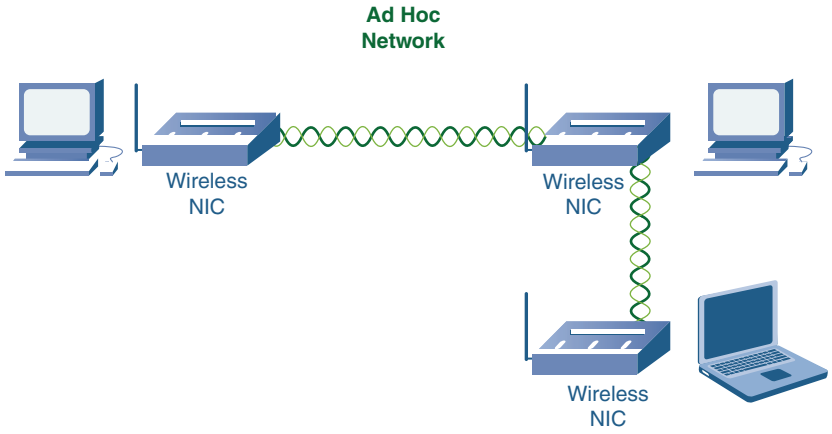
- Peer-to-peer (also called *ad hoc*)
- Peer-to-access point (also called *infrastructure*)

A peer-to-peer (or ad hoc) wireless network does not have a central point of access or control. Every computer on an ad hoc network is considered an equal "peer," having the same rights and access as any other computer on the wireless network. In other words, all the computers communicate directly



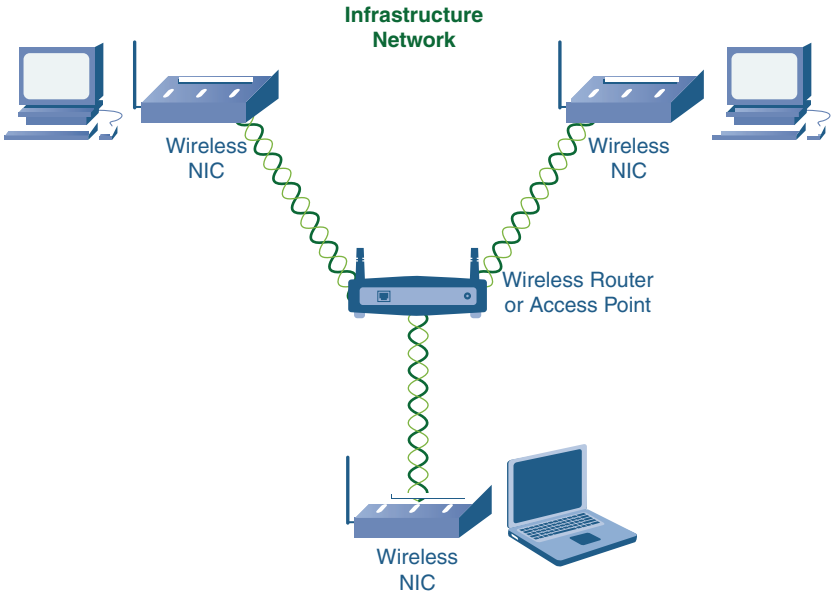
with each other, without going through an intermediary device. Any computer with a wireless network adapter (also called a network interface card [NIC]) may connect to any other wireless NIC. Figure 4-1 shows an example.

Figure 4-1 Peer-to-Peer Wireless Network



In a peer-to-access point (or infrastructure) wireless network, a central wireless "base station" provides the rendezvous point for all the wireless NICs on the network. In this case, each computer on the network always communicates only with the base station, or wireless access point, and never directly with other computers on the network. Figure 4-2 shows an example.

Figure 4-2 Peer-to-Access Point Wireless Network



Although you can set up a peer-to-peer wireless network and use a computer with a wired Internet connection to provide Internet access to your other computers, we are not big fans of that style of wireless network, for the following reasons:

- Because no central authority determines who can join the wireless network and who cannot, security becomes a real concern.
- One of the computers must be designated as the owner of the high-speed broadband Internet service and provide gateway access for all the other computers on the home network, which can end up being very restrictive.
- Because of the reason just mentioned, if the Internet gateway computer is not turned on, all other computers on the home network will not be able to access the Internet.

A peer-to-peer network offers a small cost advantage because it is not necessary to purchase a wireless router or access point, but in the end we feel strongly that it is just not worth the money you save.



Note: We assume that you will take this advice, and the "how to" sections of this book are based on this assumption. You should know, however, that even if you do use the infrastructure type of networking, you need to manually disable the ad hoc networking capability on your wireless-enabled computers. Failure to do so presents a significant security risk. Chapter 9, "Wireless Security Setup," provides a step-by-step guide on how to turn this feature off.

Sketching a Network Layout

In our opinion, the best way to start planning your wireless network is to create a drawing or sketch of the area (floor plan) in which it will be used. You don't need architectural drawings, just a simple floor plan (all floors and a rough idea of the room sizes). If you plan to (or want to) use your computer outside (for example, near a pool or on a patio in the backyard), you should include that area in the drawing as well.

Once you have the sketch completed, you need to figure out where you want (or need) to place the wireless router and where your computers and other devices that will be wireless are going to be used. If for some reason the location of your broadband modem (and therefore your wireless router) must be in a specific location, put a mark in that room on your drawing. If you have some flexibility with the location of your modem and router, put the same mark in the rooms where you have the appropriate port for Internet access (cable, DSL, or other). Figure 4-3 shows an example completed sketch. We used a red circle with an *I* in it to denote where we could put an Internet connection. You can use whatever marks you like; keep a legend on the side of the paper so you know what you meant.

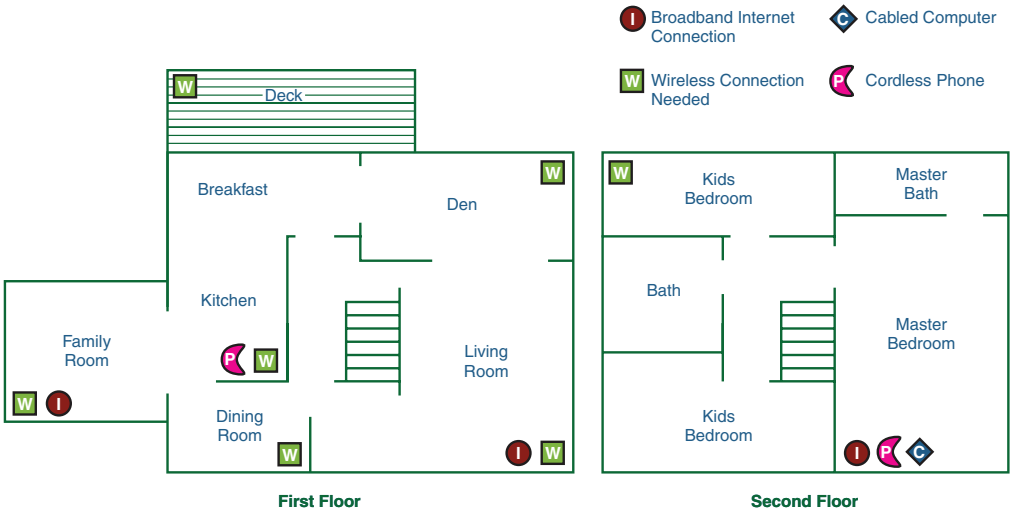
Next, put a mark in the rooms where you are likely to have a desktop computer, or other wired device such as a storage server, or network printer. In Figure 4-3, we used a blue diamond with a *C* in it to denote where we want to have a wired network connection, like a desktop computer.

Finally, put a mark in the rooms or areas where you can conceive of using a laptop computer and other wireless devices, including video cameras, printers, video game consoles, and so on. (This would include bathrooms, which we admit to using our computers in.)

In Figure 4-3, we used a green square with a *W* in it to denote where we want to have a wireless network connection, like a laptop.

In addition, if you have a cordless phone system that operates in the 2.4-GHz band (it should be written on the phone somewhere), you may want to mark the location of the phone's base station on the sketch. As we mentioned before, these phones can cause interference with your network if the wireless router is too close. In Figure 4-3, we used a pink moon with a *P* in it to denote where we currently have a cordless phone base station.

Figure 4-3 Sample Sketch of a House



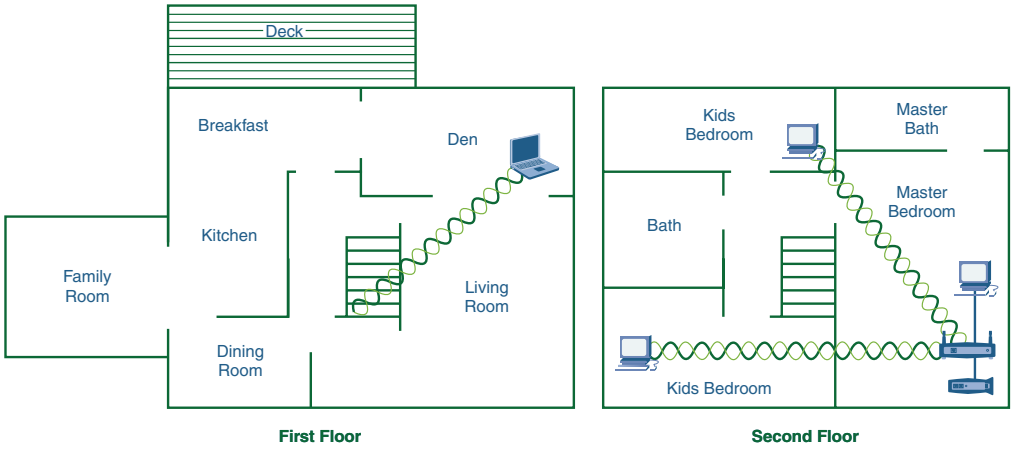
From the sketch, you can make some decisions about where you will put your wireless router, which computers will have wired connections, and which computers will have wireless connections.

Suppose, for example, that you have two desktop computers (a spouse's and a son's), one personal laptop (a daughter's), and one work laptop (yours). Suppose you also happen to have cable outlets in three areas of the house (master bedroom, living room, family room).

You need to have at least one computer with a wired connection (at least during initial setup and sometimes when changes are required). In this example, the family decides to have the high-speed broadband service installed to the outlet in the master bedroom. The wireless router can be placed next to the cable modem and the "Spouse" desktop computer. All three of these devices will be cabled together with Ethernet cables.

Because the daughter's laptop and the son's desktop computer are in other bedrooms of the house, and not easy to run Ethernet cables to, these computers will have wireless connections. The last computer is the work laptop, which is used primarily in the den, but could also be used in the living room, breakfast nook, and on the back deck. Wireless is definitely the way to go for this laptop as well. By jotting these requirements into the sketch, we have what's shown in Figure 4-4.

Figure 4-4 Adding Wired and Wireless Computers to the Sketch



For your network, determine the best location for the modem and wireless router based on your planned usage. Usually, the most central point of the house where you can set up a modem and router is the best option. If you live in a huge house, you may need a signal repeater or range extender, or a high-gain antenna. We will cover these types of devices in Chapter 6, "What to Buy," and recommend that you try a basic router first to see if the performance is adequate.

Chapter 11, "Troubleshooting: I Can Connect Sometimes," also contains some good advice on where to site your wireless router. We recommend reading that chapter before you finalize your network plan. By spending a little extra time up front understanding the trouble you could have, you could end up saving a lot of time and frustration later.

For now, mark the best available spot for your broadband modem and wireless router with an *X*. In this example, we chose the master bedroom because it has an available broadband connection jack, has a wired desktop computer (important for administration), and is fairly centrally located.

Thinking Your Network Plan Through

One of the most common errors we see with friends and family setting up a network is that even when they do plan out the usage as shown in the previous section, they typically only consider how they will use the network the day it is installed. Consider, though, all the advances that have been made in both computing and networking in just the past few years. New capabilities are being added all the time, and what was considered "advanced" yesterday is pretty much the norm today, so much so that putting a network together without the new technologies seems odd. For example, a few years ago it was not really possible to have a wireless printer on your network. Now it's quite easy to set

one up and well worth the small effort. Because of this, it's important to sit down with some blank sheets of paper and think about what you have today, what you are likely to have six months from now, and what you would love to have two years from now, in your home network.

Determining the Networking Capabilities of Your Computers

If you are not sure what type of capability your computers have, you need to figure that out to understand what, if anything, you need to purchase.

Everything we build from here on out will be connected to the network. As a result, every device we want to add to the network is going to need a NIC or equivalent network adapter. *NICs* are cards that enable a PC, laptop, printer, or other device to talk to other PCs, laptops, and so on. There are two distinct types of NICs:

- **Wired**—Uses cables to connect to the network
- **Wireless**—Uses the air to connect to the network, much like your cell phone

Keep in mind that most new PCs and laptops come with built-in NICs, and many new laptops have built-in wireless capabilities.

Let's start with the easy one first—wired—and then move on to wireless.

Looking for a Wired NIC

Pretty much every PC out there today (unless you have a really old one) has a wired NIC with an Ethernet port. The wired NIC has a slot for an Ethernet plug that looks like a fat phone cord plug. This slot is almost always located on the back of a PC, but could be on the side of a laptop as well. You may also have a plug-in card for your laptop that has the port in it. We're guessing, though, that less than 1 in 100 computers or laptops will not have the port hard mounted on the computer. Figure 4-5 shows what the wired NIC port looks like.

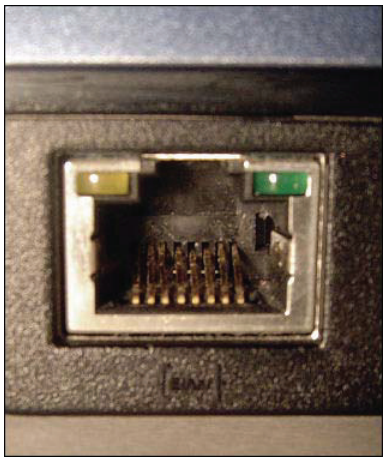


Note: Be careful that you do not confuse a modem jack with an Ethernet jack. The modem jack is the same as a phone jack on your wall. The Ethernet jack is a bit wider. Another way to tell them apart is that if you look into the jack, modems typically have two or four pins or contacts, whereas Ethernet jacks have eight.

Looking for a Wireless NIC

Determining if you have a wireless NIC is not as easy because in many cases there's nothing to actually see. If you have purchased your computer any time after 2003, there is a good chance you have built-in wireless capability.

Figure 4-5 Wired NIC Port

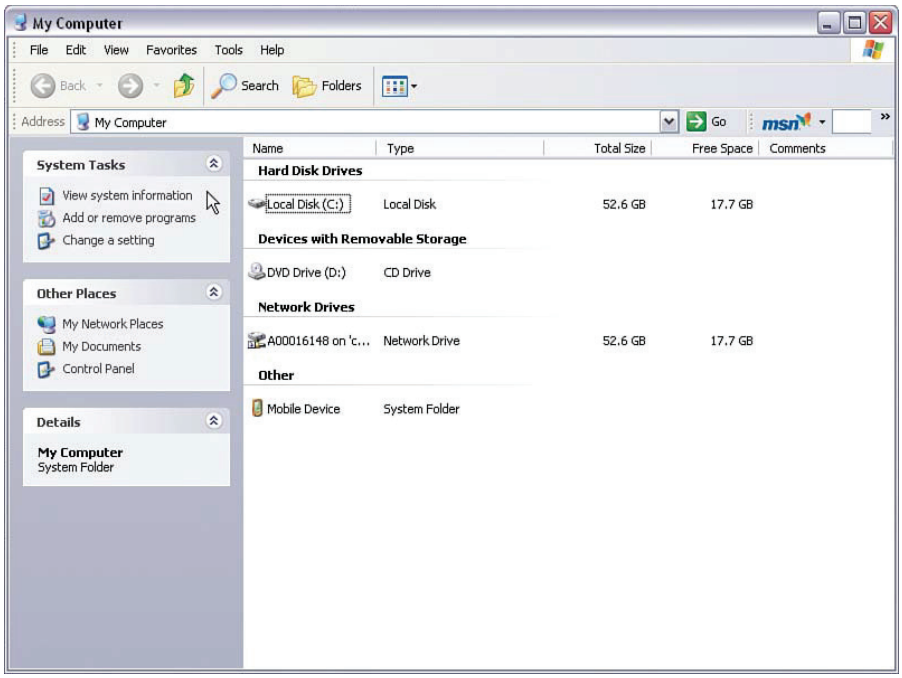


If you have Windows XP, you can quickly check your computer's wireless capability by performing the following steps (you can also follow the steps in older versions of Windows, but the path might be slightly different):

Step 1 Click the **Start** button and then click the **My Computer** icon. (Depending on your setting, you may need to right-click the **My Computer** icon and choose **Open** from the menu.)

Step 2 Click the **View System Information** option, as shown in Figure 4-6.

Figure 4-6 My Computer Window



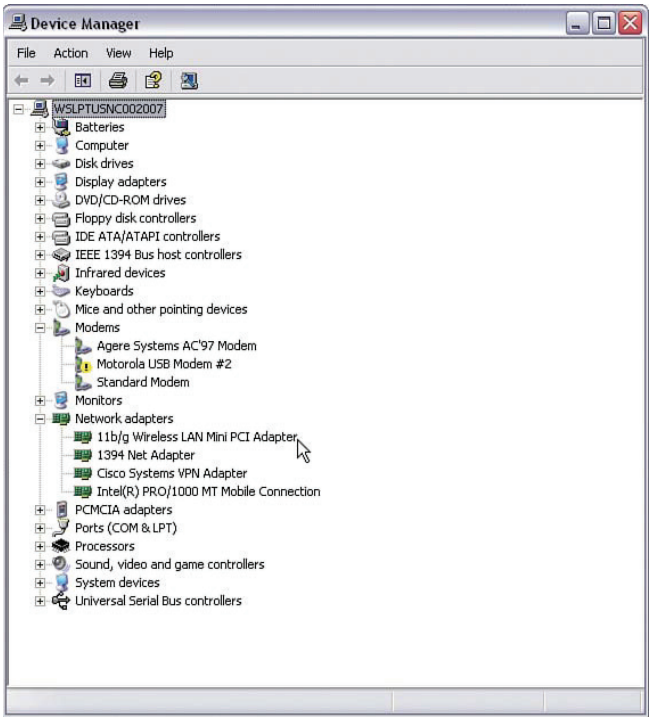
Step 3 Click the Hardware tab in the System Properties window and then click Device Manager, as shown in Figure 4-7.

Figure 4-7 System Properties Window



Step 4 In the Device Manager window, click the plus sign (+) next to the Network Adapters icon, as shown in Figure 4-8.

Figure 4-8 Device Manager Window



Step 5 Look at the list of network adapters and see if any of the options say "wireless" or "WLAN" (for wireless LAN). If any of the devices shown have either of those words in the description, you have some form of wireless capability on your PC. This screen also tells you what type of wireless you have, whether it's A, B, G, N, or some combination thereof. As you can see in Figure 4-8, the computer shown has B and G capability.



Note: If your computer doesn't run Windows XP, or if after following these steps you are still not sure whether the computer has built-in wireless, check the product documentation that came with the computer (or online).

Determining Your Immediate Needs to Create a Wireless Network

Table 4-1 shows a worksheet we found useful for planning a network. Fill it out twice: once for today and once for what you think your home network may look like one to two years from now. You can complete the table either on a piece of paper or, better yet, in a spreadsheet program. The example shown in Table 4-1 is based on our houses. It may seem like a lot, but trust us, the first time your 12-year-old daughter comes to you complaining that she can't connect to her teacher's website from the back porch to download her homework, all will become apparent.

Table 4-1 Planning Your Network: Example Worksheet

Computer or Device	Need	Have	Type to Buy
Today			
Desktop PC (Spouse)	Wired NIC and wireless NIC	Wired NIC	
Desktop PC (Son)	Wireless NIC	Wired NIC	
Laptop 1 (Work)	Wireless NIC	Wired NIC Wired B/G NIC	
Future			
Laptop 2 (Daughter)	Wireless NIC	None	
Xbox video game console	Wireless NIC	None	

At this point, you need to consider several other factors in your planning:

- What type of Internet access do you have today? Will it have bandwidth (transfer speed) adequate for your needs? For this exercise, let's assume that you are going to use the wireless G standard. We'll show how to set up both a G and an N system in the chapters that follow, but most people should pick one system, as described in Chapter 3, "Selecting the Right Wireless Standard for Your Network," and stick with it.

- Where is the Internet access physically located in your house? Is it convenient?
- Do family members need to share resources, like printers?
- Do you have computer-savvy neighbors or family members who can help?

Completing Your Plan

You should now have a good idea of where you expect to use your computers, where you are going to put your router, and what the wireless capability is for all your computers. Use the method of determining the wireless capability on all of your computers and complete the planning table you began earlier.

Don't worry too much yet about understanding all the details in this chapter. We will explain more as we build out our network. For now, just have a look at the worksheet we put together, shown in Table 4-2. This is an example where we have two desktop PCs and two laptop computers, each identified by its primary user. We also have a video camera and a video game system that we want to include on the network. Later, we will consider options for each of the items we don't yet have and make the best choice based on our needs. After you inventory your equipment, you may want to create a table similar to what's shown in Table 4-2 for your own needs.

Table 4-2 Network Readiness

Computer or Device	Need	Have	Type to Buy
Today			
Desktop PC (Spouse)	Wired NIC and wireless NIC	Wired NIC	None
Desktop PC (Son)	Wireless NIC	Wired NIC	USB wireless G NIC
Laptop 1 (Work)	Wireless NIC	Wired NIC Wired G/B NIC	None
Future			
Laptop 2 (Daughter)	Wireless NIC	—	Plug-in (PCMCIA) wireless card or USB wireless G NIC
Xbox video game console	Wireless NIC	None	Wireless G game adapter (covered later in the book)

In this case, if you happened to have a wireless card that operates on the B standard, you could use it in any of the computers. Just keep in mind that you will only get the B performance for the computer you are using it with.

Summary

This chapter was all about thinking through how and where you want to use your wireless computers so that you don't wind up buying things you don't need. Many of the calls we get from friends and family when they have trouble with their wireless network setup stem from their use of the ever-popular "ready-fire-aim" tactic of running out and buying gear and then trying to hook it all together without starting with a plan. By taking the few extra steps described in this chapter, you should be well on your way to getting your network up and running now and you should have an easier time expanding or upgrading your network later.

This page intentionally left blank

CHAPTER 5

Wireless Security: What You Need to Know

At this point you should have a good idea of which type of wireless standard will work best for you, and how and where you plan on using or accessing your wireless network. Now it's time to think about security. This is one of the most important considerations regarding your wireless network, yet, sadly, most people don't take the little bit of time required to protect themselves from hackers and identity thieves. We urge you to take the time to understand and implement security on your wireless network. This chapter focuses on the types of security (and the risks of not enabling it). Chapter 9, "Wireless Security Setup," shows you how to implement the different types of security on your network and wireless enabled devices.

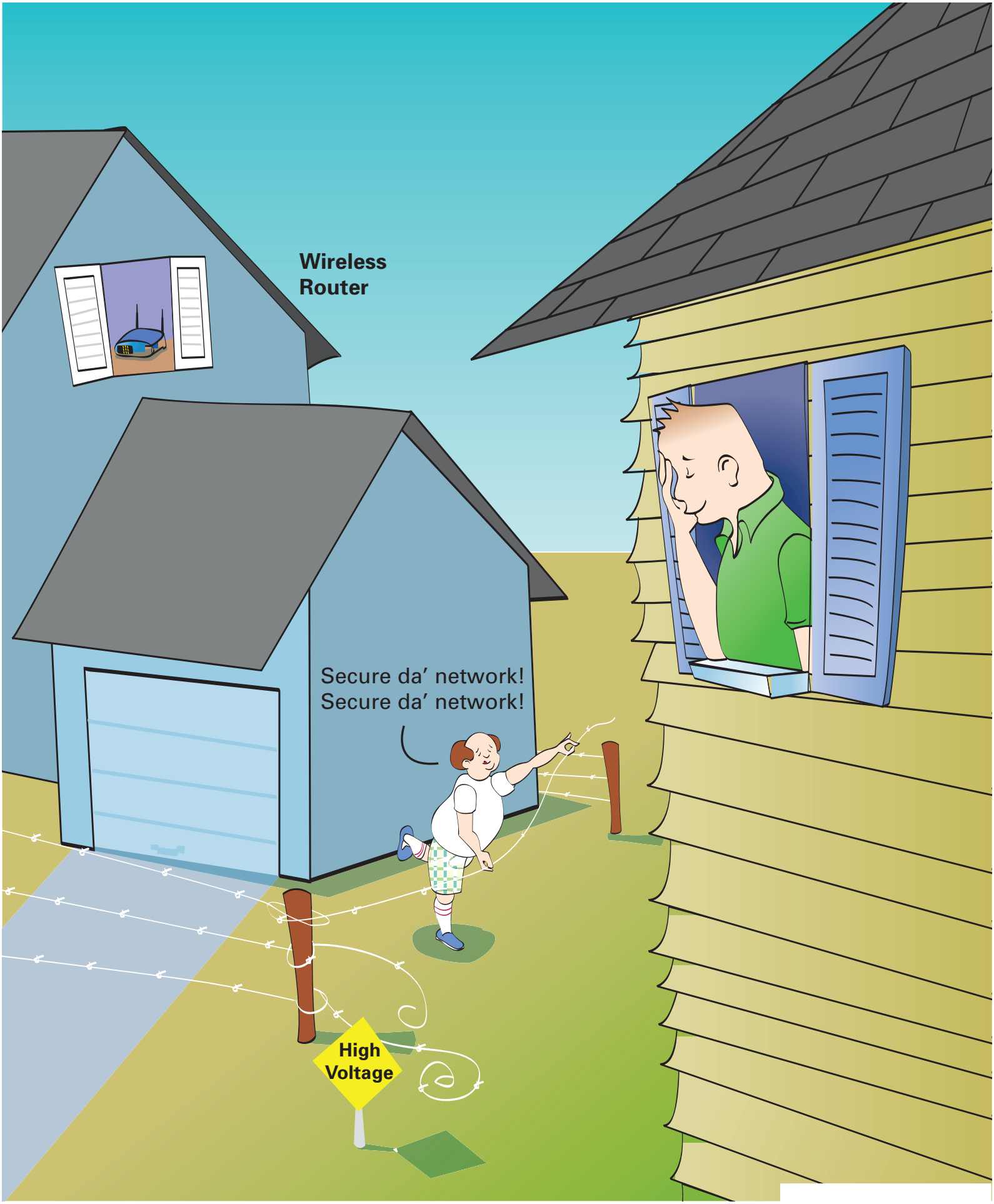


Note: Wireless security involves taking additional precautions beyond using a firewall. Even if you currently have a firewall, you still need to enable wireless security. For a more detailed treatment on the ten things everyone should know about home network security, please see *Home Network Security Simplified* (ISBN: 1158720-163-1).

Why Should I Worry About Wireless Network Security?

Controlling access to who is on your network is one of the most critical components of overall network security. Access to a wired network is easy to control, because people have to be physically inside your house to plug a computer into the router. With a wireless network, people just have to be in the proximity of your house. Physical barriers such as windows and doors do not control access in this case, so we have to take other steps to block intruders.

The security issue with a wireless network stems from the fact that the signal is omnidirectional. Unlike a wired network, where signals are fairly well contained, the wireless signal goes everywhere in all directions (including up and down, for those of you in multistory buildings) for 100–300 feet or more. Anyone who wants to gain access to your signal need only put a receiver (a computer with a wireless card) inside the signal range.


Wireless
Router
Secure da' network!
Secure da' network!
High
Voltage



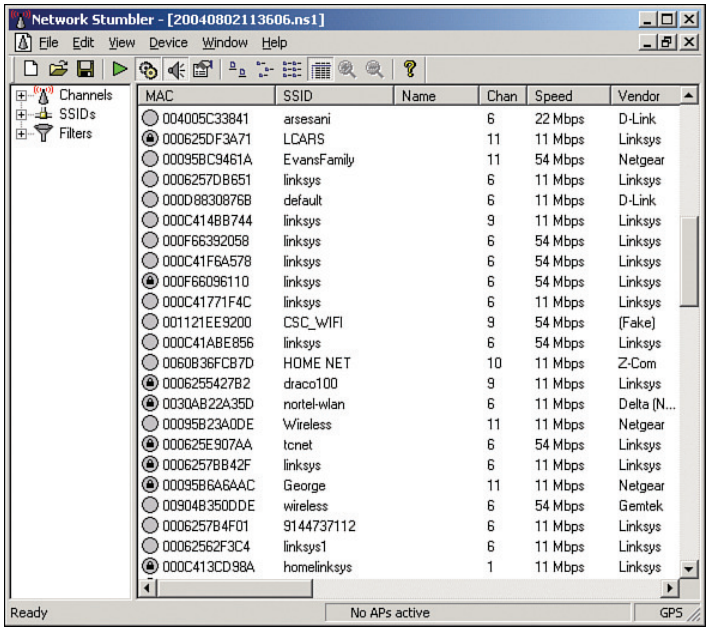
Note: Why would someone want to access your wireless network? Well, there are lots of reasons. One of your neighbors could "leech" onto your network just to receive free Internet access. Although irritating, this is not all that harmful in itself, if all they are doing is browsing the Internet on your dollar. However, *war-drivers* (hackers who drive around looking for unsecured wireless networks) or professional hackers could use the access to obtain your personal information. For example, eavesdropping while you are conducting an online purchase could expose your credit card information.

One of the most unusual illicit uses of unsecured home wireless networks also offers perhaps the strongest reason yet to secure your wireless network. Recently, several instances have surfaced where people conducting illegal activities used unsecured home networks for the anonymity that they can provide. One fellow parked in a neighborhood, easily gained access to an unprotected home wireless network, and downloaded huge amounts of illegal child pornography. He was caught and arrested, but it was due to a traffic violation, not the downloading (the police noticed the pictures on the computer after they pulled him over). If someone commits illegal activity in this manner, that activity can easily be traced to your broadband subscription, in which case you could end up having to explain to the authorities that it was not you or other family members conducting the illegal activity.

We are always amazed when we drive through a neighborhood and check how people have deployed their wireless networks. On a sample drive through a single neighborhood using cheap equipment that's easy for the average person to get and use, we easily found 114 wireless routers, only 45 (roughly 40 percent) of which were protected in any fashion. From such a scan, potential intruders can easily obtain a survey of the available wireless networks, their SSIDs, channel numbers, and, most importantly, which networks have been secured and which have been left wide open (roughly 60 percent). In Figure 5-1, the networks with a circle and a padlock inside are those that are at least using encryption. The networks with a circle without a padlock are wide open. Anyone can sit on the street near these houses (or businesses), associate to the access point, and access the Internet or try to break into the rest of the home network.

The state of your wireless router when you take it out of the box is wide open. You can get your wireless router up and running fast, but if you do not take a few minutes to secure your router (and it really only takes a few minutes), you could be asking for trouble.

Figure 5-1 Scanning for Available Wireless Networks in a Neighborhood



What Do I Do to Secure My Wireless Network?

You can take three really simple steps to dramatically increase the security of your wireless network. It is not foolproof wireless security, but it will keep you from being an easy target and it will keep most of the riffraff out.

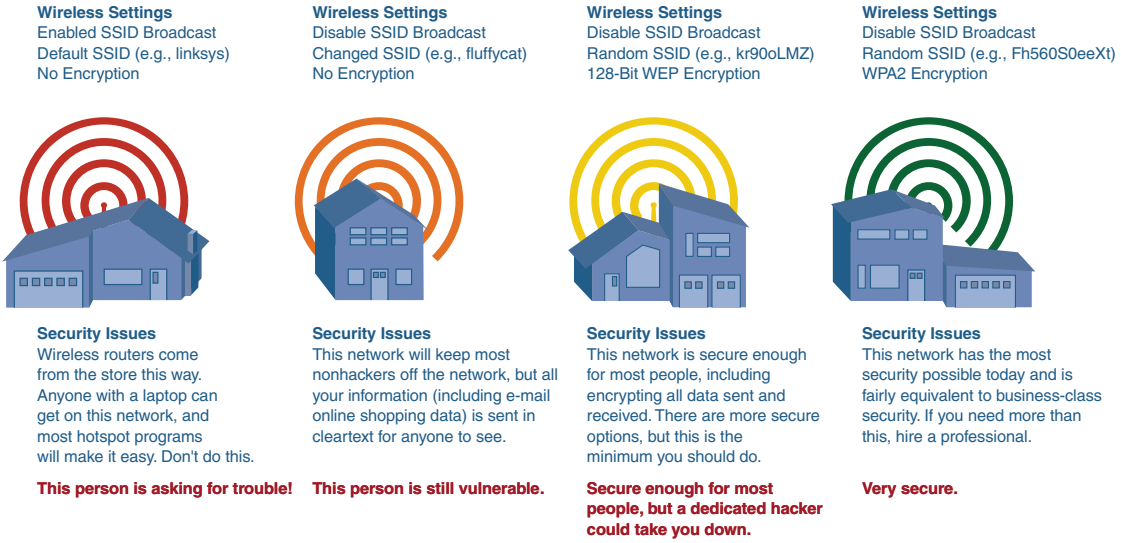
As Figure 5-1 showed, there are plenty of easy targets out there, so all you need to worry about in most cases is the curious neighbor or someone specifically looking to access a network with no protection at all. The steps described in this section will not keep out a really serious hacker, but if you have reason to worry about a hacker specifically targeting you (as opposed to someone hacking at random), then you can hire a security specialist or, better yet, just don't use wireless. For the vast majority of you, though, read on.

Figure 5-2 shows varying degrees of wireless home network security and the vulnerabilities related with the networks.

So what are the three things you need to do to improve your wireless network security?

- Don't advertise your network (turn off SSID broadcast).
- Scramble (encrypt) your wireless signal using encryption.
- Don't use ad hoc networking.

Figure 5-2 Security Examples



Don’t Advertise Your Wireless Network

Every wireless router is given a name that allows clients (that is, wireless-enabled computers) to find and associate to it. This name is called the *service set identifier (SSID)*. The first step you can take to greatly improve the security of your wireless network is to not broadcast the SSID!

Most wireless routers have the broadcast SSID setting turned on when you take them out of the box. This feature announces the name of your network to every wireless-capable computer within range. Although this makes it easy for you to connect to your network, it makes it easy for the rest of the neighborhood, too. Turn this feature off (we show you how in Chapter 9). In addition, knowing the name of a network (even if the broadcast function is turned off) gives you the power to get on that network, so you should choose a random SSID name.

Any SSID that is easy for you to remember is probably easy to figure out, so avoid SSIDs that include your name, the word “home,” the word “network,” or anything related to *your name-home-wireless-network*. We suggest that you rename the SSID to something personal (but not easily guessed) or use a random combination of numbers and upper- and lowercase letters. Don’t worry about having to memorize this, because you can just write it down and keep in a drawer or a folder where you can access it later if you need it. Remember, however, that although this step will keep out the nosy neighbors and provide your router with some level of anonymity, it will not by itself protect your network.

In Chapter 7, “Wireless Router Setup,” and Chapter 9, you will see in more detail how to set up the wireless router and how to secure it, including choosing an SSID, so don’t worry if you have not thought of one yet.

Scramble Your Signal

Another step you can take to improve the security of your network is to turn on encryption. This section describes wireless encryption technologies, how to select one for your wireless network, and how to choose an encryption key.

What Is Encryption?

If you are unfamiliar with encryption, the concept is pretty simple. Remember being a kid and making up a list like this:

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26

Then your friend wrote you a note like this:

9

12 9 11 5

3 8 5 5 19 5

You pulled out your handy-dandy decoder table and translated it to "I like cheese." Congratulations, you were doing encryption.

We are obviously oversimplifying, but encrypting your wireless network is actually a similar concept. You are going to choose a key for your wireless network. That key is known to both the sender and receiver—for example, your computer and the wireless router. Every time you send information between each other, you use the key to encode it, you transmit it, and then you use the key again to decode the message back to its real information.

In the previous simple example, the only reason you and your friend knew what each other were saying was that you both had the same decoder. As long as only you and your friend have the key, you can talk without anyone else eavesdropping on your conversation.

In the case of wireless encryption, instead of a single letter-to-number translation, a mathematical formula is calculated using the original information and the key. The result is a highly encoded piece of information that is very difficult to decode without knowing the key. In general, the longer the key, the harder it is to break. Think of an encryption key like a PIN code that has 16 or 32 digits instead of 4. (How the mathematical formulas work are beyond the scope of this book. If you are interested, pick up a book on cryptography.)

There are several standards available for wireless network encryption, including the following two most common ones:

- **Wired Equivalent Privacy (WEP)**—WEP provides a simple and fairly effective means for keeping your information private and your network secure from those wishing to access it without your knowledge or approval. WEP is the most widely available encryption standard and is offered with several different key lengths, including 64, 128, 152, and even 256 (bits). You may also see references to 40 and 104, but these are exactly the same as 64 and 128. WEP is good enough to keep any nonhacker from seeing your information but it is by no means a bulletproof encryption method.

- **Wi-Fi Protected Access (WPA)**—WPA is a newer and more sophisticated method of encryption. We recommend that you use WPA if it is available on your gear because it provides better protection than WEP. The two common types of WPA are Temporal Key Integrity Protocol (TKIP) and Advanced Encryption Standard (AES). The TKIP version is often referred to as WPA, while the AES version is often referred to as WPA2 and provides near business-level security for home networks.

The major difference between WEP and WPA is that with WEP your encryption key remains the same until you change it, whereas WPA automatically changes the key periodically for you. Changing the key makes it more difficult for someone to discover the key, and even if they do, the key is only useful for a very short time, because it will change again.

Some home networking products (wireless computers, NICs, and wireless routers) support all of the encryption options, while others support a smaller subset. This is important because both the computer and router need to be talking with the same encryption method and key to understand each other.

Choosing an Encryption Key

So how do you choose an encryption key? There are two ways, one very simple, and one not so simple. The simple way is to use the key generator that is built into the home networking products. (Linksys products offer a key generator in every wireless card and router Linksys sells.) Essentially, you just create a passphrase, which is like a password, enter it into the NIC or router (using the administration tool), and click a Generate Key button. Examples are shown later, in Chapter 9.

The rules for selecting a passphrase and choosing a password are the same: Never use names, pets, or words. Make up a random series of 8 to 63 lowercase letters, uppercase letters, and numbers. Do *not* try to spell words or use clever encoded phrases such as *weLUVr2Dogs* (Chapter 9 has more on creating strong passwords). The key generator will take the passphrase and translate it into a series of numbers (0–9) and letters (A–F). Don't worry about understanding the number system, but this is the encryption key. Write down both the passphrase and generated key; you are going to need it several times.



Note: Passphrase generators are proprietary, so each vendor's key generator works only with its router/NIC. You can still use WEP/WPA with routers and NICs from different vendors, but you will need to type in the encryption keys manually. In addition, Windows XP does not support the concept, so you have to always manually enter the key itself (for WEP).

Table 5-1 summarizes the different encryption methods mentioned previously. It is important to note that these encryption methods typically cannot be mixed together on the same network, so pick the highest level of security that all your wireless network devices can support.

Table 5-1 Available Wireless Encryption Methods

Encryption Method	Security	Recommendations
64-bit WEP (sometimes referred to as 40-bit WEP)		Minimum level of encryption. We recommend 128-bit WEP. However, if you have some older devices, they may only support 64-bit WEP.
128-bit WEP (sometimes referred to as 104-bit WEP)		Very commonly used and offers a high degree of security. A professional hacker with enough money and time can "crack" the code, but this is secure enough for most people.
WPA (sometimes referred to as WPA-TKIP)		Adds a degree of security beyond WEP. The secret key is changed periodically to reduce the opportunity for "cracking." Typically available with a software upgrade for older devices.
WPA2 (sometimes referred to as WPA-AES)		Adds a new encryption algorithm (AES) to WPA, which makes it even more secure. May or may not be available for older devices.

VERY IMPORTANT: We can't stress enough that any time you create something such as an encryption passphrase, password, or WEP key, you need to write it down in your notebook. If you lose it, you may have to reset the wireless router to the factory defaults and start over.

The second way to choose an encryption key is make it up yourself using a random combination of numbers (0–9) and letters (A–F). You will need to create an exact number of numbers and letters depending on which key length you are trying to create. For example, a 64-bit key has 10 hex digits; a 128-bit key has 26 hex digits; and so on (the administration screen where you set this up will specify the number of characters). If at all possible, use the built-in key generator from a passphrase. You will pull your hair out trying to create them by hand.

If you have guests who want to use your network, you need to give them your passphrase or security key. If you need to, you can always change the key after they leave. Chapter 9, "Wireless Security Setup," also discusses how to use a USB media key to easily add quests to your network. You can also have them use a direct (wired) connection into the router, which does not require encryption.

Disable Ad Hoc Networking

Your wireless-enabled computer has two basic modes of communication: infrastructure and ad hoc networking. In infrastructure mode, all the computers on the network must communicate through the router. So whether you are talking to the Internet or with another computer on the local network, all your communication traffic goes through the router. This is what most people are and should be doing.

In ad hoc mode, computers can communicate directly with each other without going through a router or any other device. This is great if, for example, you want to share a file with someone quickly. The bad thing is that if you have this mode enabled, someone who knows what they are doing can get access to all your files, possibly without you even noticing it. To avoid this, we strongly recommend that you disable this function using the steps outlined in Chapter 9. If you find yourself in a situation where you need to use this feature, turn it on for the duration of use and then immediately disable it.

Other Tips to Consider

One of the first things you should do is change the administrative password on your router. We cover how to do this in Chapter 7. This is an important step that you should not skip over.

Another good security tip is that you should get in the habit of turning your wireless router (and your modem) off during periods of long inactivity (if you go away for the weekend, for example). If it's not turned on, it can't be hacked.

Summary

Enabling security on your wireless network is critical even if you have a firewall, because a firewall protects you against some threats but does little to protect against wireless access threats. Broadcasting your SSID and leaving the encryption feature disabled is, at best, an invitation to give your neighbors free Internet access and, at worst, an easy path to losing your identity. Encryption is an absolute must on any wireless network. As we demonstrate in Chapter 9, it takes no more than five minutes to set up good wireless security, which could save you years of aggravation trying to get your credit history repaired.



Note: Securing your wireless network is just one aspect of home network security. To learn about the full breadth of necessary steps you should take to secure your home network, pick up a copy of *Home Networking Security Simplified*. It covers the top ten things you should do to secure your home network.

Where to Go for More Information

Check out Bradley Mitchell's article "Top 9 Tips for Wireless Home Network Security" on About.com: http://compnetworking.about.com/od/wirelesssecurity/tp/wifisecurity.htm.

JiWire has an article titled "Complete Guide to Wi-Fi Security" by Tony Bradley and Becky Waring: www.jiwire.com/wi-fi-security-introduction-overview.htm.

Linksys also has some good information about network security at www.linksys.com. Click **Network Security** on the Learning Center drop-down menu and follow the Network Security links on the left side of the page.

The U.S. Justice Department defines the federal law regarding hacking in 18 U.S.C. 1030, "Fraud and Related Activity in Connection with Computers": www.usdoj.gov/criminal/cybercrime/1030_new.html.

Wikipedia has an entry on cryptography and encryption: http://en.wikipedia.org/wiki/cryptography.

CHAPTER 6

What to Buy

The next step in building your network is to determine what you need to buy. Based on the planning diagram and tables you did in Chapter 4, "Planning Your Wireless Network," you should have a good idea of the basic device types you need to get your network up and running.

Determining Network Readiness

We'll follow the example started in Chapter 4. We first need to take inventory of the type of NICs we have already in the different computers we want to participate in the wireless home network. Make a table like that shown in Table 6-1, recording how we need to connect the computer in the Need column, and what we have today in the Have column.

Table 6-1 Network Readiness

Computer or Device	Need	Have	Type to Buy
Today			
Desktop PC (Spouse)	Wired NIC and wireless NIC	Wired NIC	
Desktop PC (Son)	Wireless NIC	Wired NIC	
Laptop 1 (Work)	Wireless NIC	Wired NIC Wireless B/G NIC	
Future			
Laptop 2 (Daughter)	Wireless NIC	None	
Xbox video game console	None	Wireless NIC	

Based on the table, we have wireless capability in one of the laptops (as a reminder, Chapter 4 showed you how to determine if your computer has wireless capability). This leaves us with one laptop and two desktop computers that need additional equipment to support wireless.

In addition to outfitting the computers with the right equipment, you also need a wireless router, which will communicate with all the computers and provide them access to the Internet via the cable or DSL modem.

In addition, you may want to consider some extra bells and whistles (such as game adapters or wireless cameras) at some point, so we'll cover them here as well.

To make this easy, we are going to go with all Linksys gear here. This is not a requirement, because all wireless equipment using the same standard should be compatible regardless of who the manufacturer is. The one exception, noted in earlier chapters, is that proprietary extensions such as Linksys SRX require compatible equipment on both sides. In other words, to get the benefit of SRX, you need both the SRX router and the SRX NIC. We're going to stay away from all that here and keep our example pretty simple.

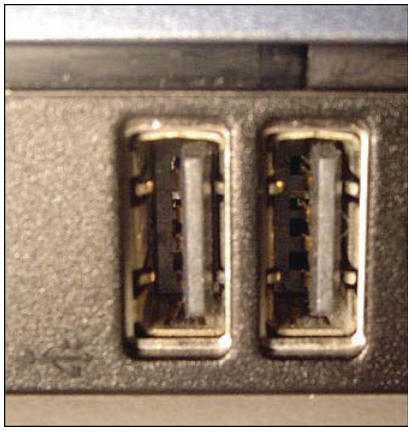
Another reason we will use all Linksys products is that, by having Linksys on both sides (that is, a Linksys wireless router and Linksys wireless NICs), we can take advantage of some advanced features that make installing and setting up the wireless network easier. These features are not always available if we have a mixed environment (meaning different manufacturers for the router and NICs).

To that end we are going to base everything from here on out on the wireless G standard. This includes the routers, NICs, and, where available, the extra stuff such as game systems. In cases where G is not available, we use B-standard devices, which, as we previously mentioned, will work with the G router, albeit at B performance levels.

Another compelling reason to avoid proprietary extensions such as Speed Booster and SRX is that the preliminary N standard is available now and offers all the benefits of these extensions (and then some) without locking you into proprietary equipment. For those who require (or think they will require in the future) speed and range beyond what G has to offer, we also provide a walkthrough for an N-based system. We cover only the router, though, because the NIC setup is identical.

For the NICs, there are a number of options. In the desktop computers, you can install a card inside the computer, but this involves taking the cover off, which is kind of a pain. We'll show you how to do it for the sake of completeness, but there are better options. One such option is to use a USB wireless adapter, which requires a USB interface. Most computers made over the last 5 years or so have a USB interface. The easiest way to determine if you have a USB interface is to look for the slot on your computer. It could be on the front, side, or back, depending on the make and model. The port is shown in Figure 6-1.

Figure 6-1 USB Interface



If you do go with a USB NIC, you can either get a small box that connects to the USB port via a USB cable or get a NIC that has the same form factor as a memory key or memory stick. Pictures of both are shown later in this chapter in the section "Wireless NIC Options."



Note: There are two kinds of USB: 1.0 and 2.0. The USB NICs we reference work with both USB standards, but both yield better performance with USB 2.0.

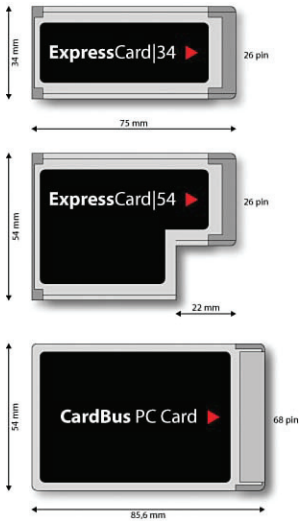
If you need to buy a NIC for your laptop, you can also use any of the USB NICs (as with desktop PCs, USB ports have been standard on laptops for several years). That said, we recommend a PCMCIA card for laptops, which is a card that plugs into a slot in your laptop. These cards are specifically made for laptops and don't stick out like USB sticks do, so you can carry your laptop around without too much worry about the card breaking off (which is not an option with a USB key). Note, though, that if you put your computer in a computer bag for transport, it's a good idea to take the PCMCIA card out to prevent the card from breaking off pins.



Note: A newer type of laptop card, called ExpressCard, is now being used. ExpressCards are roughly half the size of the previous generation of PCMCIA cards. At the time of this writing, not many ExpressCards are available, but we expect they will become popular. Whether you buy PCMCIA cards or ExpressCards is up to you; just make sure that whichever you buy matches what you have in your laptop. PCMCIA and ExpressCards are *not* compatible.

Figure 6-2 shows a comparison of a PCMCIA card (bottom) and two ExpressCards (top two).

Figure 6-2 PCMCIA and ExpressCard Comparison





Note: PCMCIA stands for Personal Computer Memory Card International Association. We had to look it up on Google. No one (except maybe for the folks paying dues to that association) would ever actually use the words instead of the acronym, and if you were to go to your favorite electronics store and ask them for a "Personal Computer Memory Card International Association card," they would probably just ask you to leave.

Later, in Part V of the book, we will cover how to connect some other devices to your wireless network, including a wireless gaming system and a wireless video camera. The wireless game adapter is perfect for those of you who like or want to play Xbox Live (or the Sony PlayStation or Nintendo GameCube versions) but have the TV and Xbox in a different room than the router and broadband modem. These game adapters are good for extending your Voice over IP (VoIP) service, such as Vonage, to another room without adding another cordless phone (and more interference) to your house. We will also show you how to install and use a wireless video camera, which is great for monitoring the baby, or the nanny, or your husband, or some combination of those people should your situation require it.



Note: In the event that you have a desktop computer that has neither a wireless card nor a USB port, you can use the wireless game adapter to provide wireless capability to your computer, assuming it has a standard wired NIC installed. If not, you probably have a really old computer and you are either looking at installing a card on the motherboard or taking heroic measures (not covered in this book) to connect that computer to the network.

Some older computers may lack the horsepower to be able to operate a wireless NIC. For example, Linksys wireless NICs are supported only in computers with 200-MHz Pentium processors and higher. Sometimes, though, we have an older computer such as a Pentium 133 MHz that we still want to use. The solution to this problem is to go ahead and install a wired NIC in the computer, and then add a wireless Ethernet bridge (such as the Linksys WET11) to provide the wireless connection. The wireless bridge is "self-contained" and does not need the PC to connect itself to the wireless router. Wireless Ethernet bridges are a little hard to find but can be worth their weight in gold if you absolutely must put an older computer on the wireless network.

So, based on all of the preceding information, we need to finish our table and round out the categories of equipment we need. The completed table is shown in Table 6-2.

Table 6-2 Network Readiness Completed

Computer or Device	Need	Have	Type to Buy
Today			
Desktop PC (Spouse)	Wired and wireless NIC	Wired NIC	USB wireless NIC (G standard)
Desktop PC (son)	Wireless NIC	Wired NIC	USB wireless NIC (G standard)
Laptop 1 (Work)	Wireless NIC	Wired NIC Wireless G/B NIC	None
Wireless router	Wireless router	None	Wireless G Router
Future			
Laptop 2 (Daughter)	Wireless NIC	None	PCMCIA wireless NIC (G standard)

Making Your List, Checking It Twice

Now that we know what types of stuff we need to buy, next we need to actually figure out models and numbers. The shopping list in Figure 6-3 includes the devices we will be using in our examples in the remainder of the book, but we want to make the point again that all of the equipment we are choosing can be substituted with the same equipment from another vendor, so long as you stick with the base N, G, or B standard.

Figure 6-3 Shopping List



For a closer look, the following sections summarize the equipment.

Wireless Router Options

Because we will be putting together a G-based network, the router we chose—WRT54G—is the base G router with no extensions, shown in Figure 6-4. If you plan to have the router sit out in the open and you want something a little smaller (and nicer looking), you can go with the compact router (WRT54GC), shown in Figure 6-5.

Figure 6-4 Linksys Wireless-G Broadband Router (WRT54G)



These materials have been reproduced by Cisco Press with the permission of Cisco Systems, Inc.
COPYRIGHT ©2007 CISCO SYSTEMS, INC. ALL RIGHTS RESERVED

Figure 6-5 Linksys Compact Wireless-G Broadband Router (WRT54GC)



These materials have been reproduced by Cisco Press with the permission of Cisco Systems, Inc.
COPYRIGHT ©2007 CISCO SYSTEMS, INC. ALL RIGHTS RESERVED

We will also show you how to set up and install the new N-based router just for kicks. Here we will use the WRT300N router (see Figure 6-6).

Figure 6-6 Linksys Wireless-N Broadband Router (WRT300N)



These materials have been reproduced by Cisco Press with the permission of Cisco Systems, Inc.
COPYRIGHT ©2007 CISCO SYSTEMS, INC. ALL RIGHTS RESERVED

Wireless NIC Options

For the desktop NICs, we have decided to use USB devices. We will go with a different kind of USB NIC for each, but this is only to show how to set them up rather than for some engineering reason. The devices we picked are the USB box WUSB54G (see Figure 6-7) and the USB stick WUSB54GC (see Figure 6-8). For the laptop, the obvious choice is the G-based PCMCIA card WPC54G (see Figure 6-9). Depending on the location of the "Spouse" PC (or any other PC, for that matter), you can use a standard Ethernet cable to connect the PC to one of the wired ports on the back of the wireless router.

For the desktop, we could have also picked an internal PCI card, such as the Linksys WMP54G (see Figure 6-10).

Figure 6-7 Linksys Wireless-G USB Network Adapter (WUSB54G)



These materials have been reproduced by Cisco Press with the permission of Cisco Systems, Inc.
COPYRIGHT ©2007 CISCO SYSTEMS, INC. ALL RIGHTS RESERVED

Figure 6-8 Linksys Compact Wireless-G USB Adapter (WUSB54GC)



These materials have been reproduced by Cisco Press with the permission of Cisco Systems, Inc.
COPYRIGHT ©2007 CISCO SYSTEMS, INC. ALL RIGHTS RESERVED

Figure 6-9 Linksys Wireless-G Notebook Adapter (WPC54G)



These materials have been reproduced by Cisco Press with the permission of Cisco Systems, Inc.
COPYRIGHT ©2007 CISCO SYSTEMS, INC. ALL RIGHTS RESERVED

Figure 6-10 Linksys Wireless-G PCI Adapter (WMP54G)



These materials have been reproduced by Cisco Press with the permission of Cisco Systems, Inc.
COPYRIGHT ©2007 CISCO SYSTEMS, INC. ALL RIGHTS RESERVED



Note: As we discussed in Chapter 5, "Wireless Security: What You Need to Know," make sure to consider the wireless security you want to use (WEP, WPA, WPA2, and so on). Most wireless routers and NICs on the market today support all of them, but you need to double-check, especially if you are buying older or used products. If all the wireless NICs in your network support WPA2, except for one that supports only WEP-128, then your entire network will need to fall back to WEP-128 as the least-common denominator.

For example, we will see in Chapter 13, "Wireless Video and Entertainment," that for networking your DVR over a wireless connection, WPA is not supported today, so WEP-128 is the maximum security possible (this could change by the time this book is published and purchased, so check the URLs listed in Chapter 13 for the latest information).

Gear for Travel Bugs and Road Warriors

If you travel a lot and want or need to maintain wireless connectivity in hotel rooms or offices with a high-speed wired connection, a wireless travel router is a good piece of kit to bring along with you, and it does not take up a lot of room in your bag. This is especially convenient if you subscribe to an Internet telephony (VoIP) service such as Vonage. Using a wireless travel router and your VoIP terminal adapter (the box your phone connects to), you can bring your office with you wherever you go. Imagine traveling to Singapore and having your office number from Boise ring in your hotel room without it costing you a dime. Cool stuff. We talk more about travel routers in Chapter 14, "Wireless to Go."

The Linksys model number for the Wireless-G Travel Router with SpeedBooster is WTR54GS and it is shown in Figure 6-11. Note that this model has the Speed Booster extension, but because we recommended that you get the standard-G NICs, you will only get standard-G performance out of this router. No worries, though, because it's still plenty fast.

Figure 6-11 Linksys Wireless-G Travel Router with SpeedBooster (WTR54GS)



These materials have been reproduced by Cisco Press with the permission of Cisco Systems, Inc.
COPYRIGHT ©2007 CISCO SYSTEMS, INC. ALL RIGHTS RESERVED

Extra Stuff

In Chapter 13 we will discuss connecting a video game console, such as Microsoft Xbox, to the wireless network so that we can participate in online gaming over the Internet. For this we chose the Wireless-G Game Adapter, model number WGA54G, shown in Figure 6-12.

In Chapter 13 we will also discuss connecting a wireless video camera to our wireless network. For this we chose the Wireless-G Video Camera, model number WVC54G, shown in Figure 6-13.

Figure 6-12 Linksys Wireless-G Game Adapter (WGA54G)



These materials have been reproduced by Cisco Press with the permission of Cisco Systems, Inc.
COPYRIGHT ©2007 CISCO SYSTEMS, INC. ALL RIGHTS RESERVED

Figure 6-13 Linksys Wireless-G Internet Video Camera (WVC54G)



These materials have been reproduced by Cisco Press with the permission of Cisco Systems, Inc.
COPYRIGHT ©2007 CISCO SYSTEMS, INC. ALL RIGHTS RESERVED

Where to Buy Your Gear

You can shop for this stuff in just about any electronics or computer store. Pretty much everything on the shopping list in Figure 6-3 should be available in the larger retail chains and easily available online.

If you are looking for equipment alternatives (whether the same Linksys equipment or the same type of stuff from different vendors), we highly recommend www.cnet.com. From the main page, click the **Reviews** tab and then the **Networking** tab, as shown in Figure 6-14 and Figure 6-15, respectively. Once there, you can drill down by networking type, manufacturer, price, or other categories. You can also search on a specific item such as wireless G routers. The results page gives you a table of all the compatible devices, with CNET.com's rating score, summary review, and price ranges. You can drill down further to detailed reviews. Clicking the Check Prices link will take you to a page that lists the verified prices for many of the stores selling the item. Figure 6-16 shows the results for a search on wireless G routers.



Note: Rebates are quite common for consumer networking equipment such as wireless routers, wireless NICs, and other wireless equipment. But the rebates may not be reflected in such online comparisons, and may be offered by one retailer and not another. So shop around and check the prices on a couple different retail sites to see who has the best price and potential rebates.

Figure 6-14 CNET.com Main Screen

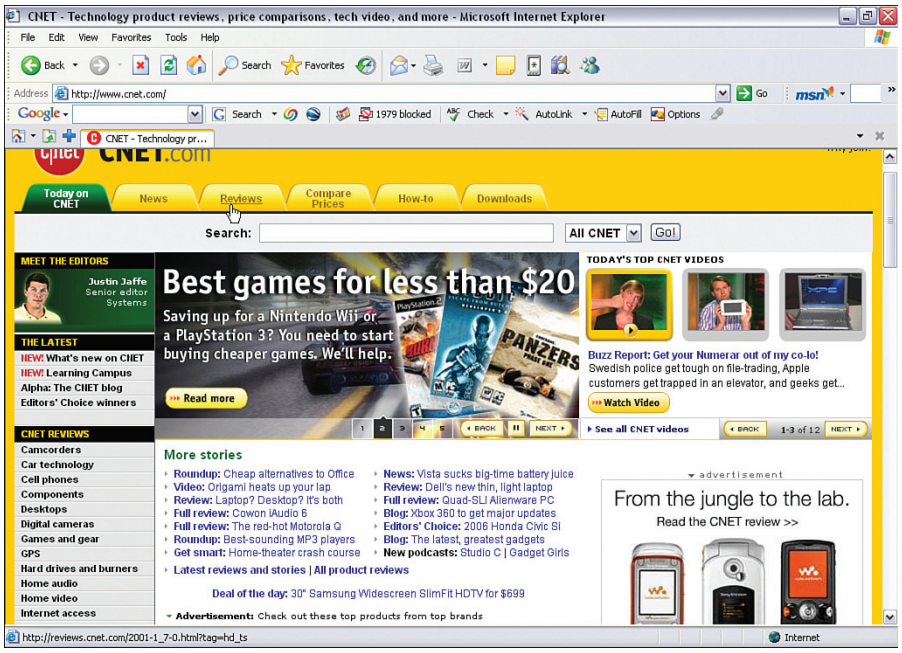


Figure 6-15 CNET.com Networking and Wi-Fi Page

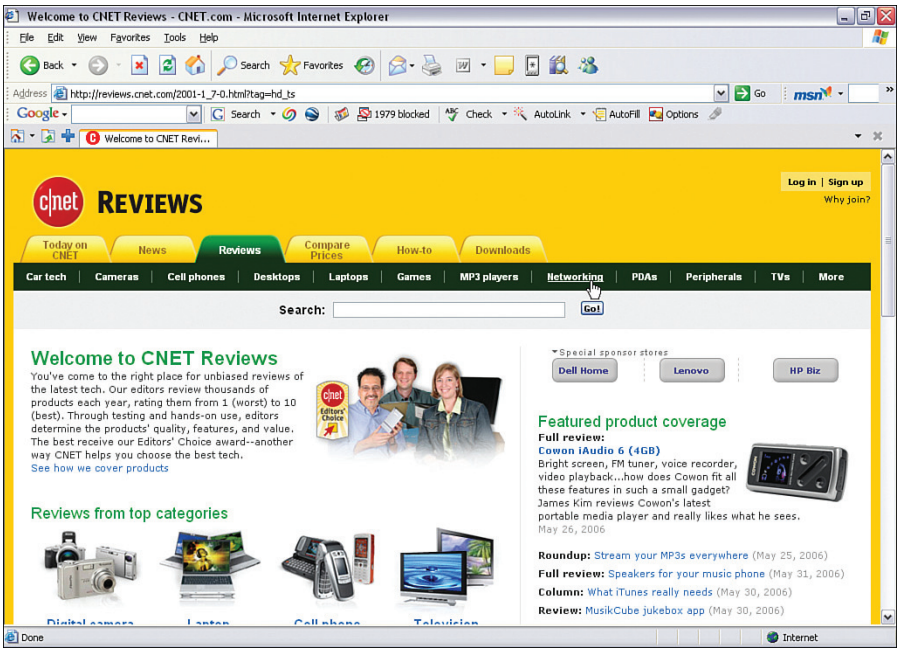
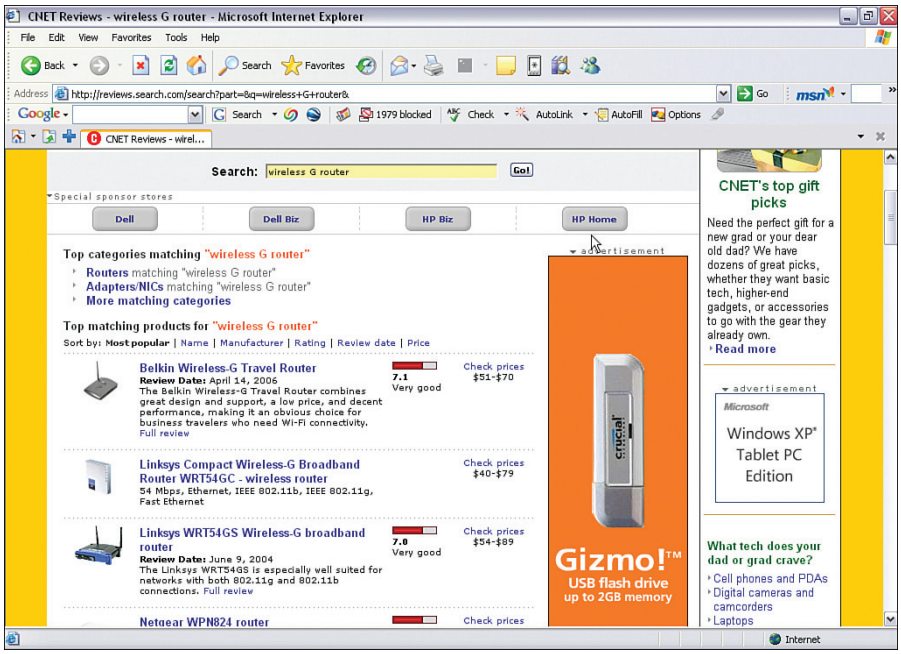


Figure 6-16 CNET.com Search Results for Wireless G Router



You may have noticed while drilling down into the Networking section that the site also reviews computers, MP3 players, and other electronics, so it's worth bookmarking if you buy tech stuff. There are lots of sites like this, but if we had to pick one, this would be it.

Summary

So that's it for the shopping list. Keep in mind, though, that you do not need to go out and buy all new equipment, especially if you have compatible equipment. For example, if you have a couple of wireless B NICs, you can still set up your network with a wireless G router and use the wireless B NICs.

There is also a healthy market for the "older" standards, so if you are not one of those people who always needs to have the latest and greatest tech gadgets, you can probably get some used wireless B equipment for a good price.

Where to Go for More Information

CNET's website is a good resource: www.cnet.com.

PC Magazine has a pretty good website that includes reviews on many wireless networking products: www.pcmag.com/category2/0,1874,4236,00.asp.

Linksys provides product information at its website: www.linksys.com.

This page intentionally left blank



PART III

PART III

How Do I Set It Up?

Chapter 7 Wireless Router Setup

Chapter 8 Wireless NIC Setup

Chapter 9 Wireless Security Setup

Now that you have gotten an overview of wireless networking, put some thought into planning your wireless network, and purchased the stuff you need to build it, it's time to start putting it together. "Finally," you may be saying to yourself, but trust us, every minute you put into some thought up front will save you hours of frustration later on.

The next step is to start building the network. If it's the first time you have ever built a home network, don't worry, we will keep the steps straightforward and easy to understand. If you are upgrading your network to wireless or extending your wireless network's capabilities, again we will give you the information you need to build a solid and secure wireless network. Even if you have built a wireless network before, you may learn a thing or two (we do just about every time we build one).

Chapter 7, "Wireless Router Setup," shows you how to set up the wireless router, which is the heart of your wireless home network. We'll cover how to connect the router to your broadband service and get the wireless part up and running.

Chapter 8, "Wireless NIC Setup," shows you how to set up the wireless NICs on your computers. We'll cover how to get the computers talking to the wireless router. We also show you several different ways of setting up the wireless NICs, including using Windows XP to set up a laptop with a built-in wireless NIC, as well as using a couple of the Linksys programs that come with add-on wireless NICs.

We wrap up Part III with Chapter 9, "Wireless Security Setup," which shows you how to lock down your wireless network with the essential security. This is a critical step in building your wireless home network that unfortunately many people do not take. We will show you how a couple of very simple steps can make your wireless network secure enough and still usable.

CHAPTER 7

Wireless Router Setup

The wireless router is really the brains, or at least the heart, of your home network. The wireless router provides a number of functions, including

- Enabling several computers to connect to your home network either through a wired Ethernet cable or a wireless signal
- Providing a gateway to your broadband Internet connection so that several computers can share it
- Enforcing security policies to protect your home network from unauthorized access

This chapter provides the steps necessary to set up your wireless router, starting with connecting the wireless router to your broadband service. CHapter 8, "Wireless NIC Setup," then walks you through getting wireless NICs to join the wireless network, to get your wireless home network up and running.



The starting assumption is that you already have a broadband Internet connection set up, either to a single computer in your house or with a wired home router. If you do not, we recommend that you read through *Home Networking Simplified*.



Note: It is possible to build a home network without wireless, using a wired router and Ethernet cables. It's also possible to build a home network without a router at all, using ad hoc networking and Internet connection sharing on one of your computers. Both of these types of home networks have significant disadvantages. The focus of this book is on wireless home networks, which offer many advantages over wired and ad hoc home networks, so we will not discuss these other network types further in this book.

Connecting the Wireless Router

The first step to building your wireless home network is to connect the wireless router. The steps to connect the wireless router depend on what you are starting with. Most often you will be starting with a single computer connected to your broadband cable or DSL service, which is typically how the broadband service is required to be installed initially. In this case, do the following:

Step 1 Power off or unplug the cable or DSL modem. It's a good idea to have the wireless router and PC turned off also at this point.

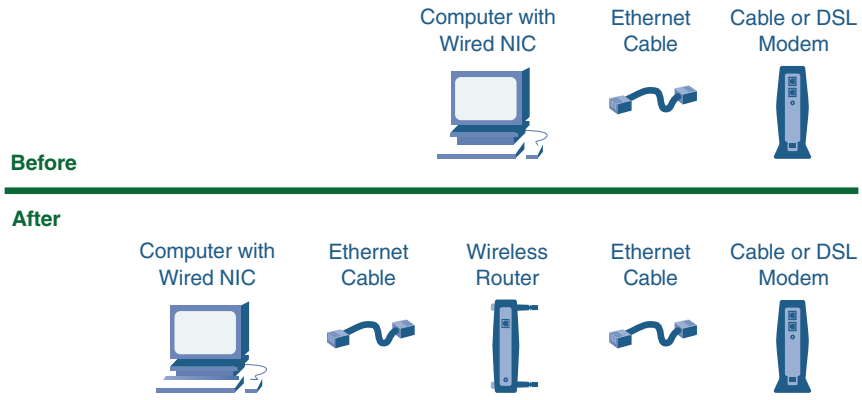
Step 2 Unplug the Ethernet cable from the back of the PC that is connected to the cable or DSL modem.

Step 3 Connect the Ethernet cable just unplugged to the port on the wireless router marked Internet or WAN.

Step 4 Take another Ethernet cable and plug it into the computer where you unplugged the cable in Step 2.

Step 5 Plug the other end of that same cable into a port on the wireless router marked 1. Figure 7-1 shows how the connections should look.

Figure 7-1 Connecting the Wireless Router



Step 6 Power on the cable or DSL modem first and then the wireless router.

After a minute or two, the cable or DSL modem should finish booting and connect to the broadband service. On the front of the wireless router, the power LED and the LED for Ethernet 1 should be lit (assuming it's a Linksys, that is). The Internet LED may or may not be lit. Ignore it for now. We need to start setting up the wireless router.



Note: If you are upgrading from dial-up to broadband DSL or cable service and your service is not installed yet, it's probably a good idea to wait until the installation has occurred before proceeding with your wireless router setup. You could still set up the wireless router and wireless on your computers, but very often a good way to test the connection is to try and browse the Internet, which you will not be able to do until the broadband service is up and running.



You may be asking yourself, "Why are we setting up a wireless router and the first step is to connect a computer to it with a wired cable?" The answer is that whenever you are making changes to your wireless home network, you want to do so from a computer connected to your wireless router with a wired connection. Sometimes you will change settings on the wireless network that affect the wireless signals. If you are changing settings from a wireless-connected computer, it is possible to "cut off the limb you are standing on," so to speak, meaning you can disconnect yourself inadvertently and not be able to get back into the wireless router over a wireless connection. For this reason, we strongly recommend changing settings from a wired computer.

Configuring the Wireless Router

Now that you have finished connecting the router and it's powered on, you need to tell the router a few things about the home network you want to set up. Out of the box, the wireless router has some default assumptions about what the network should look like, but you need to tailor a few of the options, including what type of broadband service you have, and give a name to your wireless network.

To set up a wireless router, you can access the settings in a couple different ways. Almost all wireless routers provide a way to use your Internet browser (such as Internet Explorer) to access all the different settings on the router in a very straightforward manner, just as easy as filling out a web page on the Internet.

Linksys in particular is simplifying this process even further. When you purchase your wireless router, the box includes a CD that contains a Setup Wizard. The Setup Wizard allows you to quickly enter a few settings and get up and running fast. The Setup Wizard will not allow you to change some of the more advanced settings on the wireless router, however. When we need to set some of these later, we will use a method other than the Setup Wizard.

Finally, Linksys is taking new steps to make home networks easy to set up and manage with a product called EasyLink Advisor.

The following sections cover all three types of setups: with Linksys Setup Wizard, with an Internet browser, and with Linksys EasyLink Advisor. Keep in mind that even if you set up your wireless router now using the Setup Wizard, for example, at some point you will probably decide you want to customize your settings a bit more than the Setup Wizard or EasyLink Advisor allow. In that case, it will be necessary to use the Internet browser method, so it's a good idea to get familiar with that option now. Table 7-1 summarizes the different setup methods.

Table 7-1 Wireless Router Setup Options

	When to Use	Where It Runs	Which Settings Can Be Configured
Linksys Setup Wizard	First-time setup only	On the PC (with wired connection), used to initially set up the wireless router	Basic settings only
Internet browser	First-time or subsequent changes	Any PC or laptop connected to the network (wired highly recommended)	All settings
Linksys EasyLink Advisor	First-time or subsequent changes	On a single computer designated as your administration PC (with a wired connection)	Many settings

Check the instructions that come with the wireless router you buy to see which method(s) is included for setup.

Note: You may be tempted to go ahead and set up some of the security features of the wireless router. In fact, the Setup Wizard and EasyLink Advisor prompt you to do so. We strongly recommend not doing so yet. If you jump the gun, you may have trouble and then not know whether the problem is caused by a basic connection issue or a security feature. Get the wireless router and your computers connected first (which we will do in this chapter and Chapter 8, "Wireless NIC Setup") and then apply the security settings (which we walk through in Chapter 9, "Wireless Security Setup").

Using the Linksys Setup Wizard

The current software setup utility shipping with most Linksys routers is the Setup Wizard. The steps for setting up the wireless router with this program are as follows (the Linksys WRT54G is shown as an example):

Step 1 Insert the CD containing the Setup Wizard in the CD or DVD drive of your computer.

Step 2 The Setup Wizard should start automatically. If it does not, access the CD drive using My Computer and double-click the **Setup.exe** program file.

Step 3 Click **Click Here To Start** as shown in Figure 7-2.

Figure 7-2 Starting the Linksys Setup Wizard

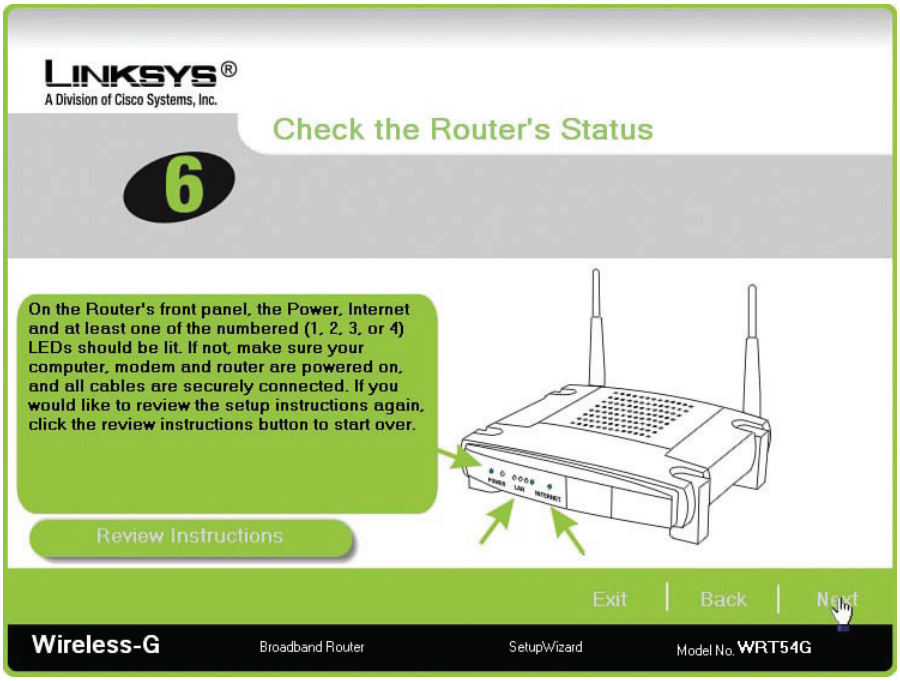




Note: Some of the figures contain a step number in a big black circle on the dialog box. This step number does not correspond to the steps that follow, so do not pay much attention to them.

Step 4 Several steps will be displayed to guide you through the connection steps that we finished in the previous section. You do not need to repeat these steps. Just click **Next**. The last step is shown in Figure 7-3. We skipped showing all the steps to save some space.

Figure 7-3 Guided Connection of Cables

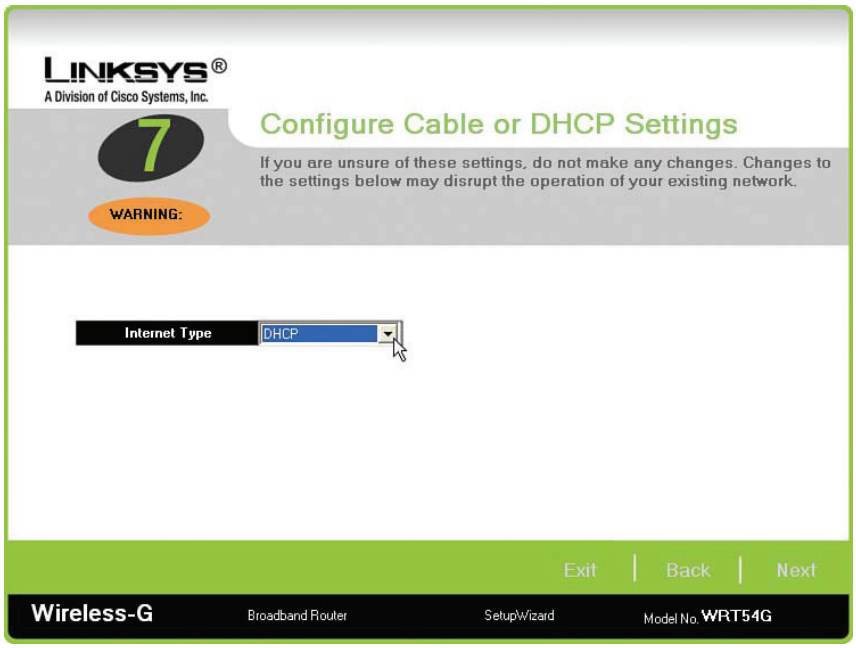




Note: The Linksys Setup Wizard indicates in Figure 7-3 that the Internet LED should be lit. This may or may not be the case. If it is lit, it is because the default out-of-the-box setup happened to match your broadband Internet service settings. It's quite possible the default settings will not match and the LED will not be lit. This is normal, so just move on with the rest of the steps.

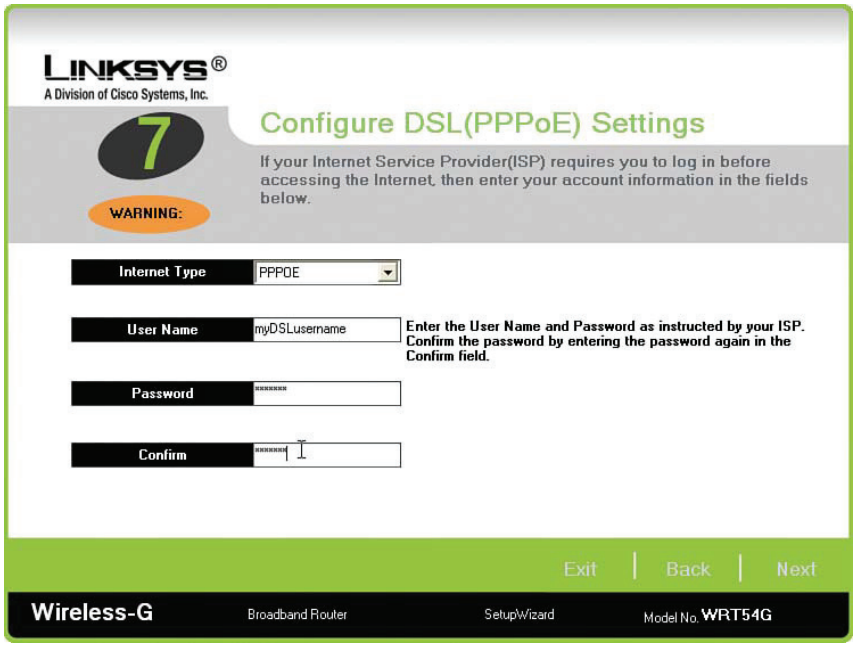
Step 5 If you have cable as your broadband Internet service, set the Internet Type to **DHCP**, as shown in Figure 7-4. Click **Next**. Skip Steps 6 and 7.

Figure 7-4 Set Internet Type to DHCP for Cable



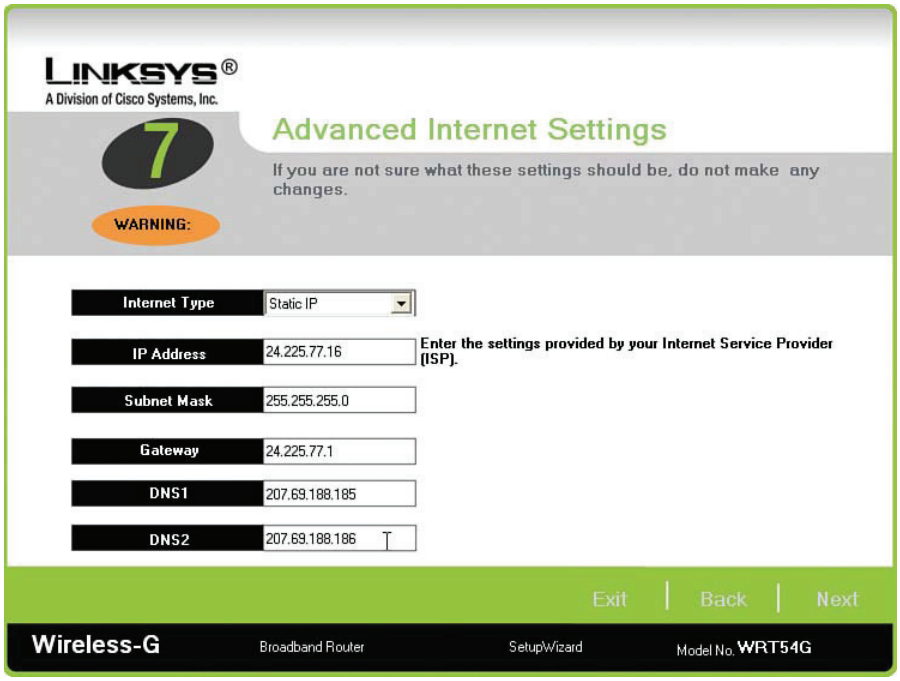
Step 6 If you have DSL as your broadband Internet service, set the Internet Type to **PPPoE**, as shown in Figure 7-5. Enter the username and password for the DSL service from your DSL provider. Click **Next**. Skip Step 7.

Figure 7-5 Set Internet Type to PPPoE for DSL



Step 7 If you have DSL or cable as your broadband Internet service, and have a static IP address from your provider (you usually have to specifically request this and pay extra for it), set the Internet Type to **Static IP**, as shown in Figure 7-6. Enter in the fields provided the IP address, subnet mask, gateway, and DNS addresses given to you by your broadband provider. Click **Next**.

Figure 7-6 Set Internet Type to Static IP for a Static IP Address



Step 8 Enter a new password for the wireless router, as shown in Figure 7-7. This password is to enable you to protect who can log in to the router and change its settings. Choose a strong password (as described in Chapter 9). Write it down. Click **Next**.

Step 9 The Setup Wizard checks to see if the Internet connection was set up correctly and is working, as shown in Figure 7-8. If it is confirmed to be working, the wizard proceeds with the next step; otherwise, the wizard asks whether you want to try repairing the connection.

Figure 7-7 Change the Router's Administrative Password

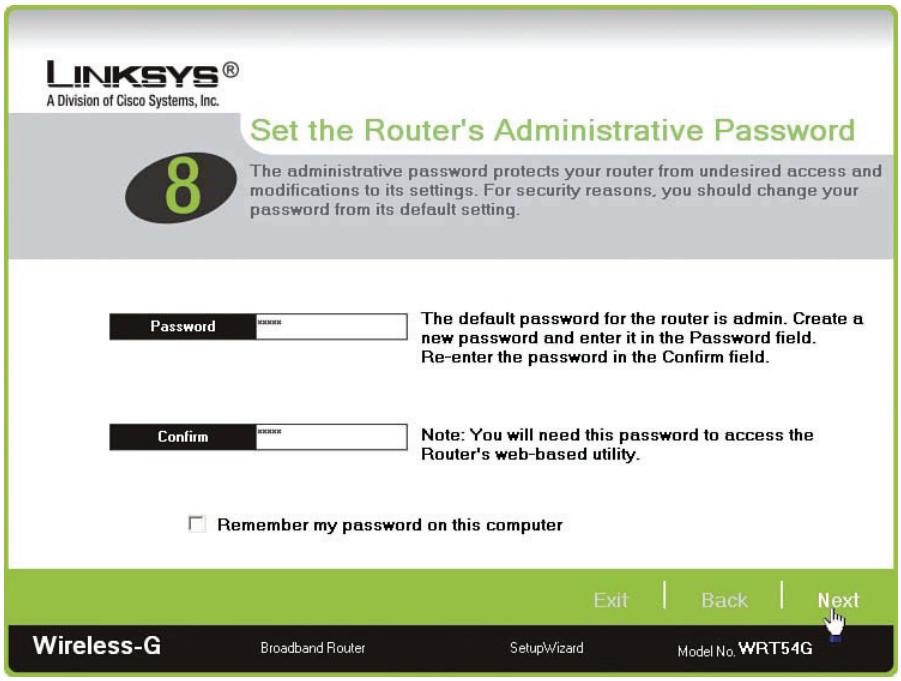
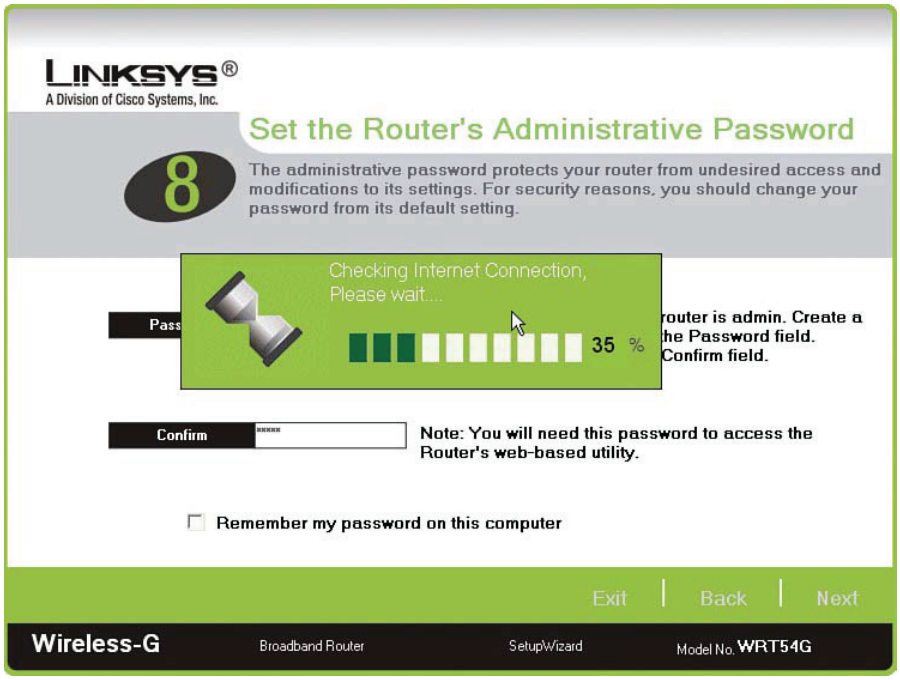
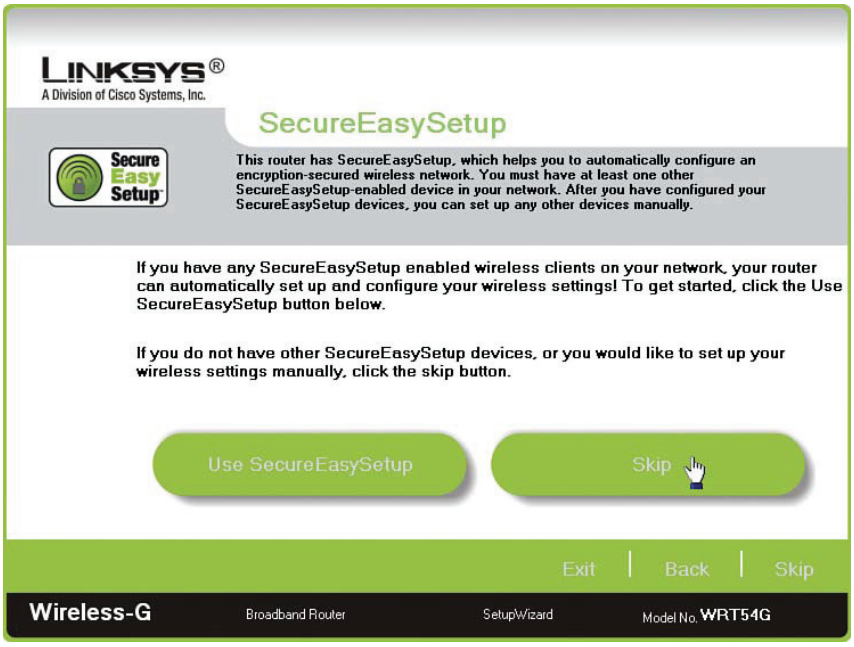


Figure 7-8 Setup Wizard Checks the Internet Connection



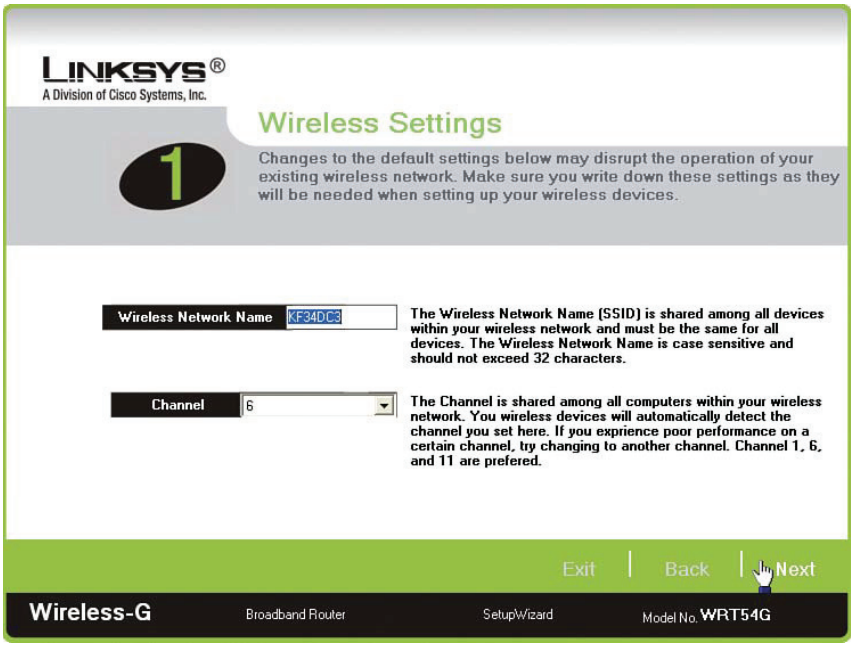
Step 10 If the wireless router you are using supports the Linksys SecureEasySetup feature, you may see a screen such as shown in Figure 7-9. Click **Skip**.

Figure 7-9 SecureEasySetup Screen (if available)



Step 11 Enter the SSID you have chosen for your wireless network, as shown in Figure 7-10 (KF34DC3 in this example). Write it down. Keep the channel at the default setting. Click **Next**.

Figure 7-10 Set the SSID for the Wireless Network



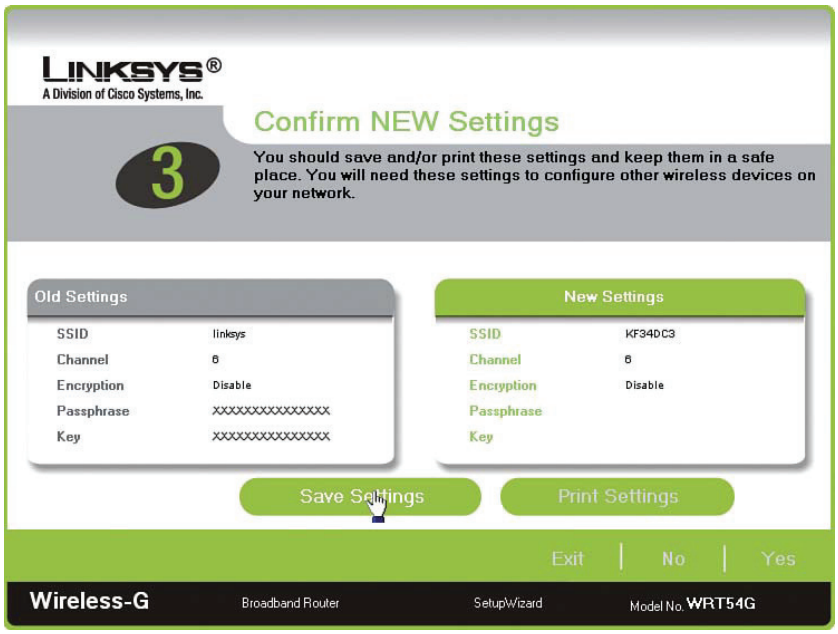
Step 12 Set the Security setting to **Disable**, as shown in Figure 7-11. We will take care of the security settings later (in Chapter 9) after we make sure the network is operating properly. Click **Next**.

Figure 7-11 Leave Wireless Security Disabled for Now



Step 13 Confirm the wireless router settings, as shown in Figure 7-12. Under New Settings, you should see the SSID you have chosen, the default channel number, and that encryption is disabled. Click **Save Settings**.

Figure 7-12 Confirm and Save the Settings



Step 14 As shown in Figure 7-13, that is the end of the setup process. Click **Exit**.

Figure 7-13 Successful Setup



The wireless router should now be set up, connected to the Internet, and broadcasting the wireless signal for your home network.

To test the Internet connection, launch your Internet browser (such as Internet Explorer) and try browsing a web page.

Unfortunately, the Setup Wizard does not provide confirmation that the wireless network is working as planned. We will have to wait until we connect a wireless computer in Chapter 8.

Using an Internet Browser

As mentioned before, the Setup Wizard is a really good approach the first time you set up the wireless router. After that, you are going to want to familiarize yourself with using an Internet browser to change the settings on your wireless router.



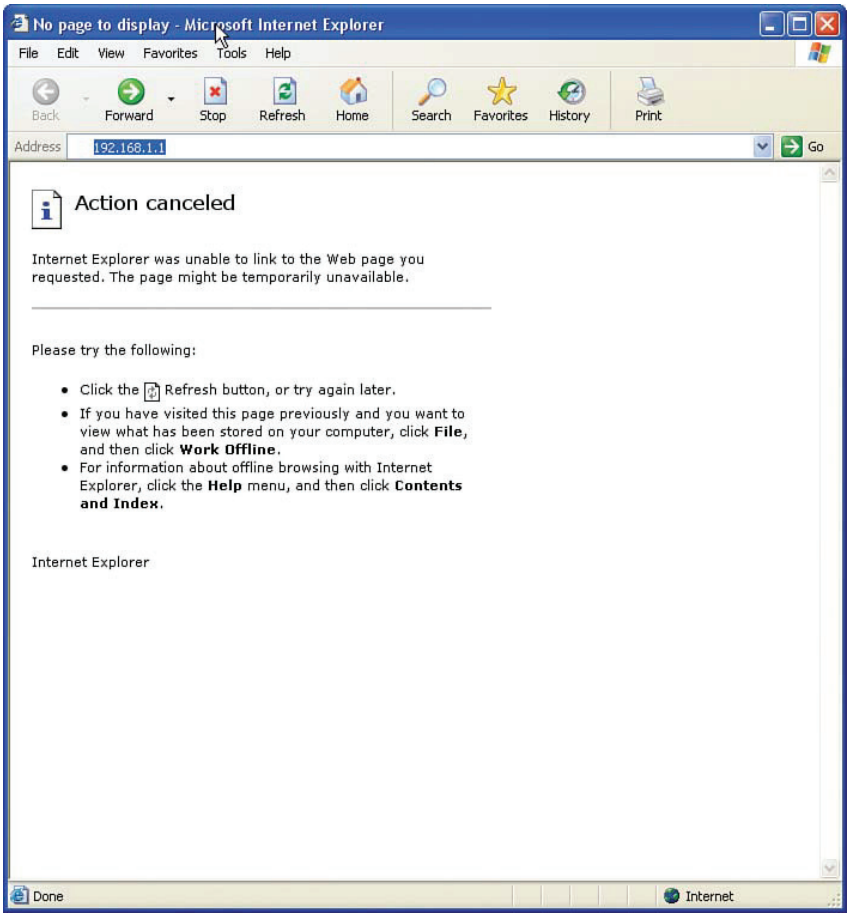
Note: If you used the Setup Wizard to set up the wireless router, you do not need to repeat the steps that follow. They essentially do the same thing, just using the Internet browser method instead. As mentioned earlier, using the Internet browser allows you to configure a lot more settings than the Setup Wizard.

The steps for setting up the wireless router with a browser are as follows (the Linksys WRT54G is shown as an example):

Step 1 Start the Internet browser you use (such as Internet Explorer). Type **192.168.1.1** in the Address field, as shown in Figure 7-14, and click **Go**. This is the default IP address of Linksys routers out of the box.

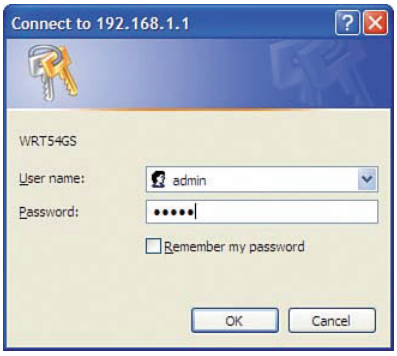
Note: The default IP address used by Linksys wireless routers is 192.168.1.1. Wireless routers from other manufacturers could use a different default, so consult the user guide to see what the default is.

Figure 7-14 Point Your Internet Browser to the Wireless Router



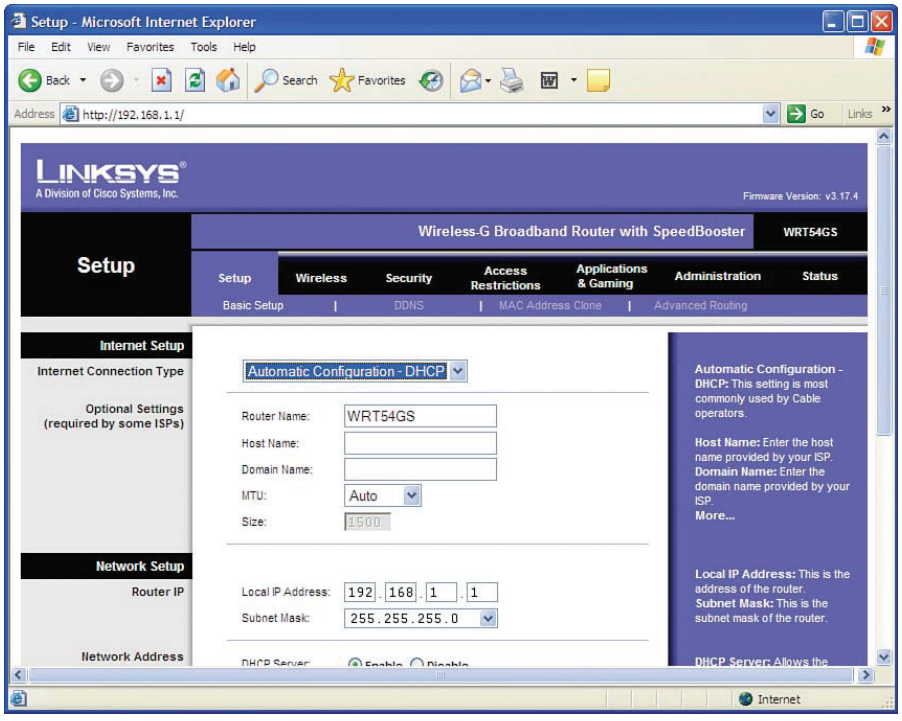
Step 2 You are prompted for the wireless router's username and password, as shown in Figure 7-15. Enter the default for Linksys routers, which is **admin** for the User Name field and **admin** for the password. Click **OK**.

Figure 7-15 Enter the Username and Password for the Wireless Router



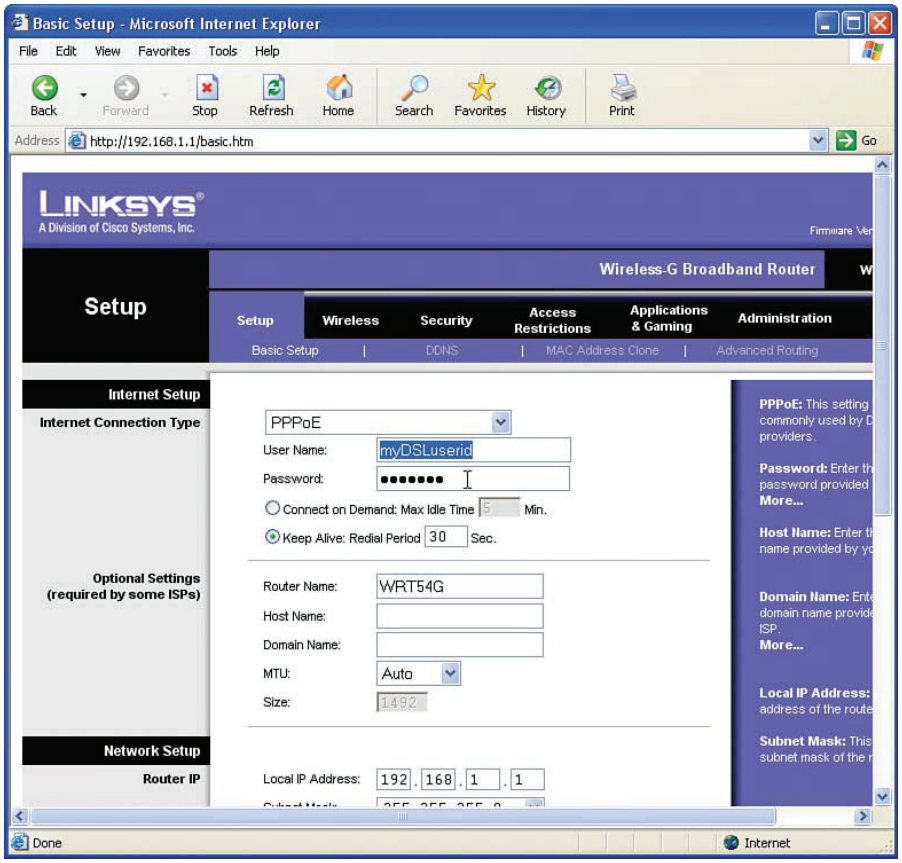
Step 3 If you have cable as your broadband Internet service, set the Internet Connection Type to **Automatic Configuration – DHCP**, as shown in Figure 7-16. Click **Save Settings**. Skip Steps 4 and 5.

Figure 7-16 Set Internet Connection Type to DHCP for Cable



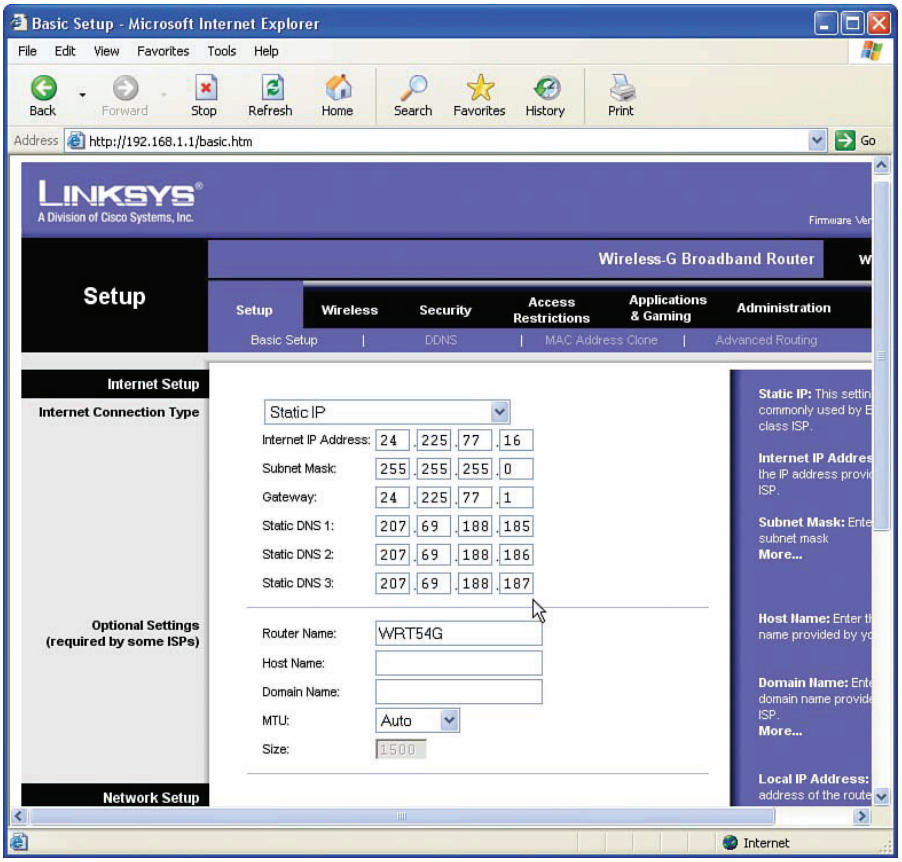
Step 4 If you have DSL as your broadband Internet service, set the Internet Connection Type to **PPPoE**, as shown in Figure 7-17. Enter the username and password for the DSL service from your DSL provider. Click **Save Settings**. Skip Step 5.

Figure 7-17 Set Internet Connection Type to PPPoE for DSL



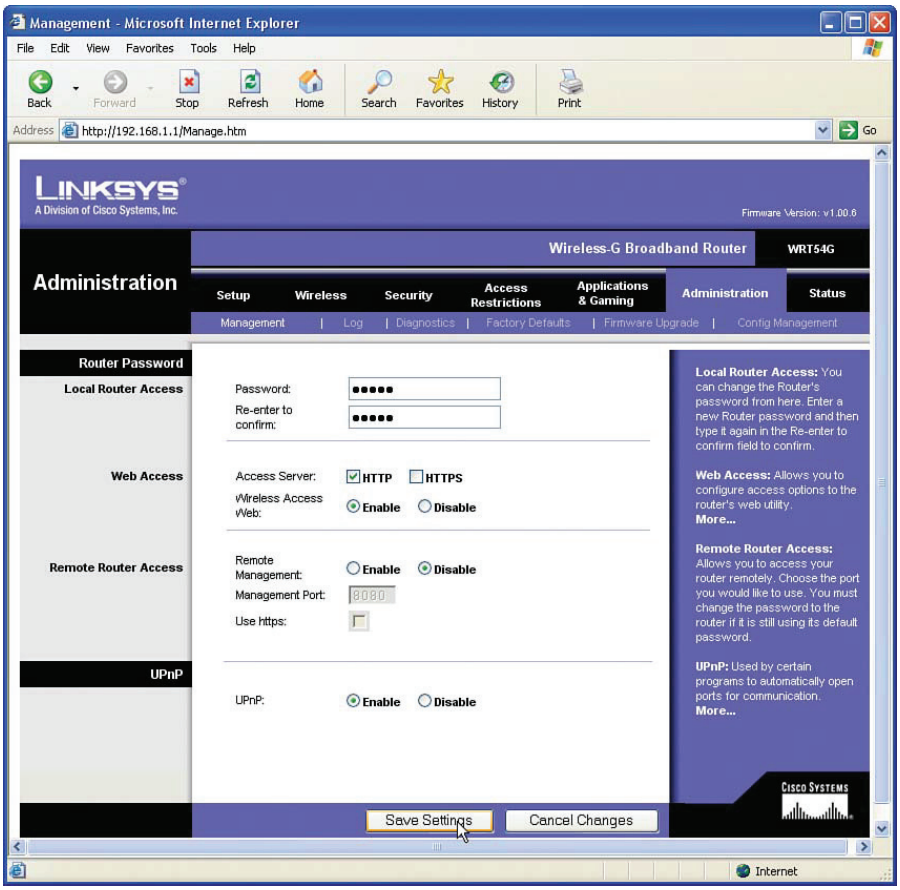
Step 5 If you have DSL or cable as your broadband Internet service and have been assigned a static IP address (typically you must request this for a specific reason and pay extra), set the Internet Connection Type to **Static IP**, as shown in Figure 7-18. Enter in the fields provided the Internet IP address, subnet mask, gateway, and static DNS addresses given to you by your broadband provider. Click **Save Settings**.

Figure 7-18 Set Internet Connection Type to Static IP for Broadband with Static IP Addresses



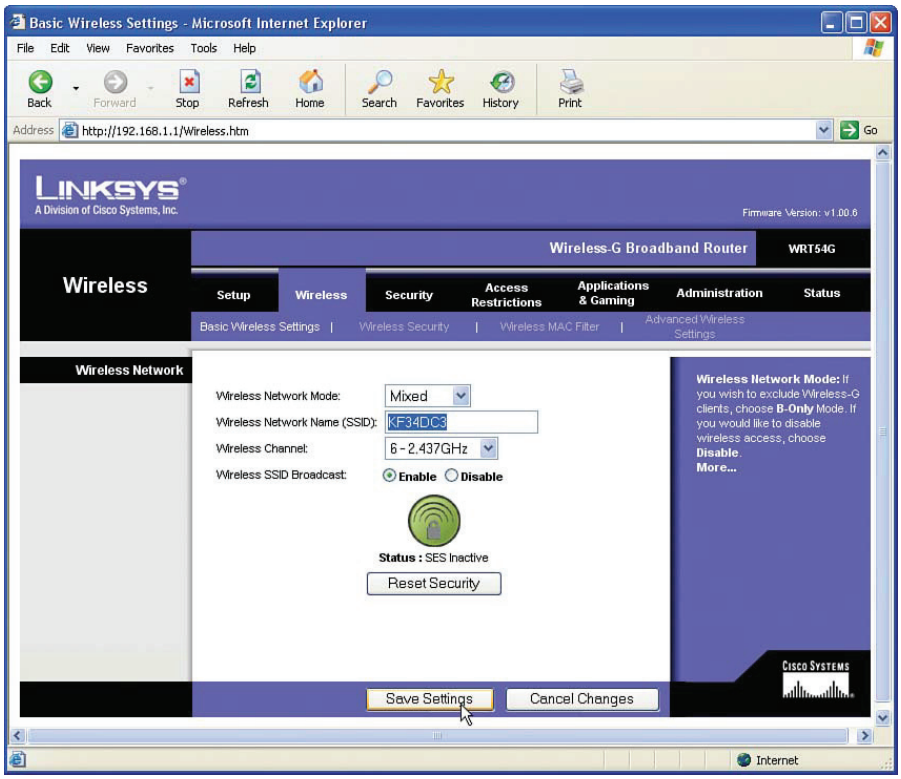
Step 6 Click the **Administration** tab near the top of the browser and then click the **Management** subtab. Enter a new password for the wireless router, as shown in Figure 7-19. This password is to enable you to protect who can log in to the router and change its settings. Choose a strong password. Write it down. Click **Save Settings**. You may be prompted to log in again to the router using the new password.

Figure 7-19 Change the Router's Administrative Password



Step 7 Click the **Wireless** tab and then click the **Basic Wireless Settings** subtab. Enter the SSID you have chosen for your wireless network, as shown in Figure 7-20 (KF34DC3 in this example). Keep Wireless Channel at the default setting. Click **Save Settings**.

Figure 7-20 Set the SSID for the Wireless Network

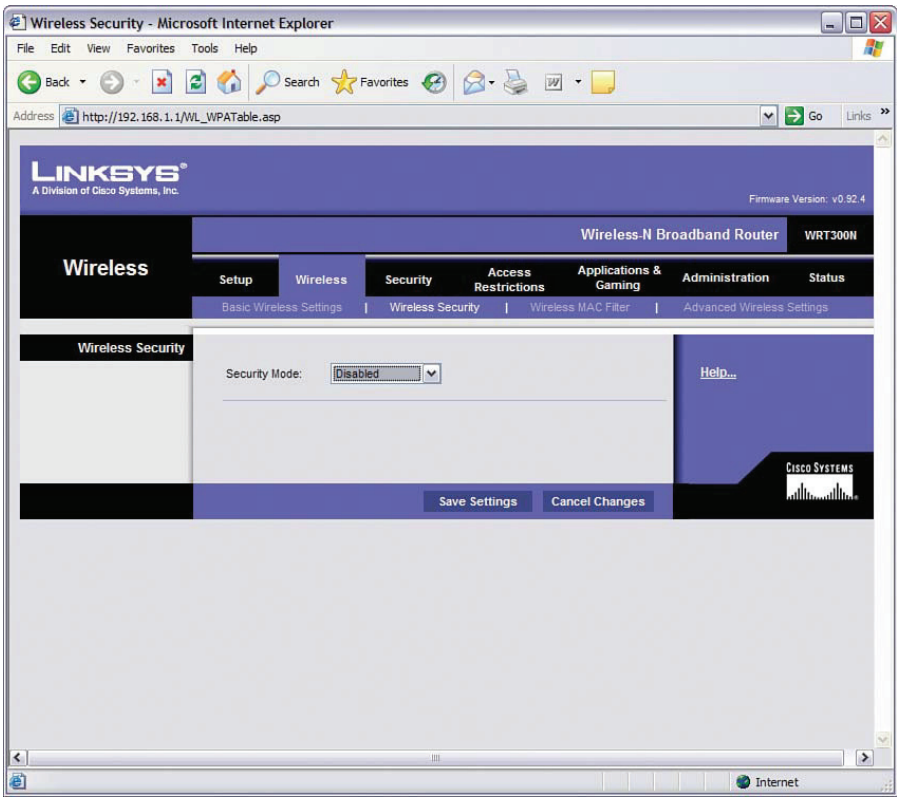


Step 8 Click the **Wireless Security** subtab. Verify the Security Mode is set to **Disabled**, as shown in Figure 7-21. We will take care of the security settings later, in Chapter 9, after we make sure the network is operating properly. Click **Save Settings**.

The wireless router should now be set up, connected to the Internet, and broadcasting the wireless signal for your home network. To test the Internet connection, start your Internet browser (such as Internet Explorer) and try browsing a web page.

To confirm that the wireless network is working as planned, we will have to wait until we connect a wireless computer (in Chapter 8).

Figure 7-21 Leave Wireless Security Disabled for Now



Using Linksys EasyLink Advisor

The newest software setup utility for Linksys routers (at the time of this book's publication) is the EasyLink Advisor program.

EasyLink Advisor is different from the two methods described previously. The Setup Wizard runs one time (for the most part) on a computer connected to the router with a wired connection. The Internet browser can be used any time you want to change settings on the wireless router.

In comparison, EasyLink Advisor is a program that is installed on a designated computer on your home network; one with a wired connection to the wireless router. The program keeps a database of the settings for the router on that computer, and it can be used anytime to monitor the network status, change settings, add new computers and devices, and so on.

The steps for setting up the wireless router with Linksys EasyLink Advisor are as follows (the Linksys WRT54G is shown as an example):

Step 1 Insert the CD containing the EasyLink Advisor software in the CD or DVD drive of your computer.

Step 2 The installation should start automatically. If it does not, access the CD drive using My Computer and double-click the **EasylinkAdvisorWeb.exe** program file.



Note: If you have a personal software firewall program installed on the computer that you are installing EasyLink Advisor on, it may block EasyLink from accessing your wireless router. Click **Allow** when your personal software firewall asks if you want to allow EasyLink to access the Internet (and router), or temporarily disable the software firewall while you are setting up your network.

Step 3 After installation the program will launch, as shown in Figure 7-22.

Figure 7-22 Starting Linksys EasyLink Advisor



Step 4 EasyLink asks for a network name, as shown in Figure 7-23. Enter a name for your network (we used KF34DC3 in this example). The name cannot contain any spaces or special characters because EasyLink also uses this name for the SSID of your wireless network. Click **Next**.

Step 5 EasyLink scans the network, as shown in Figure 7-24. It first tries to configure the settings for cable broadband, and then, if unsuccessful, prompts you for your DSL username and password.

Figure 7-23 Setting the Network Name

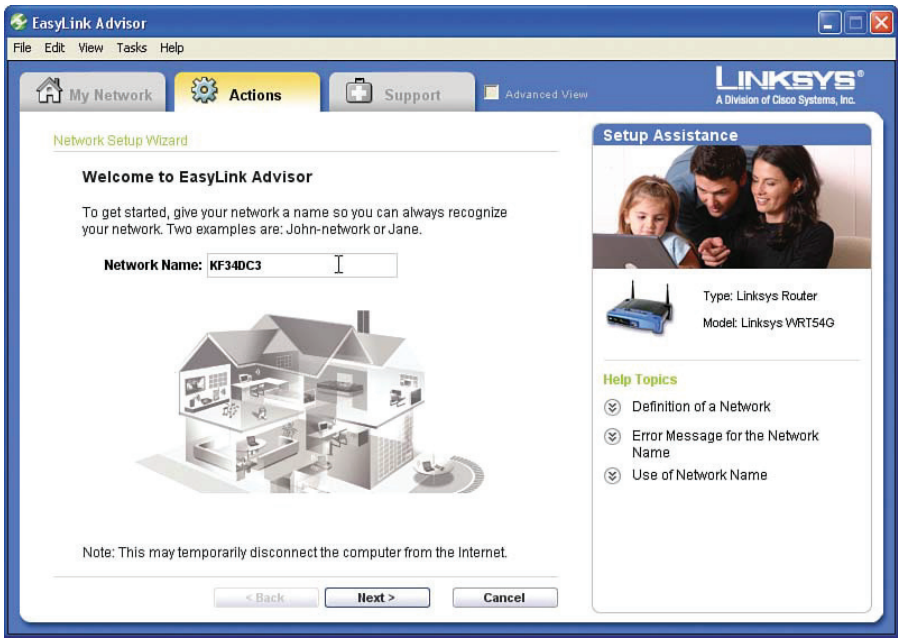
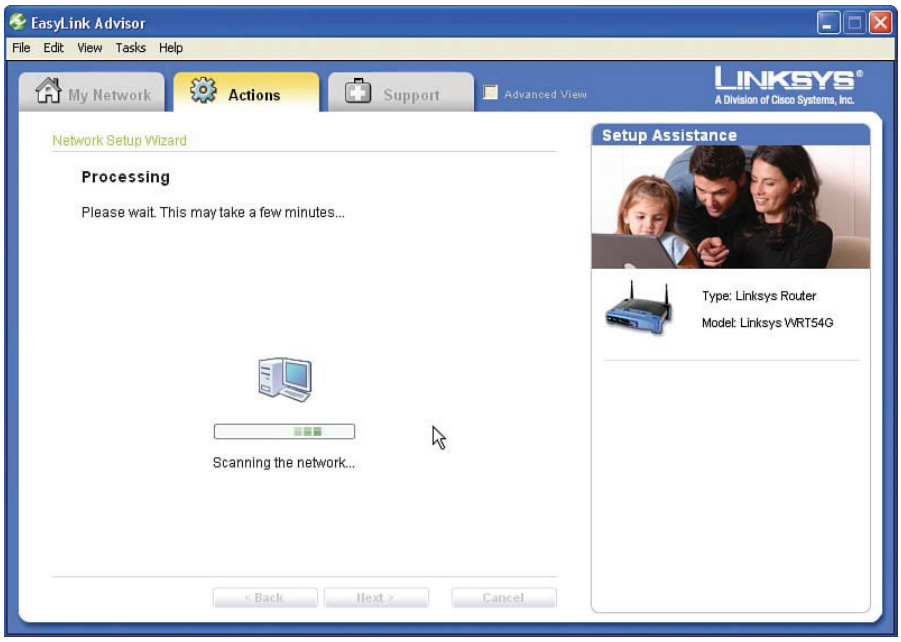


Figure 7-24 EasyLink Scanning Your Network



Step 6 EasyLink asks you to visually confirm that the wireless router LEDs are lit appropriately, as shown in Figure 7-25. Check your router and click **Next** after confirming.

Figure 7-25 Visually Confirm the Wireless Router Operation



Step 7 EasyLink asks if you want to turn on wireless security, as shown in Figure 7-26. As in the previous sections, we recommend not turning it on at this point. We will take care of the security settings later, in Chapter 9, after we make sure the network is operating properly. Click the **Turn Off Wireless Security** radio button and click **Next**.

Figure 7-26 Leave Wireless Security Disabled for Now



Step 8 EasyLink confirms that the wireless network is set up properly, including the broadband Internet access, as shown in Figure 7-27. Click **Click Here to Test Your Internet Connection with Your Web Browser**, which starts your Internet browser. If you can browse a web page, great. If not, see the troubleshooting suggestions on the right side of the window and also the troubleshooting chapters later in this book (Chapters 10 through 12). Click **Finish** when done.

Figure 7-27 Wireless Network Is Now Set Up



Step 9 Click the **My Network** tab, as shown in Figure 7-28. Starting at the top left, your ISP is displayed, then the broadband modem, followed by your wireless router. Underneath the wireless router you will see the computers (and other devices) connected to your home network. Right now only the computer we used to set up the network is shown.

Note: At the time this book was written, EasyLink Advisor did not provide a means to change the administrator password on the router. We recommend doing so (for security reasons). So if you use EasyLink to set up and manage your home network, we recommend using the Internet browser method to change the password. EasyLink will try to access the router using the default password (admin) and then prompt you for the new password you assigned, so that it can still communicate with the router.

Figure 7-28 EasyLink Graphical View of Your Network

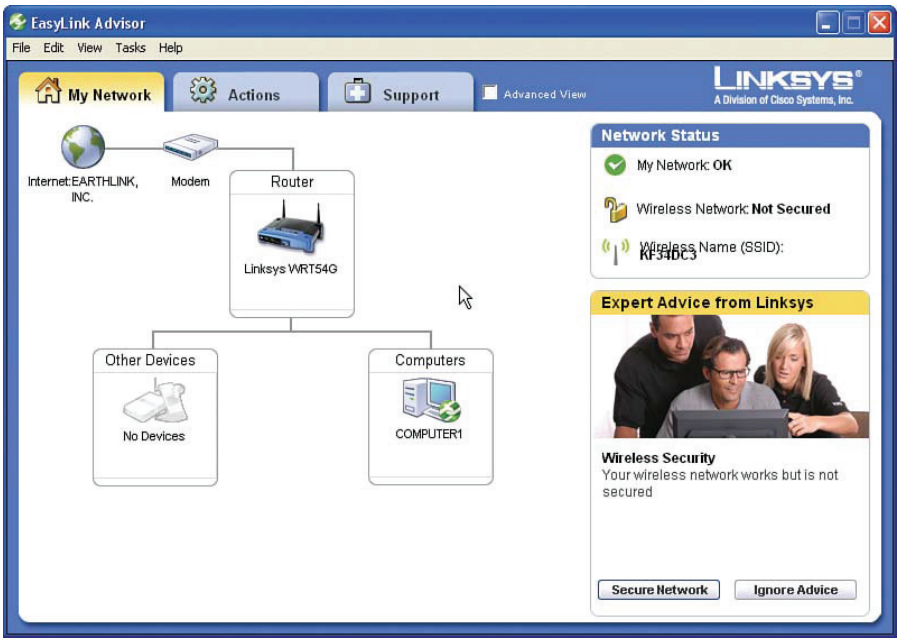
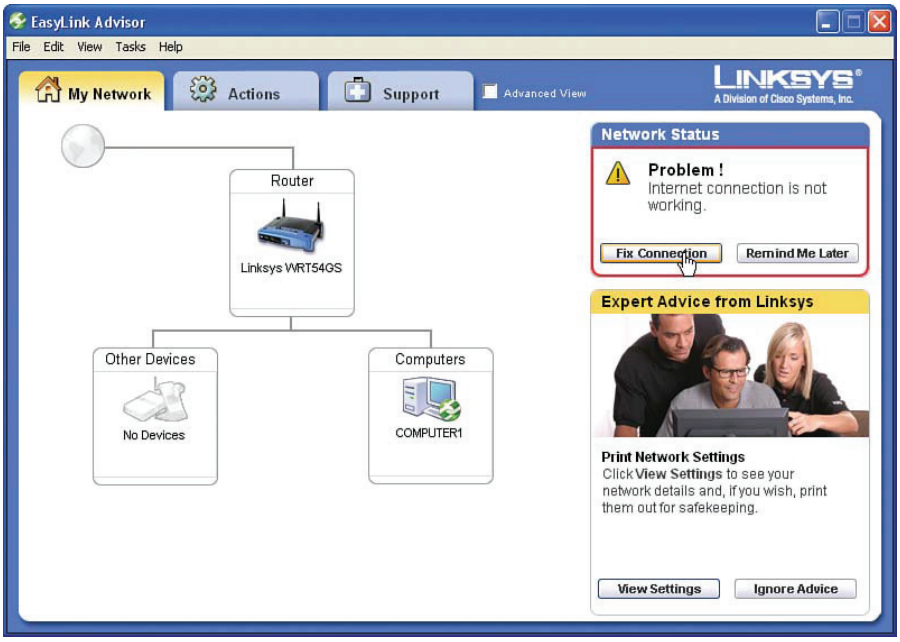


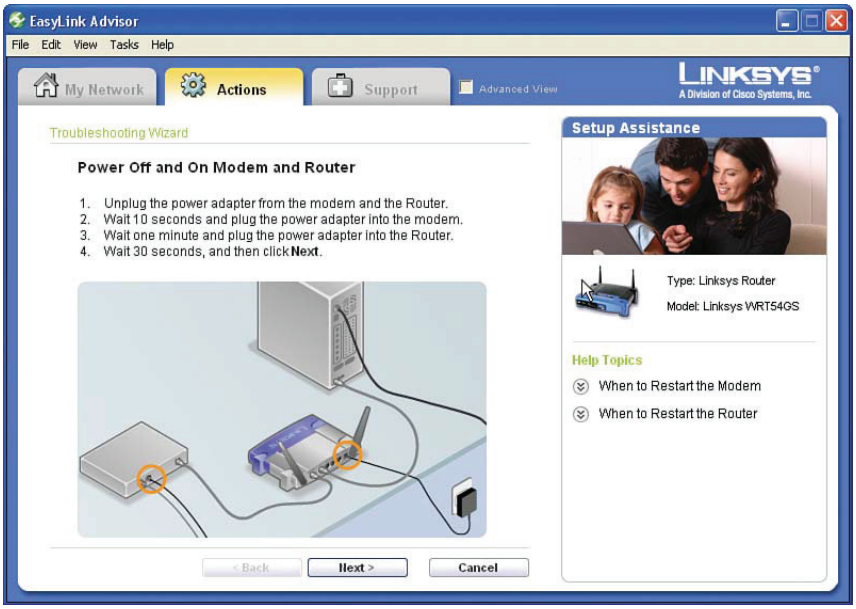
Figure 7-28 shows what the initial network should look like if things are working properly, including connectivity to the Internet. EasyLink Advisor can also help troubleshoot when something is not quite right. If, for example, the Internet connectivity is not working properly, EasyLink tells you, as shown in Figure 7-29.

Figure 7-29 EasyLink Advisor Notices the Internet Connection Is Not Working



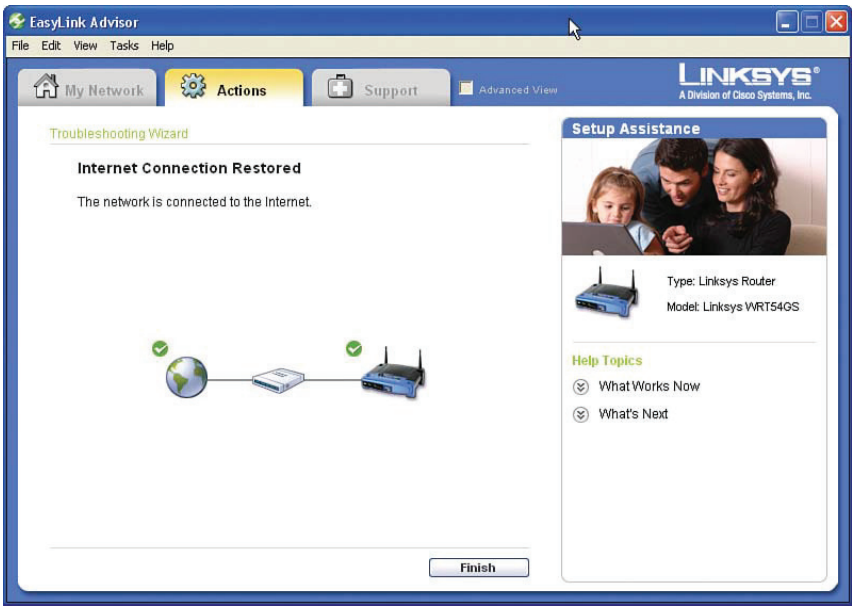
If you click **Fix Connection**, EasyLink Advisor will walk you through different steps to help you find out what is wrong. Figure 7-30 shows an example of EasyLink suggesting to reboot the wireless router and shows the steps to do so.

Figure 7-30 EasyLink Advisor Advises How to Fix the Internet Connection



After one of the steps is successful at repairing the Internet connection, EasyLink Advisor shows that the connection is working, as shown in Figure 7-31.

Figure 7-31 EasyLink Advisor Shows the Internet Connection Status Working



As you can see, EasyLink Advisor provides an easy way to set up your home wireless network. Keep in mind that EasyLink is not just for setup, but also for making ongoing changes and additions to your home network.

Chapter 8 shows how to use EasyLink to add computers to the network, and Chapter 9 shows how to turn on wireless security with EasyLink.

Summary

There are a couple of methods for setting up the wireless router in your home network. It's getting easier and easier to do so.

The Linksys Setup Wizard is an easy way to set up the network initially but does not provide a good way to make ongoing changes.

Using an Internet browser to access and change the router settings provides access to all the settings in the router. At some point you will likely have to change a setting that the other setup utilities do not enable you to change, so it's a good idea to be familiar with this method even if you use an automated program (like the Setup Wizard or EasyLink Advisor) to set up the wireless network.

EasyLink Advisor is both a setup tool and a good way to make ongoing changes and additions to your home network. As Linksys evolves this program, it will provide more extensive capabilities for easy management of your home network.

When you purchase your Linksys wireless router, it will come with a CD containing either the Linksys Setup Wizard or the Linksys EasyLink Advisor. Use whichever one comes with your wireless router. You use the Setup Wizard only once, and then switch to using the Internet browser to make further changes. EasyLink Advisor can be used for both initial setup and ongoing changes; however, there may be settings that you cannot perform with EasyLink Advisor, and in those cases you should just use the Internet browser to set them.

Where to Go for More Information

For more information about Linksys EasyLink Advisor, go to the Linksys main website: www.linksys.com.

Check out Bradley Mitchell's article on About.com titled "Networking with a Router": http://compnetworking.about.com/od/homenetworking/a/routernetworks.htm.

CHAPTER 8

Wireless NIC Setup

Each computer or device that you want to join your wireless network needs a wireless network interface card (NIC). A wireless NIC provides a number of functions, including

- Enabling a computer (or device) to connect to your home network through a wireless signal
- Securing the communications path between the wireless router and your computers and devices connected over wireless
- Providing a way for you to connect your computer to other wireless networks outside your home

This chapter provides the steps necessary to set up your wireless NICs, getting them to communicate with your wireless home network. The starting assumption is that you have already completed the wireless router setup in Chapter 7, "Wireless Router Setup."

Installing the Wireless NIC

There are several types of wireless NICs to consider (as introduced in Chapter 6), including

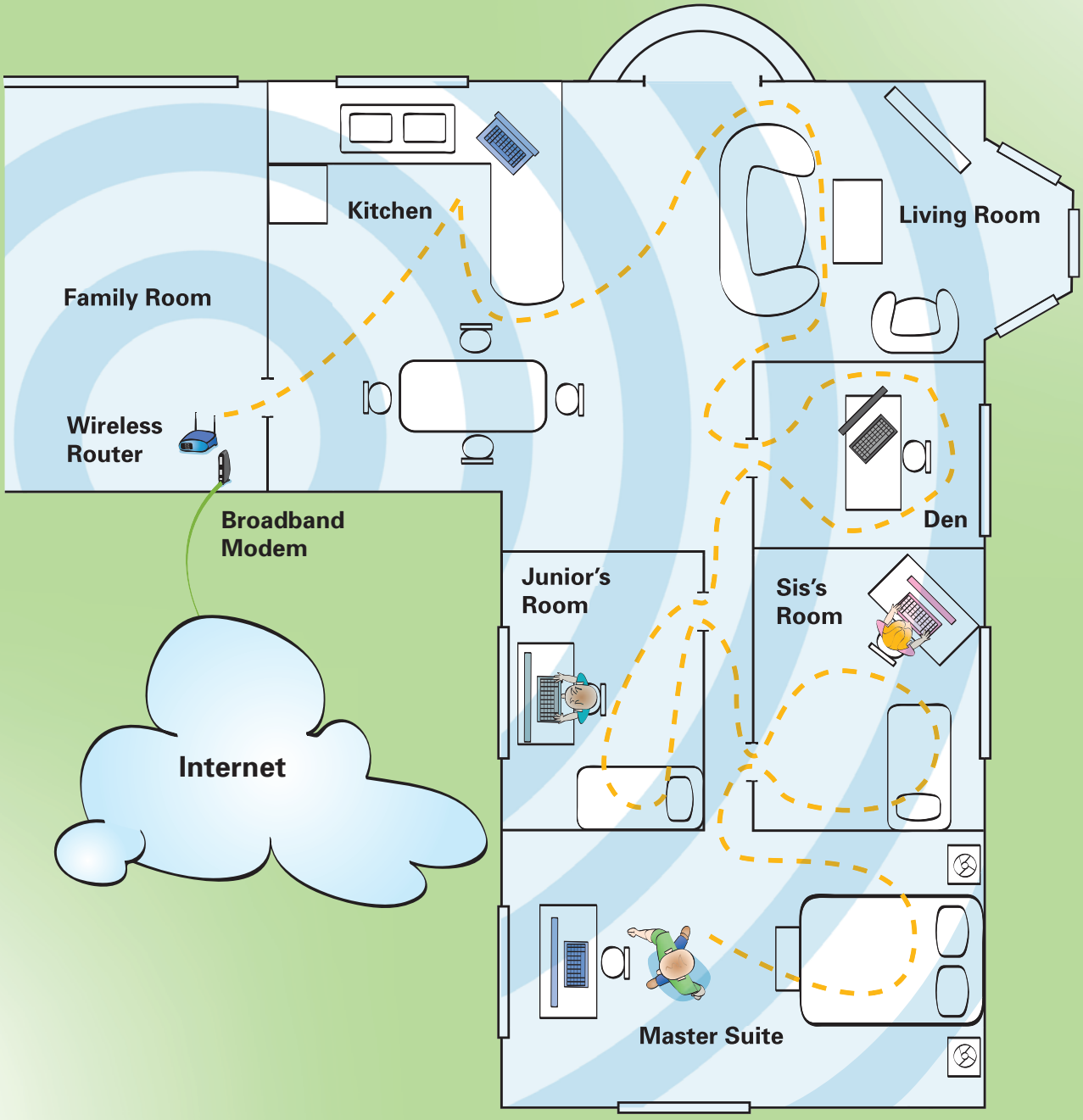
- **PCI card**—Installs inside a desktop PC
- **PCMCIA or ExpressCard**—Plugs into a laptop
- **Integrated**—Is already built into a laptop
- **USB**—Plugs into the USB port of any computer

If you have a laptop, first check whether it already contains an integrated wireless NIC. If it does, then you are all set. If your laptop does not have a built-in wireless NIC (or if it does but not the wireless standard you want to use), then the best option is to buy a PCMCIA wireless card.

If you have a desktop (or tower) PC, check whether it already contains an integrated wireless NIC, because (although not that common) some are now shipped with one. If not, then you have two options:

- Buy a PCI wireless card that installs inside the computer in an open card slot
- Buy a USB wireless NIC that plugs into any open USB port

USB NICs are handy because you can avoid opening up a computer to install them, but they do provide another box (albeit a little one) to add to a cluttered computer desk. USB is also an option for laptops, but they are a bit unwieldy on the go, so most people opt for a PCMCIA card.


Kitchen
Living Room
Family Room
Wireless
Router
Broadband
Modem
Den
Junior's
Room
Sis's
Room
Internet
Master Suite

If you have an older PC or an early version of the Xbox, then there's a good chance that you either don't have a USB port or do have one but it is taken up by something else such as a printer. In this case, a wireless Ethernet bridge is a good alternative. It works just like a wireless USB NIC, except that it plugs into your Ethernet port, essentially changing a wired port to a wireless one.



Note: By the way, USB wireless NICs may also be a good option for other devices you want to connect to your wireless network, such as a DVR or video game console. However, make sure that the device supports the specific USB wireless NIC, because they are not as universally supported as they are in PCs. We will discuss some of these options more in Chapter 13, "Wireless Video and Entertainment," which explains how to connect entertainment devices to your wireless network.

The next few sections discuss installing the different types of wireless NICs. Skip to the sections that match the types of NICs you chose for the computers to connect to the network. In general, there are two types of installation procedures:

- Load software from a CD that comes with the NIC and then actually plug the NIC into the PC or laptop
- Plug the NIC into the PC or laptop, and then Windows XP performs an auto-install, possibly asking for the CD that comes with the NIC

Which type you follow depends on the type of NIC and the version of Windows you are running. If you are running a Windows version older than XP (such as 2000, 98SE, and so on), you will likely follow the first type. If you are running Windows XP or Vista, you will likely follow the second type. However, you should look at the quick setup instruction sheet that comes with the wireless NIC to see which is recommended.

Installing a PCI Wireless Card in a Desktop Computer

To install a PCI wireless card in a desktop computer, follow the manufacturer instructions that came with the card you purchased. In general, you will do the following:

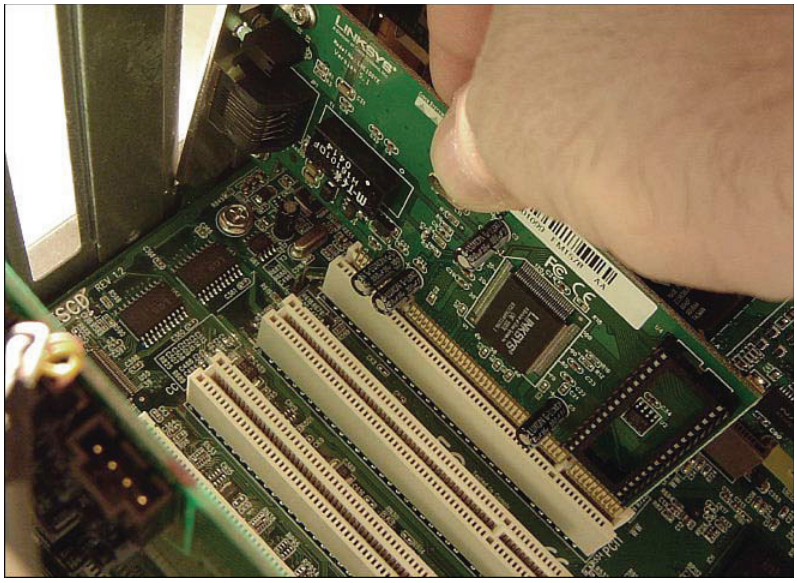
Step 1 Shut off and unplug the PC and then open it up. This is typically done by removing the screws on the outer edge of the back of the computer. Once the screws are off, the outer casing should slide off (see the user manual for your computer for how to remove its cover).



Caution: Because of the potential damage that can be caused by static electric discharge, it's a good idea to take precautions so that you don't zap your computer. As long as you don't shuffle across your shag carpet wearing your socks or play with balloons beforehand, you're probably okay. But you should touch a metal doorframe or doorknob to discharge yourself.

Step 2 Plug the new NIC into an available slot (see Figure 8-1).

Figure 8-1 Installing a PCI Wireless Card



Step 3 Close up the computer.

Step 4 Turn on your computer and let your operating system boot.

Step 5 Windows may have all the drivers needed, or it may need to copy some from the CD that came with your NIC. If you are prompted to do so, put the CD into your CD drive.

Step 6 The install program on the CD should start by itself. If it does not, open a directory window and double-click the install or setup icon in the CD directory.

Again, for some installations you will insert the card first, for others you will run a setup utility from a CD first, and then plug in the card. Look at the quick setup instruction sheet that comes with the wireless card to see which you should do. Make sure to consider which Windows version you are using. Many setup instructions will have one set of instructions for Windows XP/Vista and another for older versions of Windows.

Installing a PCMCIA Wireless Card in a Laptop Computer

To install an PCMCIA NIC in a laptop, plug the NIC into an available PCMCIA slot in your laptop. Again, look at the quick setup instruction sheet that comes with the wireless card to see if you should run a setup utility from the CD first or plug the card in first.

The following steps install a PCMCIA wireless card from Linksys (WPC54G) into a laptop running Windows XP:

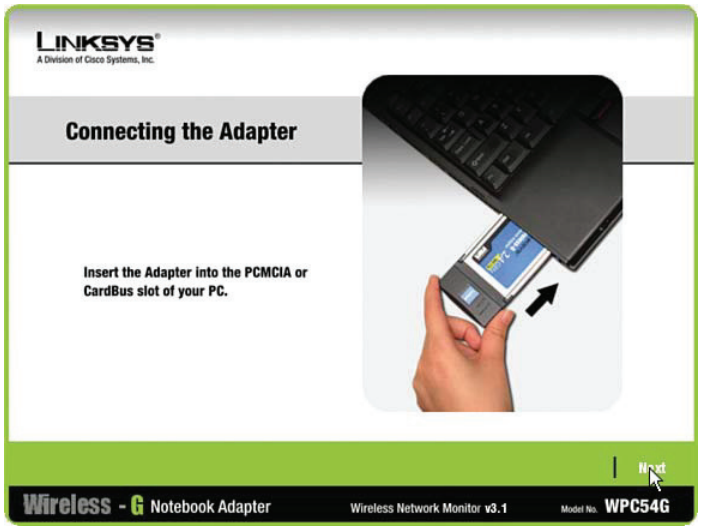
Step 1 Insert the CD that came with the wireless card in your CD or DVD drive. The setup program should start automatically. If it does not, browse the files on the CD and double-click the install program to start it. Click **Click Here to Start** (see Figure 8-2).

Figure 8-2 Installing a PCMCIA Wireless Card (Linksys WPC54G)



Step 2 When the setup utility prompts you to do so, insert the PCMCIA wireless card into an available slot in the laptop (see Figure 8-3).

Figure 8-3 Plugging in a PCMCIA Wireless Card



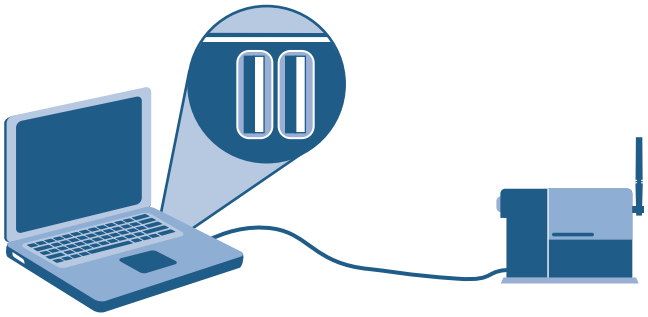
You generally do not need to shut down the laptop, just plug in the card.

Installing a USB Wireless NIC in a Computer

Let's take one example of installing a USB wireless NIC from Linksys (WUSB54G) into a computer running Windows XP. In this case, the setup instructions tell us to plug the USB NIC in first, and then insert the CD if Windows XP asks for it.

Step 1 Connect one end of the USB cable to the wireless NIC (see Figure 8-4) and the other to an open USB port on your computer (desktop, tower, or laptop).

Figure 8-4 Connect the USB Wireless NIC



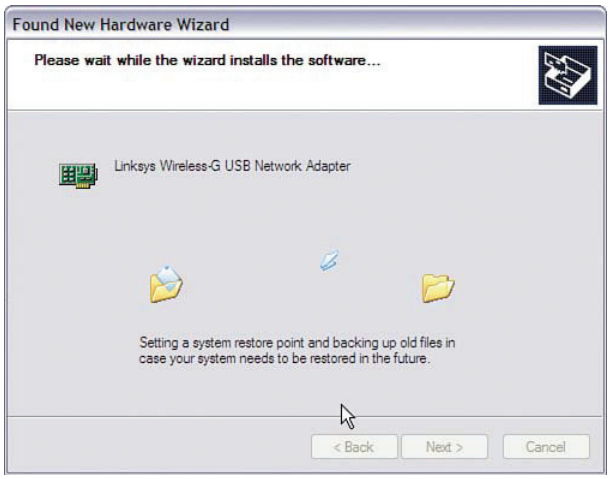
Step 2 Windows XP detects the new hardware plugged into the computer and starts the process of installing the software. Check the **Install the Software Automatically** check box and click **Next** (see Figure 8-5).

Figure 8-5 Windows XP Detects the New Hardware



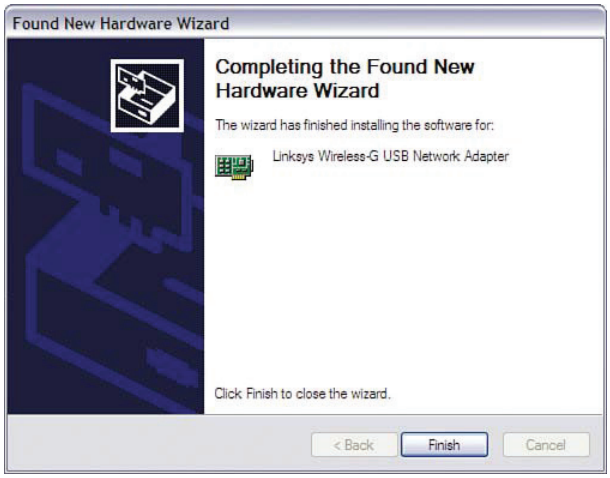
Step 3 Windows XP locates the software drivers for the USB wireless NIC (see Figure 8-6). If it cannot locate them automatically, it may prompt you to insert the CD that came with the NIC when you bought it. Click **Next**.

Figure 8-6 Windows XP Locates the Driver Software



Step 4 The install was successful (see Figure 8-7). Click **Finish**.

Figure 8-7 Installation Is Complete



You generally do not need to shut down the computer, just plug in the USB NIC. Because the wireless USB NIC gets its power from the computer it is connected to through the USB cable, you do not need to worry about a power cord.

Associating the Wireless NIC to the Wireless Router

The next step after installing the wireless NIC is to "teach it" how to find and communicate with your wireless router (that you installed in Chapter 7).

Whenever your wireless NIC is enabled and turned on, it starts scanning for a wireless router to communicate with, much like when you turn on your cell phone and it immediately starts searching for a cell tower to connect to.

It's quite possible (likely, even) that your NIC will be able to see signals from two or more wireless routers. Figure 8-8 in the next section shows an example where we can see the signals from our own wireless router, but also from a neighbor's and from a coffee shop's across the street. So how does the NIC know which is your router?

The answer is the SSID. Remember in Chapter 7 that when we set up our wireless router we assigned it a unique name for our wireless network (KF34DC3 in our example). Each wireless router (and access point) identifies itself using its assigned SSID. So, for our NIC to communicate with our router, we have to tell it which SSID to look for.



Note: One question that comes up is what happens if two wireless routers use the same SSID? The answer depends somewhat on your wireless NIC, but in general the NIC will pick the strongest signal it sees and try to associate to that wireless router. In most cases, "strongest" means the one in your house, but that is not always the case. If your neighbor's wireless router has a stronger signal than yours and you are both using the same SSID, it's very possible your NIC will try to associate with their router, not yours. This is another reason it's very important to pick a unique SSID for your network.

Wireless Profiles

The process of "teaching" NICs how to talk to a wireless router is called managing wireless connections. The process of managing wireless connections is pretty simple for desktop computers and other devices that never leave your home, because you have to manage those connections just once. For laptops, it's a little more complicated, because you may want to connect to your wireless router when you are home, and to other wireless connections when you are not at home (for example, at work, at the airport or a hotel, at a coffee shop, and so on).

If wireless NICs could only remember how to connect to a single wireless router, we would have to reprogram the NIC every time we wanted to connect to a different wireless signal (see Figure 8-8).

Fortunately, we can use any number of wireless connection managers and create a set of wireless profiles. Each profile contains the critical information the NIC needs to know to remember how to connect to a wireless router. Profiles can include the SSID, the type of wireless security being used, the encryption key (see Chapter 9, "Wireless Security Setup"), and other information.

Then, when the wireless NIC encounters wireless signals, it compares the information being advertised by the wireless router with the stored profiles to see if there is a match. In the example shown in Figure 8-9, the wireless NIC has three wireless profiles configured, named Home, Work, and Hotel. The SSIDs for these three wireless networks are KF34DC3, Corporate-G, and StayWithUs, respectively.

Figure 8-8 Wireless NIC Scanning for Wireless Networks

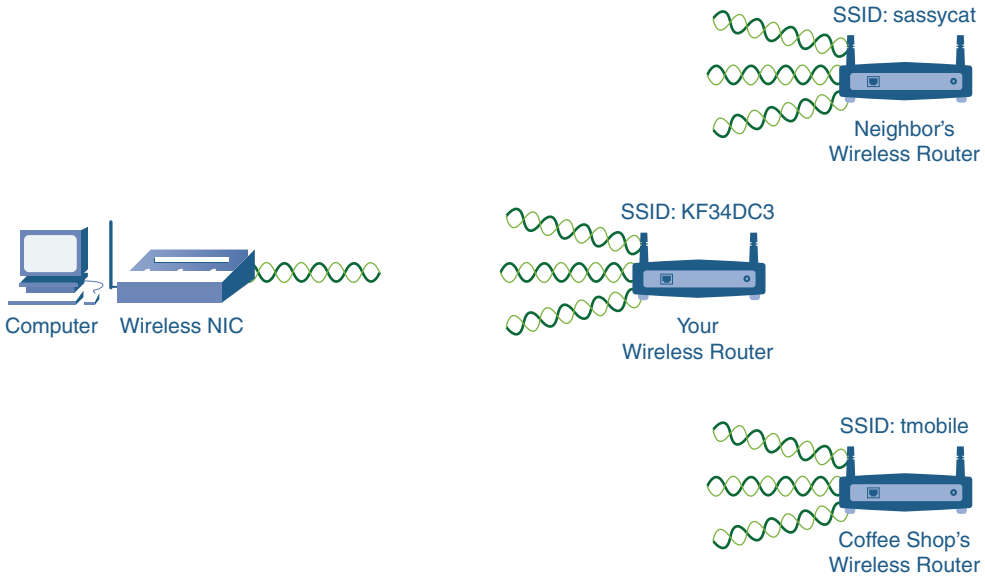
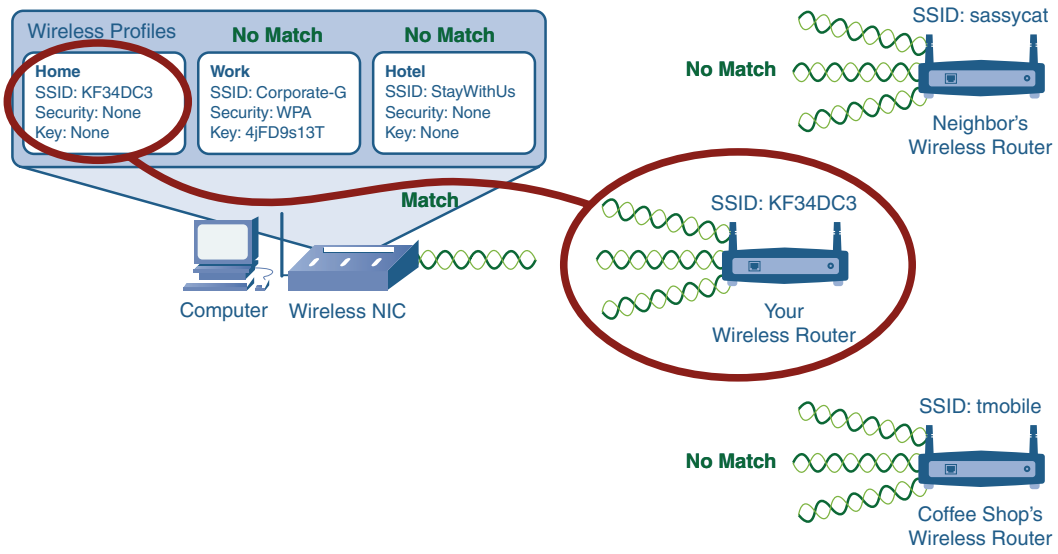


Figure 8-9 Matching Wireless Profiles to Available Wireless Networks



In this example, the wireless NIC scans for signals (much like a cell phone scans for cellular towers) and detects three wireless signals with SSIDs: sassycat, KF34DC3, and tmobile. The wireless NIC matches the profile for the Home network to the wireless router advertising the same SSID and then tries to associate to it.

Associating is kind of like seeing someone who looks familiar at a party. From a distance it looks like Ned Flanders. So you walk over to take a closer look and say, "Aren't you Ned Flanders? Didn't we go to high school together?" Ned answers, "Yes, of course," and you have a lengthy conversation about the good old days…'65 Mustangs, Def Leppard, blonde girls who feathered their hair like Farrah Fawcett. Ah, let's pause a moment to reminisce.

Wireless association is very similar. The wireless NIC sees a signal that has the same SSID as one in its set of profiles. It attempts to associate by starting a conversation with the wireless router, sending certain signals to let the router know the NIC is there and wants to communicate. The wireless router may grant access or may not. In addition to the SSID, if wireless security is enabled, those parameters must match also (including type of encryption, encryption key, and so on). We will cover more on wireless security in Chapter 9.

If the wireless router grants access, it then typically assigns the NIC an IP address to use on the wireless network, at which point we can begin exchanging data. If it denies access for some reason (maybe we are not speaking the same wireless security language or are not authorized to use that wireless signal), the association fails and we must keep trying other wireless router signals until we find one to associate with.

Wireless Connection Managers

Wireless connection managers are programs that let you manage the wireless profiles in your computer, and which one you are currently connected to. If you use your computer only at home, such as a desktop PC or some other device that does not leave your home, you will typically use the wireless connection manager when you first set up your wireless network, and maybe again if you make changes. In this case you will likely also have only a single wireless profile: your home network.

If you own a laptop, chances are you will have several wireless profiles, including your home wireless network and several other profiles for traveling. Chapter 14, "Wireless to Go," covers how to use wireless outside your home.

There are several types of wireless connection managers, including

- Windows Wireless Network Connection utility
- Linksys WLAN Monitor utility
- Other programs such as Boingo

In this chapter we show the Windows Wireless Network Connection utility and the Linksys WLAN Monitor utility. We cover other programs such as Boingo in Chapter 14.

Starting with Windows XP and continuing with Vista (also available via patch updates for Windows 2000), it is possible to manage wireless connections within Windows, and not require an add-on program. This is the long-term direction for wireless NIC management: letting Windows manage the devices just like most other devices in the PC or laptop.

If managing your wireless NIC using Windows is supported, it is probably the best option. For those NICs that you cannot manage with Windows, you need an add-on program from the NIC manufacturer. These cases include

- NICs that use a very new wireless standard or type of wireless security that is not yet supported by Windows
- Wireless NICs from manufacturers that force you to use their specific software

Reference the documentation that comes with the wireless NIC you purchase to see if Windows can be used to manage the NIC or if you must install a program provided by the manufacturer. We expect the vast majority of wireless NICs will use Windows for wireless connection management.

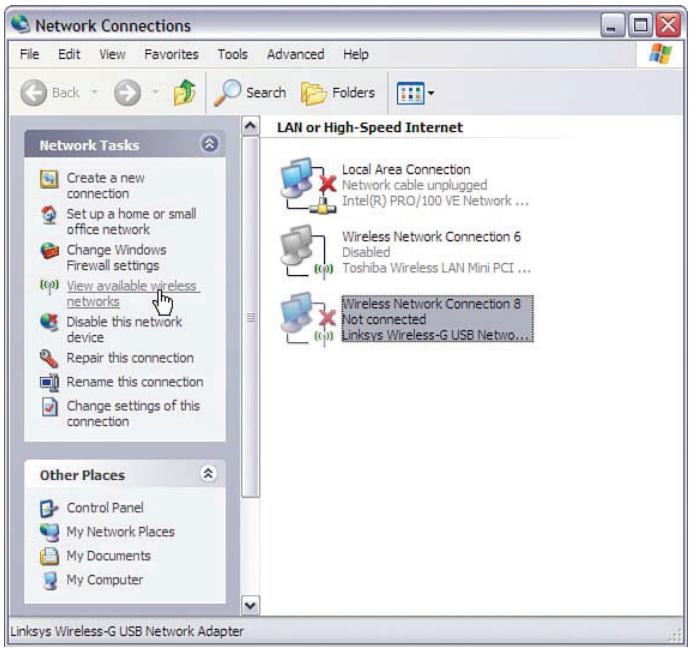
As a final note, you typically use either the Windows Wireless Network Connection utility or a manufacturer's utility, such as Linksys WLAN Monitor, and not both. Most commonly, the two options are mutually exclusive, meaning you cannot use both at the same time.

Using the Windows Wireless Network Connection Utility

Let's look at an example of using the built-in wireless connection manager functionality of Windows XP to manage the USB wireless NIC we installed earlier (Linksys WUSB54G). The steps to associate the NIC to the wireless router are as follows:

Step 1 Choose **Start > Connect To > Show All Connections**. Select the USB wireless NIC on the right side of the dialog box and then click **View Available Wireless Networks** on the left side. (See Figure 8-10.)

Figure 8-10 Locate the Wireless NIC

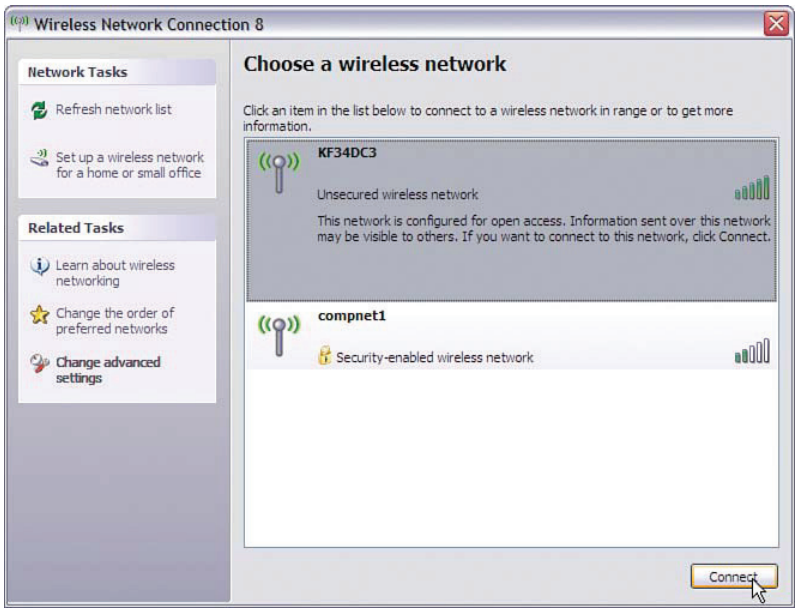


Step 2 You will see a list of available wireless network signals, as shown in Figure 8-11. If you do not, try clicking **Refresh Network List**. Locate your wireless network in the list. The SSID you chose should be displayed (in our example we used KF34DC3). Select it and click **Connect**.



Note: If your wireless NIC is managed using a manufacturer's proprietary utility, such as Linksys WLAN Monitor, and you attempt to use the Windows Wireless Network Connection utility, you will see a message such as "Windows cannot configure this wireless connection." In that case, you need to use the manufacturer's utility or disable that utility and let Windows manage the NIC before proceeding.

Figure 8-11 Connect to the Wireless Router



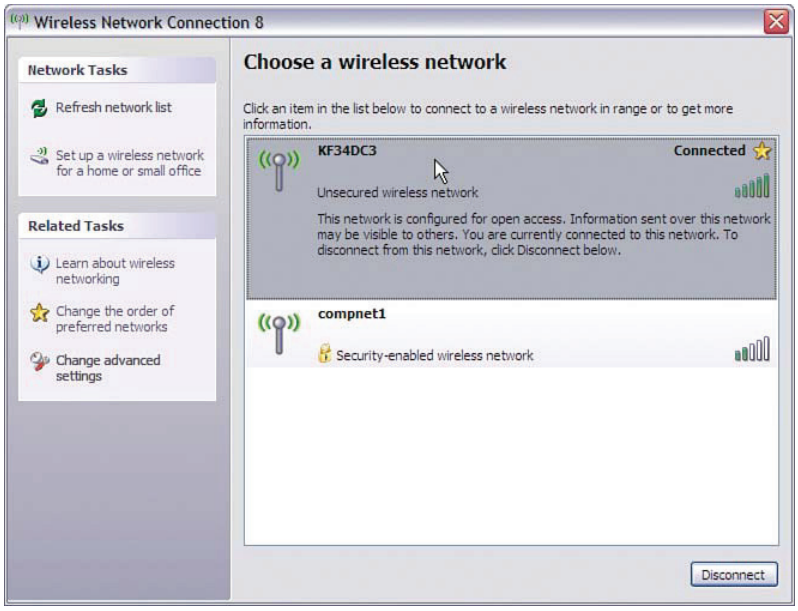
Step 3 You may be prompted that you are connecting to an unsecured wireless network, as shown in Figure 8-12. This is because we have not enabled wireless security yet (which we do not recommend doing yet, but we will do it in Chapter 9). Click **Connect Anyway**.

Figure 8-12 Confirm Connection to an Unsecured Wireless Network



Step 4 The NIC will associate to the wireless router. The status will change to Connected in the dialog box to view available wireless networks, as shown in Figure 8-13.

Figure 8-13 Connected to Wireless Network



You can test the connection by trying to browse the Internet. Launch your web browser (such as Internet Explorer) and see if you can browse a web page.

Using Linksys WLAN Monitor

Now let's look at an example of using the Linksys WLAN Monitor program to manage the PCMCIA wireless NIC we installed earlier (Linksys WPC54G). The steps to associate the NIC to the wireless router are as follows:

Step 1 Launch the WLAN Monitor utility by double-clicking the icon on the running tasks taskbar (lower right of your screen) or choose **Start > Linksys Wireless Card > WLAN Monitor** and then click **Site Survey**. Locate your wireless network in the list (see Figure 8-14). The SSID you chose should be displayed (in our example we used KF34DC3). Select it and click **Connect**.

Step 2 Click the **Link Information** tab. If the wireless NIC connects properly to the wireless router, you will see green bars in the Signal Strength and Signal Quality boxes on the dialog box, as shown in Figure 8-15. Strength in this case measures the power your NIC is sensing, and quality is a measure of the speed (data rate) you are getting as compared to the maximum amount possible.

Figure 8-14 Perform a Site Survey and Connect

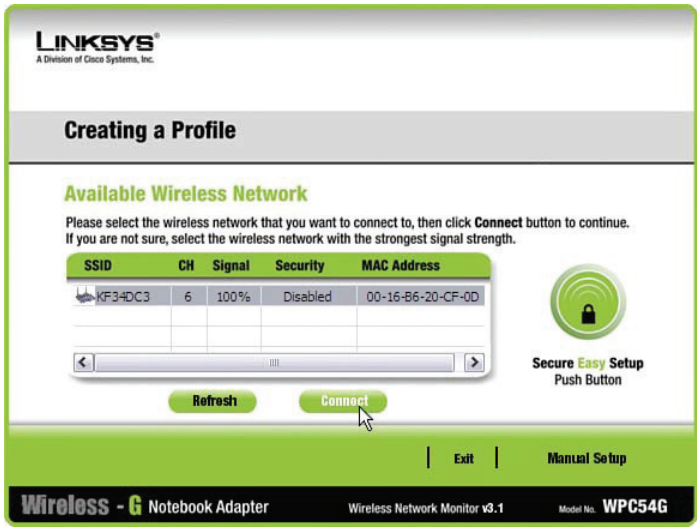
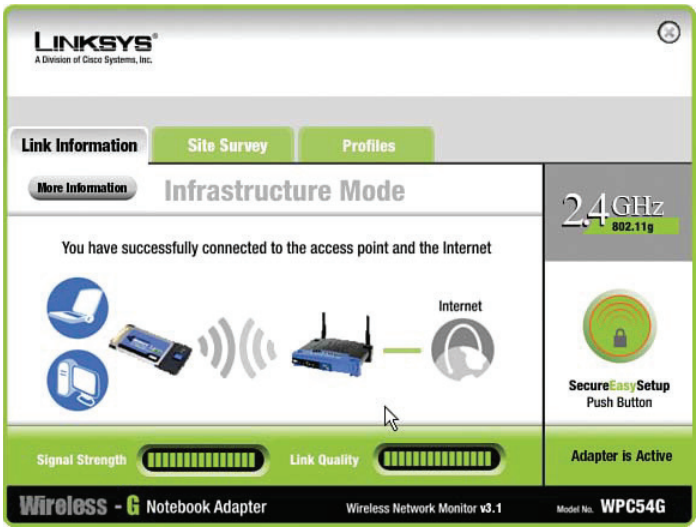


Figure 8-15 Verify Connection to the Wireless Router



Step 3 Click **More Information**. You will see the status information for the wireless network and a display of the wireless parameters, including the SSID, security, and so on, as shown in Figure 8-16. Click **Save to Profile**. Remember that the name of the profile can be (and probably should be) different from your SSID name.

Step 4 You are prompted for a name for the wireless profile, as shown in Figure 8-17. Enter a descriptive name (we chose "home network" for this example). Click **OK**.

Figure 8-16 Save the Connection as a Wireless Profile

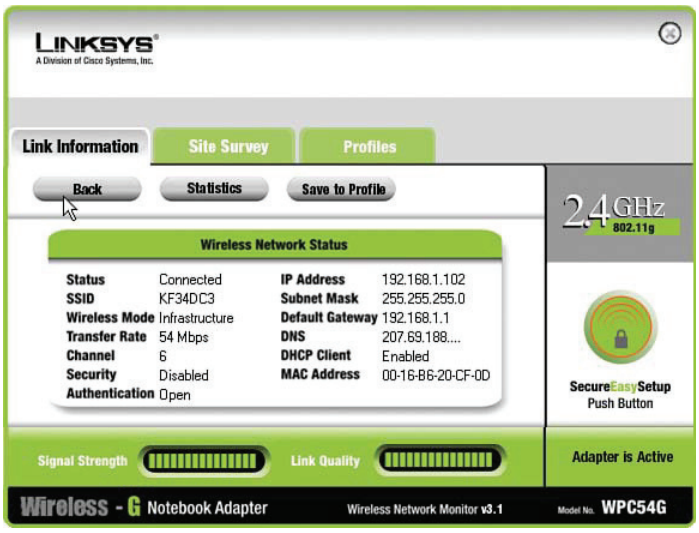
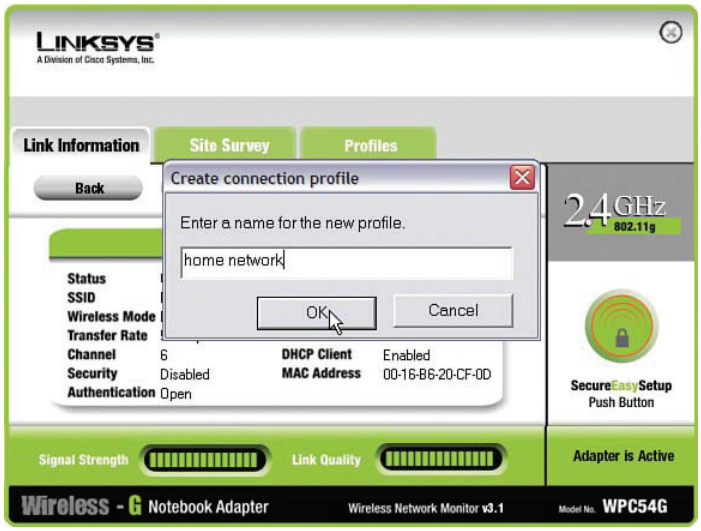


Figure 8-17 Assign a Name to the Wireless Profile



You can test the connection by trying to browse the Internet. Launch your web browser (such as Internet Explorer) and see if you can browse a web page.

Using Linksys EasyLink Advisor

As discussed in Chapter 7 on setting up the wireless router, there is a new software setup utility for Linksys routers (under development at the time this book was written) named EasyLink Advisor. EasyLink provides a simplified way to set up wireless routers.

EasyLink can also aid in the setup of wireless NICs. Before starting, you need a USB memory stick. If the computer is running Windows XP, we can use EasyLink to create a wireless profile on a USB memory stick, and then simply plug that USB memory stick into the computer we want to add,

automatically creating the wireless profile. As you'll see later in this section, several steps are involved, but they are all straightforward.



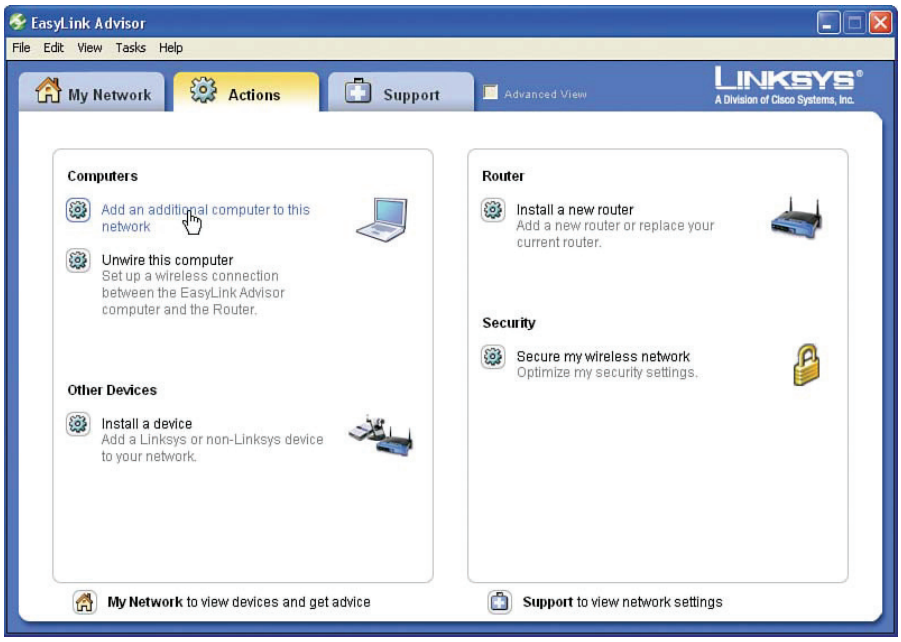
Note: At the time this book was written, using a USB memory key to add a computer to a wireless network using EasyLink Advisor only works for computers running Windows XP and higher, and only when using the Windows Wireless Network Connection utility to manage wireless NICs. It does not work if a separate program utility is required to manage wireless NICs, including the Linksys WLAN Monitor program or other manufacturers' wireless connection manager programs.

If you are using an older version of Windows (for example, Windows 2000 or 98SE), the EasyLink program helps you print out the wireless profile data you need. Then you have to use the printout to manually set up your wireless NIC using a wireless connection manager program, like the example shown in the preceding section for the Linksys WLAN Monitor program.

The following example uses a Linksys WRT54G wireless router and two computers with wireless NICs, both running Windows XP:

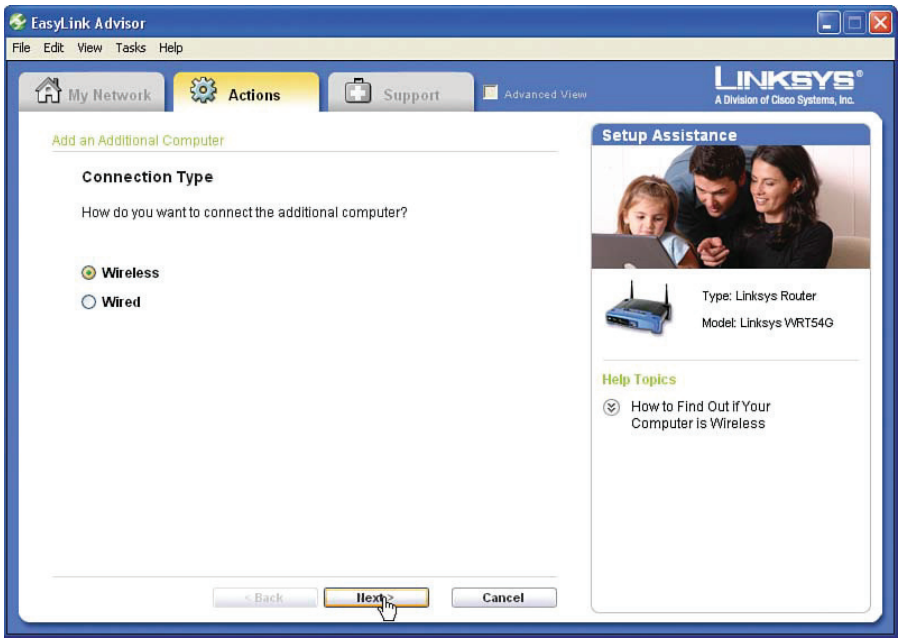
Step 1 On the computer with Linksys EasyLink Advisor installed, launch the EasyLink Advisor program by double-clicking the icon on the running tasks taskbar or by choosing **Start > Programs > Linksys EasyLink Advisor**. Click the **Actions** tab and then click **Add an Additional Computer to This Network**, as shown in Figure 8-18.

Figure 8-18 Adding a Computer with Linksys EasyLink Advisor



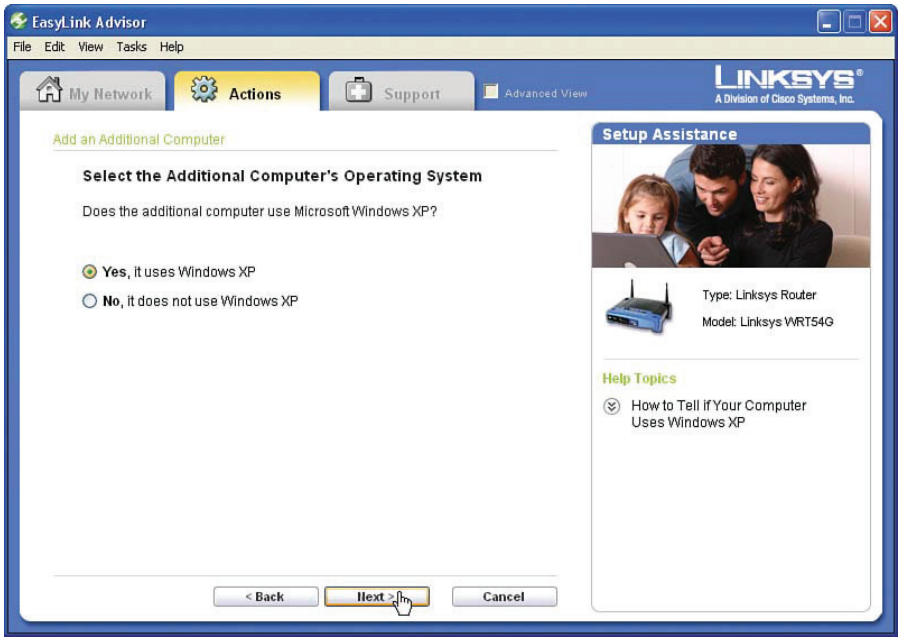
Step 2 Select **Wireless**, as shown in Figure 8-19. Click **Next**.

Figure 8-19 Select Wireless to Add a Wireless-Connected Computer



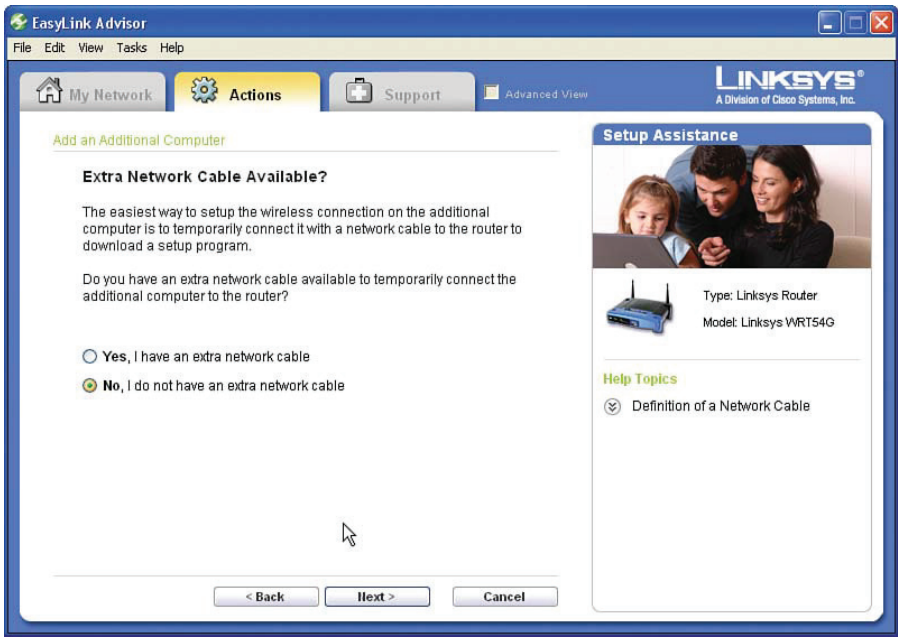
Step 3 If you are using at least Windows XP or higher, select **Yes, It Uses Windows XP**, as shown in Figure 8-20. Click **Next**.

Figure 8-20 Verify It Is a Windows XP Computer



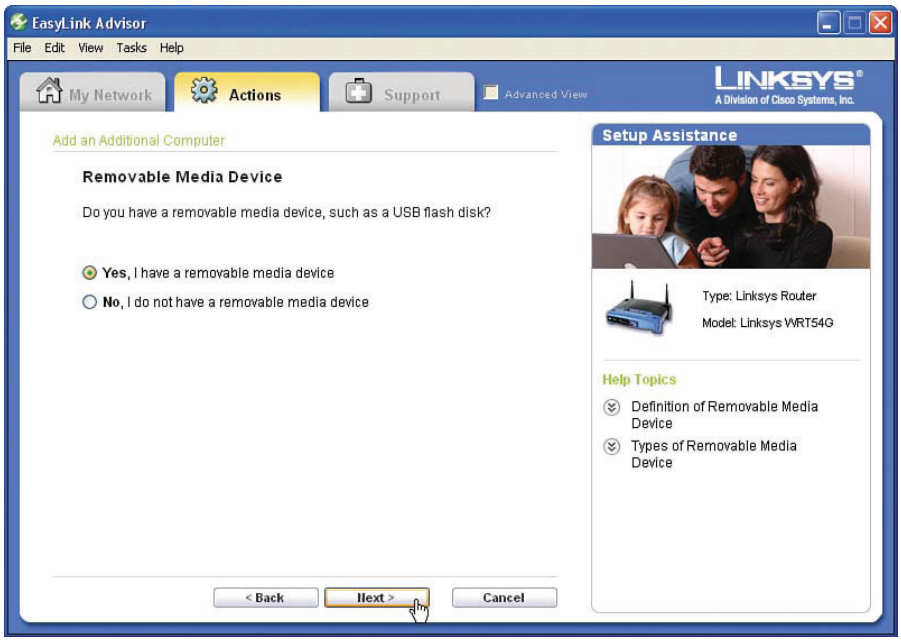
Step 4 EasyLink asks if you want to set up the computer with a network cable, as shown in Figure 8-21. Click **No, I Do Not Have an Extra Network Cable** and then click **Next**.

Figure 8-21 Bypass the Network Cable Setup



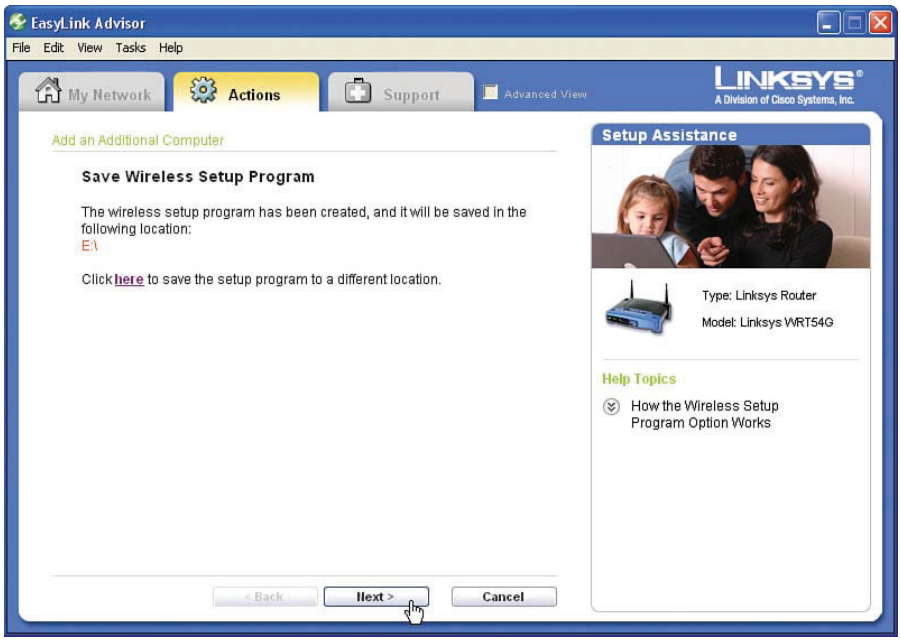
Step 5 Click **Yes, I Have a Removable Media Device**, as shown in Figure 8-22. Plug a USB memory stick into an open USB port on the computer running EasyLink and click **Next**.

Figure 8-22 Choose to Set Up Using a Removable USB Memory Key



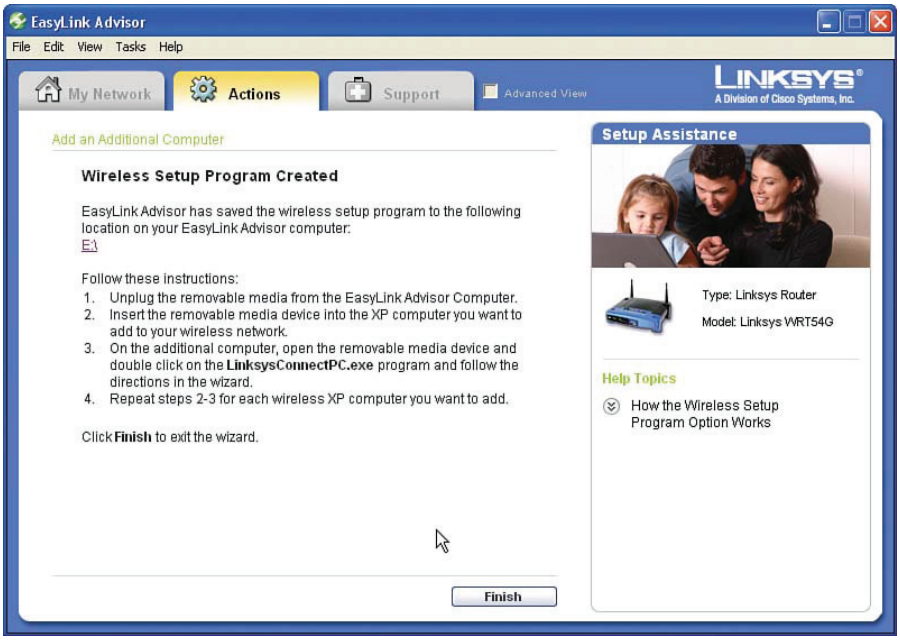
Step 6 EasyLink confirms the location you want to save the wireless profile to (on the USB memory key, in this example E:/), as shown in Figure 8-23. Confirm that EasyLink has the right location and then click **Next**.

Figure 8-23 Confirm the Save Location on the USB Memory Key



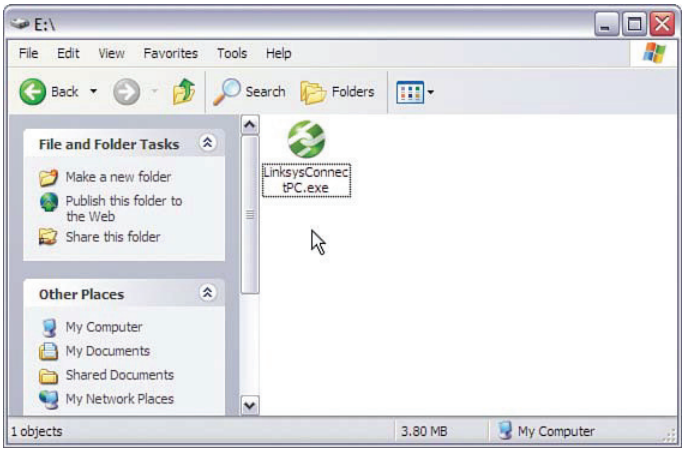
Step 7 EasyLink saves a program file to the USB memory key, as shown in Figure 8-24.

Figure 8-24 Wireless Profile Program Saved on the USB Memory Key



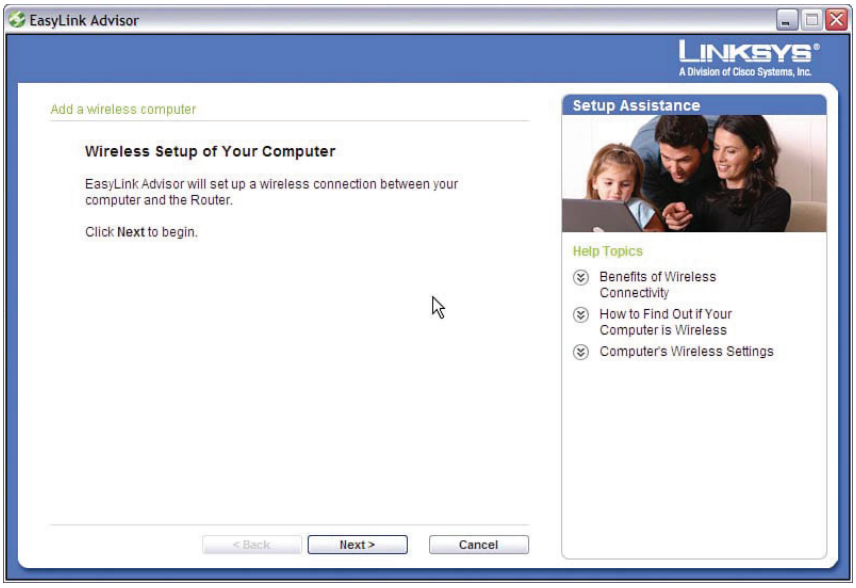
Step 8 Remove the USB memory key and take it to the computer you want to add to your wireless network. Plug in the USB memory key to an open USB port. Double-click **My Computer** and then double-click the USB memory key "drive" (E:/ in this example). You will see a program on the USB memory key named LinksysConnectPC.exe, as shown in Figure 8-25. Double-click the program icon to launch the program.

Figure 8-25 Launch the Wireless Profile Creator Program on the USB Memory Key



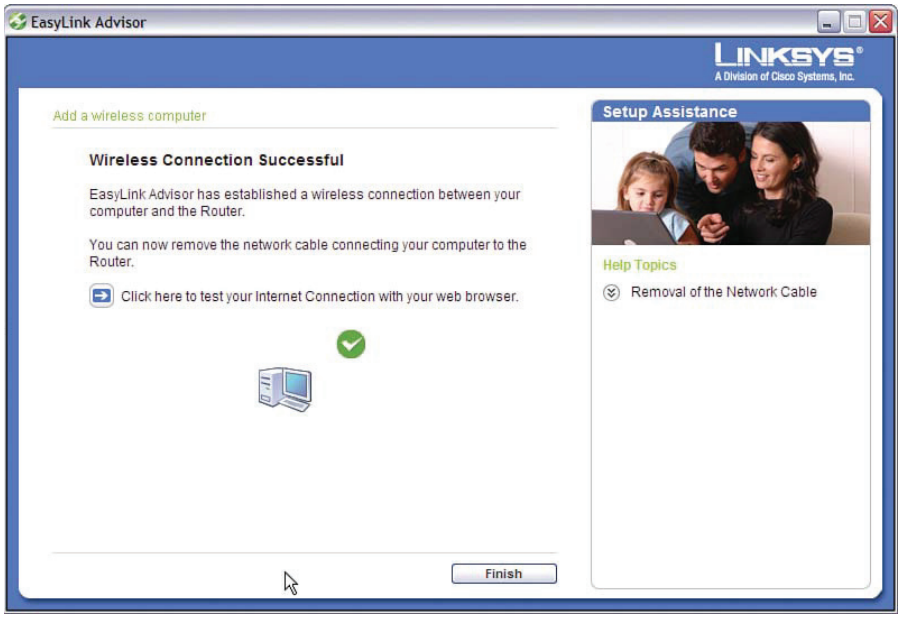
Step 9 A very small version of the Linksys EasyLink Advisor program starts executing on the computer you are adding to the wireless network, as shown in Figure 8-26. Click **Next**.

Figure 8-26 Linksys EasyLink Advisor Wireless Profile Creator Utility Launches



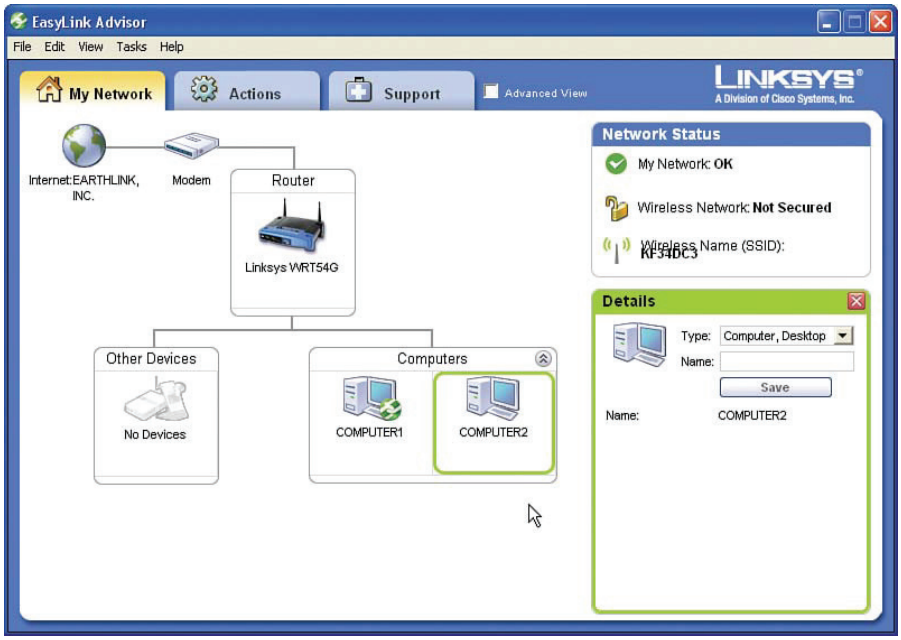
Step 10 As shown in Figure 8-27, the program creates a wireless profile using the wireless network information from the wireless router (that it has stored on the USB memory key). Click **Finish**.

Figure 8-27 Wireless Profile Created



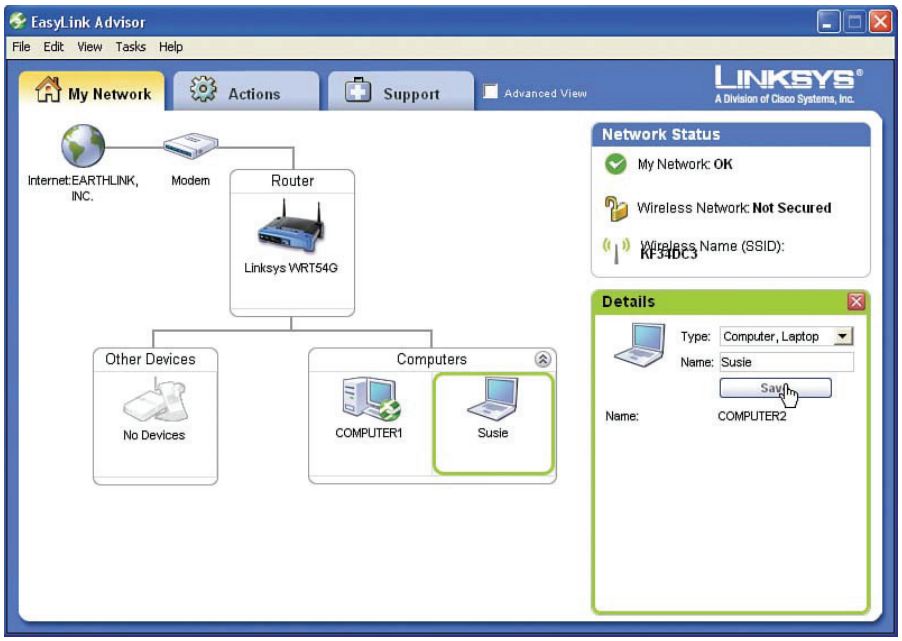
Step 11 Go back to the computer where the (main) EasyLink Advisor program is installed and see if the router now "sees" the computer we just added. Click the **My Network** tab. As shown in Figure 8-28, you can now see graphically that two computers are now connected to the wireless router: Computer1, which is the wired computer we used in Chapter 7 to set up the wireless router, and Computer2, which is the computer we just added to the wireless network.

Figure 8-28 Newly Added Computer Appears in the Network Diagram



Step 12 If desired we can set the type of computer (Laptop in this example) and even assign a name so we know which computer it is (Susie in this example). As shown in Figure 8-29, set the type and name and then click **Save**. This does not change the computer's own name; it simply gives it an alias that EasyLink Advisor remembers.

Figure 8-29 Assign a Type and Name to the Added Computer



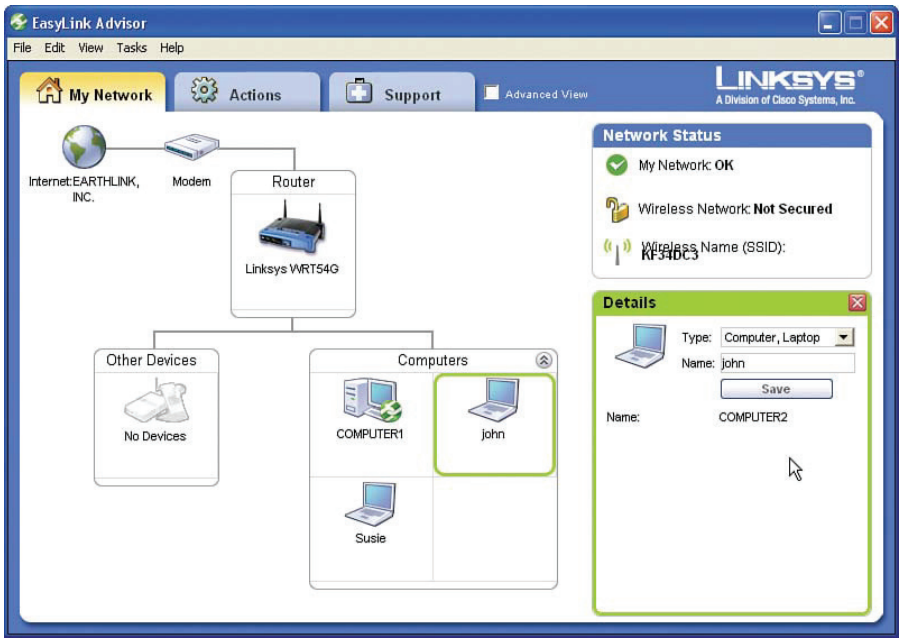
Step 13 Take the same USB memory key to additional computers (running Windows XP) and add them as well. Just repeat Steps 8 through 12 for each computer you want to add. For this example we added a third computer, as shown in Figure 8-30.

Note: The USB memory key you created is valid until you change any of the settings on your wireless network. We recommend keeping it handy (hang it on the side of your refrigerator or some other easily accessible place). When you have a guest staying at your home who wants to connect to your wireless network, you can hand them the USB memory key and walk them through creating a wireless profile on their Windows laptop.

At this point the wireless profile should be created and your wireless NIC should associate with your wireless router. Just like in the other examples, start your Internet browser and see if you can now browse a web page.

As you can see, EasyLink Advisor provides a fairly easy way to add computers to your home wireless network. In Chapter 9 we will see how to turn on wireless security with EasyLink Advisor.

Figure 8-30 Third Computer Added Now Appears



Summary

The two major steps to setting up a wireless NIC in your computers are installing the NIC itself (assuming one is not already built in to your computer or laptop) and creating a wireless profile so that the NIC can associate to your wireless router.

You can manage the wireless connections on your computers in one of a few different ways, including using the Windows Wireless Network Connection utility or using a separate program utility provided by the NIC manufacturer, such as the Linksys WLAN Monitor program. Use the Windows Wireless Network Connection utility unless the NIC requires its own program for some reason (see the installation documentation that comes with the NIC).

Managing wireless connections and adding new wireless profiles with Windows XP is pretty easy.

If you are using the Linksys EasyLink Advisor program to manage your wireless router, there is also a very nice way to set up your wireless profiles by using a USB memory key to propagate the wireless network information to each of your computers. As Linksys evolves this program, it will no doubt provide more extensive capabilities for easy management of your wireless computers.

We intentionally separated out information on troubleshooting into a separate section of this book. If you run into trouble at any point, seek out the troubleshooting chapters in Part IV.

Where to Go for More Information

For more information about the Windows Wireless Network Connection utility, visit the Microsoft website and view the article "Set Up a Wireless Network": www.microsoft.com/windowsxp/using/networking/setup/wireless.mspx.

For more information about Linksys EasyLink Advisor, go to the Linksys main website: www.linksys.com.

Also check out Bradley Mitchell's article on About.com titled "Networking with a Router: Using a Router on Broadband and/or Wireless Home Networks": http://compnetworking.about.com/od/homenetworking/a/routernetworks.htm.

CHAPTER 9

Wireless Security Setup

With the wireless router set up and all the computers now communicating with it, it is time to turn our attention to securing the wireless network.



Note: The starting assumption is that you have already been successful in setting up the home wireless network without security in Chapters 7, "Wireless Router Setup," and 8, "Wireless NIC Setup." If not, stop and do that first. Turning security on in a wireless network that is already having issues is only going to increase the problem, not solve it.

As discussed in Chapter 5, "Wireless Security: What You Need to Know," wireless networks have no security enabled when you buy the router and NICs. This is necessary because the wireless router and NICs have to be set up with the same security information (that you choose) to communicate with each other. For the reasons discussed in Chapter 5, it's very important to take the few extra steps that are necessary to properly secure your wireless network. The steps are pretty easy:

- Enable encryption (either WEP or WPA) between the wireless router and wireless NICs.
- Disable SSID broadcast on the wireless router.
- Prevent unintentional roaming on all wireless NICs.
- Turn on the firewall on the wireless router (applies to any router, wireless or otherwise).
- Change the wireless router's administration password (applies to any router, wireless or otherwise).

This chapter shows how to set up wireless security.

Setting Up Wireless Encryption

The first (and most important) step to securing your home network is to turn on encryption between the wireless router and the computers in your home network. In order for the computers on your home network to communicate with the wireless router, both sides of the wireless connection (wireless router and wireless NICs) must be using the same type of encryption and the same encryption key.

Figure 9-1 shows what the security options look like before and after.

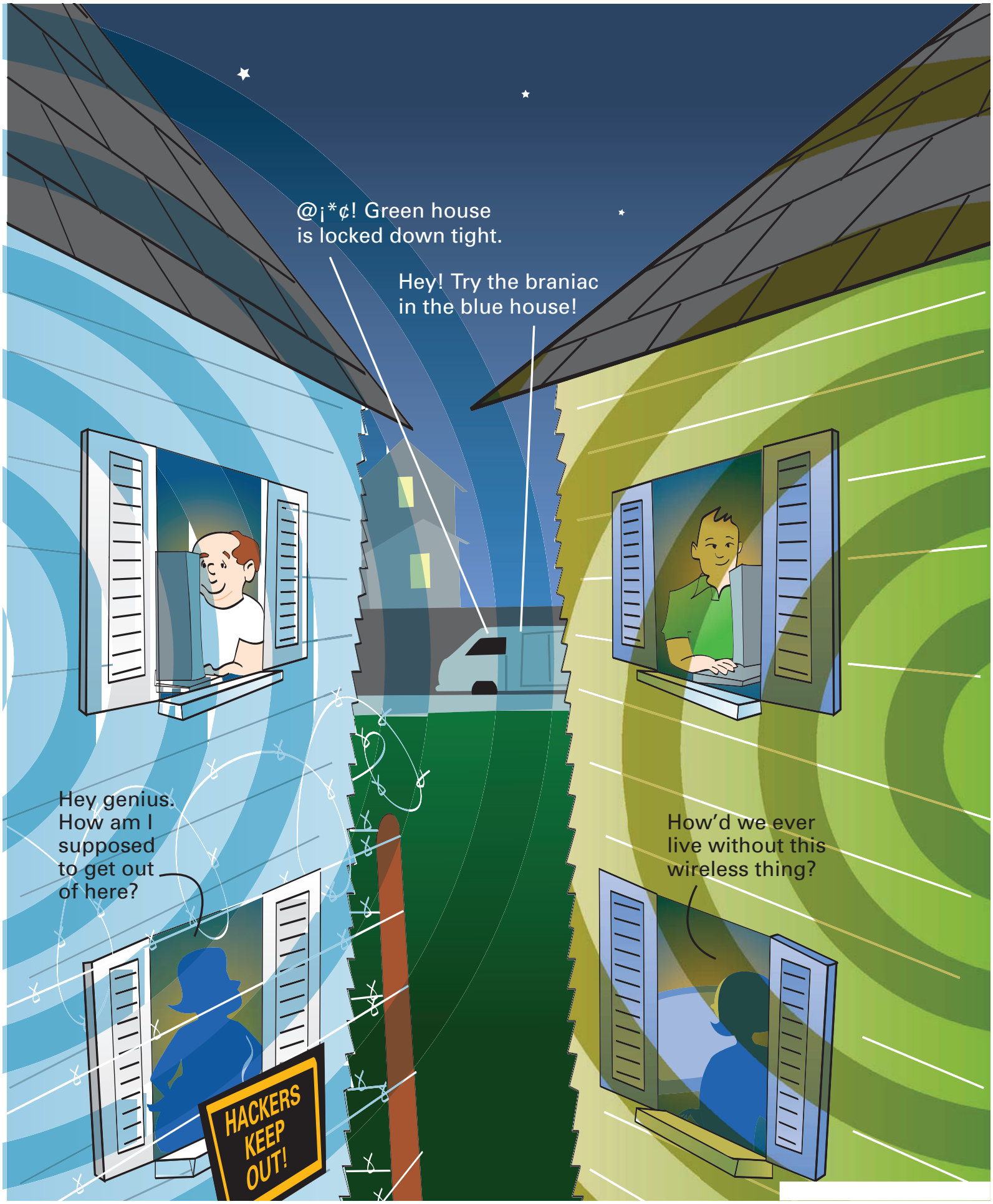
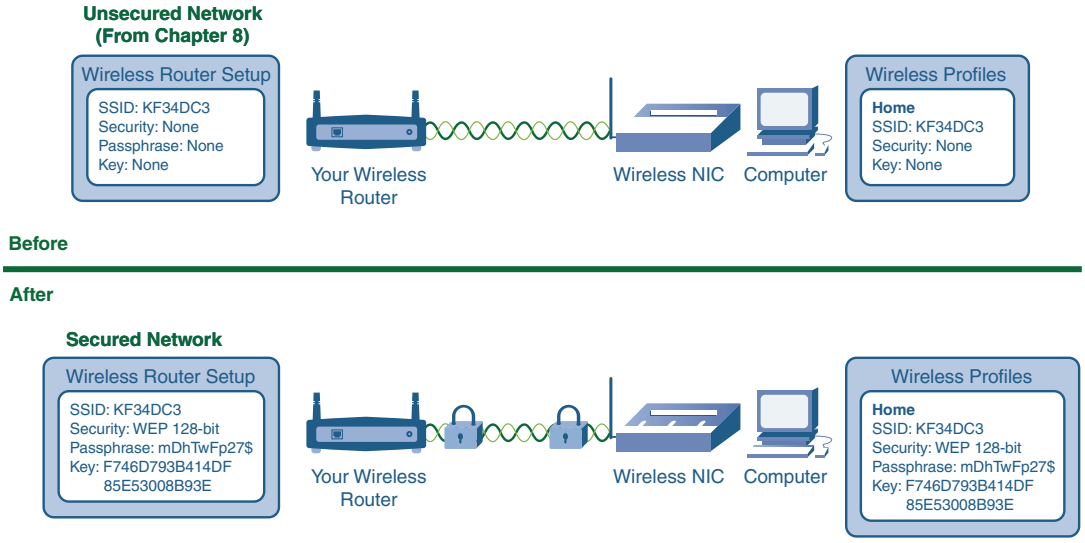

@¡*¢! Green house is locked down tight.
Hey! Try the braniac in the blue house!
Hey genius. How am I supposed to get out of here?
How'd we ever live without this wireless thing?
HACKERS KEEP OUT!

Figure 9-1 Adding Encryption to a Home Wireless Network



First, we will turn on encryption and assign security key information that is unique to our home wireless network. Then, we will "teach" each wireless NIC in each computer how to "speak" the same security language as the wireless router. The security information will be added to the wireless profile for the home network, including both the type (WEP or WPA) and the unique encryption key.

Tips Before We Start

Before we start turning on wireless encryption, there are a few important things to understand and a couple of tips to follow.

First, understand the difference between some of the terminology that will be used in this chapter:

- **WEP key**—26-character key code (assuming 128-bit WEP) consisting of the characters 0–9 and A–F, which is the actual encryption key. All wireless routers and NICs that support WEP use a WEP key
- **WEP passphrase**—8- to 16-character passphrase, like a password, consisting of upper- and lowercase letters, numbers, and special characters. Linksys wireless routers and NICs can use a passphrase to generate a WEP key for you. The Linksys passphrase is not supported on non-Linksys routers and NICs. If you mix vendor equipment (for example, if you have a NETGEAR router and a Linksys NIC), you need to manually type in the WEP key.
- **WPA preshared key (PSK)**—8- to 63-character key, like a long password, consisting of upper- and lowercase letters, numbers, and special characters. All wireless routers and NICs that support WPA use a WPA PSK.

If you are using WEP as your encryption for security, you can either create your own lengthy 26-digit key (assuming 128-bit WEP) or create a passphrase and ask the Linksys wireless router to generate a WEP key for you. In the latter case, any Linksys NICs can also use the same passphrase to generate the WEP key.

If you are using WPA as your encryption for security, you will create an 8- to 63-character key that you will "share" with both the wireless router and NICs.



Note: Your network can support only one type of encryption, so make sure the router and all the NICs are using the same type of encryption. If you use WPA and one of your computers has an older NIC (one that only has WEP), that computer will not be able to access your wireless network.

You might find enabling encryption on the wireless NICs a little confusing right now, because it depends on the type of NIC and whether it is being managed with the Windows Wireless Network Connection utility or with its own program such as the Linksys WLAN Monitor. The next few sections walk through different types of setups.

Regardless of the type, there are a several tips that are critical to remember:

Tip 1 Write it down. Keep a notebook and write down the SSID, the type of encryption (WEP, WPA, WPA2), the WEP passphrase and key, or the WPA PSK. Keep the notebook in a locked drawer or cabinet.

Tip 2 Keep your terms straight. Understand whether you are using a WEP key, a WEP passphrase, or a WPA PSK. Write them down that way in the notebook. Avoid labeling them as "wireless security key" or other terms that are too general.

Tip 3 Case can be important. Whether you are using upper- or lowercase letters matters *a lot* for a WEP passphrase and for a WPA PSK. Case does not matter for a WEP key itself.

Tip 4 If you cannot get it working, turn wireless security off on the wireless router and NICs and start over.

If Only It Were That Easy

How you enable wireless encryption on your wireless home network will depend on how you set up your network in Chapters 7 and 8 earlier. If you set up your wireless router using either the Internet browser method or using the Linksys Setup Wizard, you will use your Internet browser to set up wireless security. (See the following section, "Manually Setting Up Wireless Encryption.")

One exception would be if your Linksys wireless router and Linksys wireless NICs support Linksys SecureEasySetup. SecureEasySetup provides a push-button way to enable wireless security (see "Setting Up Wireless Encryption with Linksys SecureEasySetup" later in this chapter).

If you set up your wireless router using Linksys EasyLink Advisor, you will also use EasyLink to set up wireless security (see "Setting up Wireless Encryption with Linksys EasyLink Advisor").

Confused? Yes, there are quite a few different options available. Table 9-1 simplifies the decision about which steps you need to take. Start with the left column and determine which method you are using to manage the wireless security settings on the wireless router: using an Internet browser (in other words, manual), using Linksys SecureEasySetup, or using Linksys EasyLink Advisor.

Table 9-1 Wireless Security Settings Setup Method Summary

	Linksys NICs Managed with Linksys Utility	Linksys NICs Managed with Windows	Other NICs Managed with Windows	Other NICs Managed with Other Utility
Linksys Wireless Router Using Internet Browser (Manual Setup)	Generate a key from WEP passphrase or enter WPA PSK	Enter WEP key or WPA PSK	Enter WEP key or WPA PSK	See the instructions that came with the NIC
Linksys Wireless Router Using SecureEasySetup (SES)	Push the SES button on the router and NIC	Enter WPA PSK generated by SES	Enter WPA PSK generated by SES	See the instructions that came with the NIC
Linksys Wireless Router Using EasyLink Advisor	Generate WEP key from passphrase or enter WPA PSK generated by EasyLink Advisor	Use a USB media key to transfer the EasyLink Advisor settings	Use a USB media key to transfer the EasyLink Advisor settings	See the instructions that came with the NIC

After you determine which method you are using, find the column to the right that matches how the wireless NIC you need to configure is managed. For Linksys NICs, as discussed in Chapter 8, you may be using Windows to manage them or using a Linksys software utility, such as WLAN Monitor. For non-Linksys NICs, such as one already built in to your laptop, see the "Other NICs" columns.

In general, this book will help with those other NICs managed using Windows. For non-Linksys NICs managed with a program that comes with the NIC, we can't give the details here due to space limitations, but the general approach is the same. The same goes for non-Linksys wireless routers: See the instructions that come with the equipment if you purchase non-Linksys routers or NICs.

Each of the cases shown in Table 9-1 in green are covered in the rest of this chapter.

Manually Setting Up Wireless Encryption

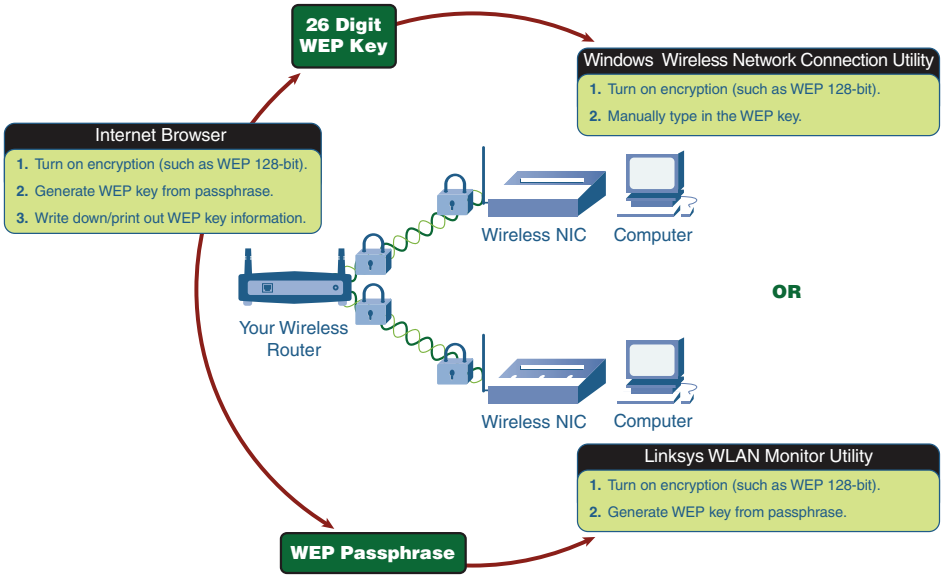
If you set up your wireless router in Chapter 7 using either the Internet browser method or the Linksys Setup Wizard, you will use your Internet browser to set up wireless security.

One exception would be if your Linksys wireless router and Linksys wireless NICs support Linksys SecureEasySetup. SecureEasySetup provides a push-button way to enable wireless security (see the section "Setting Up Wireless Encryption with Linksys SecureEasySetup" coming up).

To enable encryption manually, Figure 9-2 shows the steps we will go through.

Figure 9-2 Manually Setting Up Wireless Encryption

First, we will enable encryption on the wireless router. We will do this using an Internet browser to



connect to the router and generate an encryption key from a passphrase. How we enable encryption on the computers depends on what we are using to manage our wireless connections (Windows Wireless Network Connection utility, Linksys WLAN Monitor, and so on), as discussed in Chapter 8.



Note: You will want to do this step using a physical (wired) connection to your router. If you do this over a wireless link, you may be disconnected as soon as you enable the changes you are about to make.

We will show one example with the Linksys WAN Monitor utility, where we can simply enter the same WEP passphrase as the router and generate the encryption key. We will also show an example using Windows XP to manage the connection, in which case we need to enter the WEP encryption key manually, as Windows does not support the ability to generate the key from the passphrase. The first encryption example we show will be done using 128-bit WEP. The second will be shown using WPA.

Enabling WEP Encryption on the Wireless Router

First, let's take an example of implementing 128-bit WEP encryption. We will pick a passphrase of mDhTwFp27$.



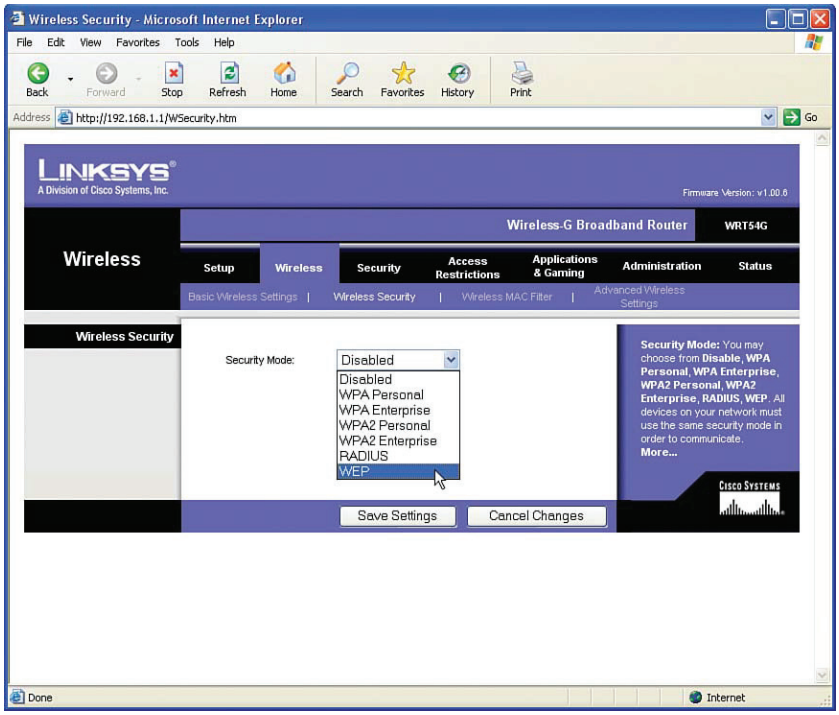
Note: When choosing a WEP passphrase or a WPA preshared key, you should use the same process as picking a password. Make it a strong password, not a weak one, using at least eight characters consisting of upper- and lowercase letters, numbers, and special characters. Avoid passphrases that spell something either literally or phonetically. For a more thorough discussion of strong passwords, pick up a copy of *Home Network Security Simplified*.

Now, let's program the wireless router to use this WEP key:

Step 1 Access the wireless router using your Internet browser. Click the **Wireless** tab.

Step 2 Click the **Wireless Security** subtab (see Figure 9-3). From the Security Mode field, choose **WEP**.

Figure 9-3 Select WEP as Your Security Mode

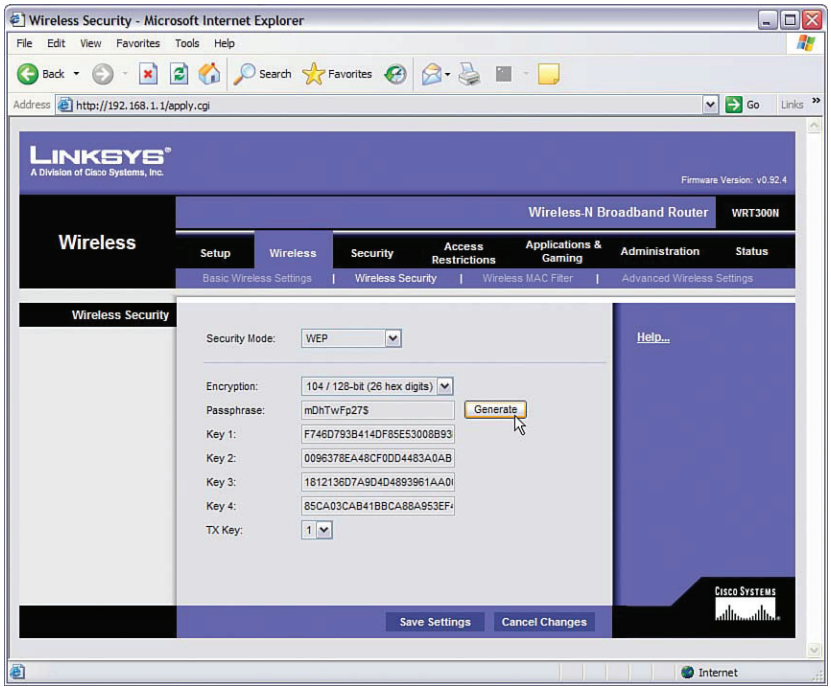


Step 3 On the line labeled WEP Encryption, select **128 bits**. In the Passphrase field, enter the passphrase you made up. In our example, we chose mDhTwFp27$ (see Figure 9-4). Click **Generate**. This translates the passphrase into the actual key to be used (F746D793B414DF85E53008B93E). Do not forget to write down the passphrase and the generated key.

Step 4 Click **Save Settings**.

Immediately after you click Save Settings, any computers that were connected with a wireless card to the wireless router will lose connectivity. This is normal, because you have just changed the way they are supposed to communicate with the wireless router, but you have not told them the super-secret password to use yet.

Figure 9-4 Generate the WEP Key





Note: You may notice that four keys are listed after you generate the WEP key. In general, you can choose any of the four keys, but most often you can just pick Key 1. The other three keys are just alternate keys that you can use if you want to keep the same passphrase but change the actual key. Regardless of which key you use, write the chosen key down in the notebook we suggested that you keep. Whenever you have visitors who want to use your network, they will need to enter either the passphrase or the key depending on whether or not they are using gear from the same manufacturer.

Enabling WEP Encryption on the Wireless NIC

As discussed in Chapter 8, there are a couple different ways to manage the wireless connection in each of your computers. Windows offers a built-in function for wireless NIC management. For computers with older versions of Windows (2000, 98SE, and so on), you most likely need to use a wireless management program that comes with the NIC. The same wireless connection manager you use to associate and set up wireless connections is used to also enable wireless security.

The sections that follow show two examples:

- A Windows XP laptop computer with a PCMCIA wireless card that we set up with the Linksys WLAN utility
- A Windows XP laptop with a built-in wireless NIC that we set up using the Windows Wireless Network Connection utility

Enabling WEP Encryption Using the Linksys Utility

First, let's walk through an example of setting up WEP encryption on a computer running Windows XP, using a PCMCIA wireless NIC (Linksys WPC54G) and the Linksys WLAN utility:

Step 1 Launch the Linksys WLAN Monitor by double-clicking the icon on the far right of your Windows taskbar (the example shows a computer running Windows XP). If you do not see such an icon, try going through **Start > Programs > Linksys Wireless Card > WLAN Monitor**.

Step 2 Notice that there is no connection to the wireless router (the signal bars are not "lit up"). This is normal since we enabled encryption on the wireless router but have not yet enabled it on the wireless NIC. (See Figure 9-5.)

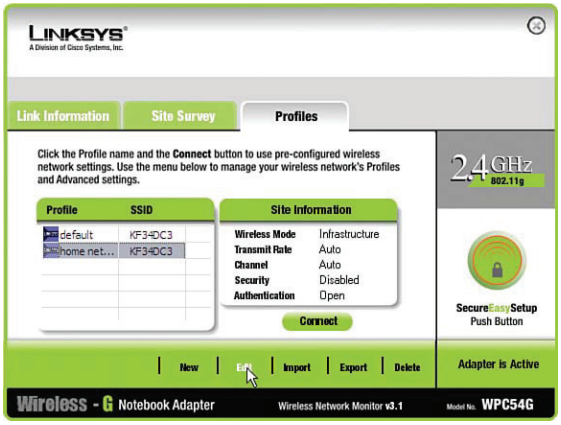
Step 3 Click the **Profiles** tab.

Figure 9-5 Launch the WLAN Monitor Utility



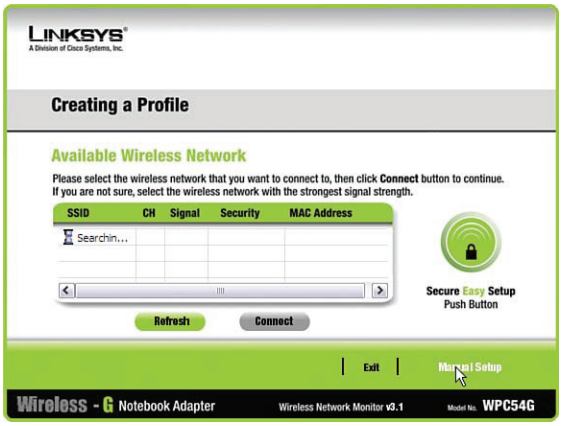
Step 4 Select the profile for your home wireless network and click **Edit** (see Figure 9-6).

Figure 9-6 Select and Edit the Wireless Profile



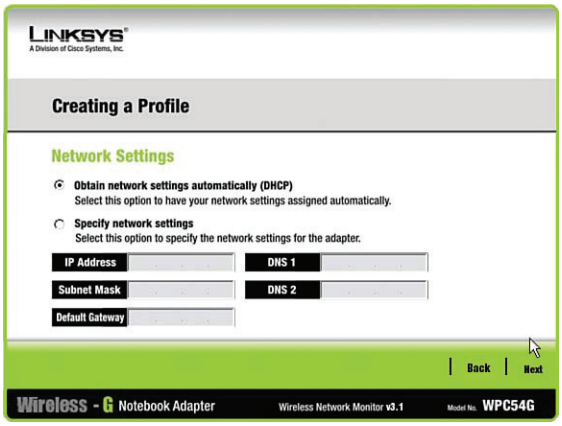
Step 5 Click **Manual Setup** (see Figure 9-7).

Figure 9-7 Click Manual Setup



Step 6 No changes are needed to the network settings (see Figure 9-8). Click **Next**.

Figure 9-8 Network Settings Stay the Same



Step 7 No changes are needed to the wireless mode either (see Figure 9-9). It should be set to Infrastructure Mode and have the SSID we set in Chapter 8. Click **Next**.

Step 8 The Wireless Security window appears (see Figure 9-10). Choose **WEP** and click **Next**.



Note: You will see several options in the Security drop-down list, including WPA-Enterprise, RADIUS, and LEAP. These are options for corporate networks, not home networks, so just ignore them.

Figure 9-9 Wireless Mode Stays the Same

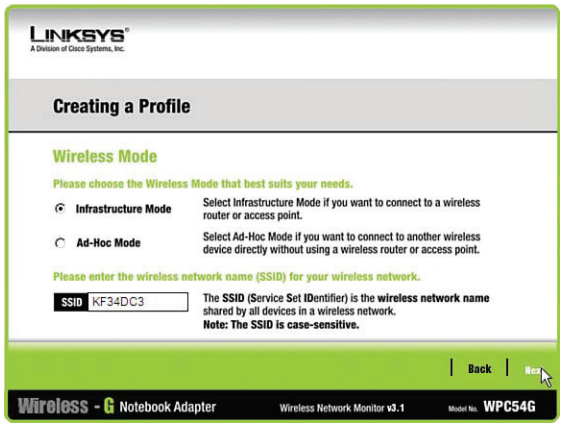
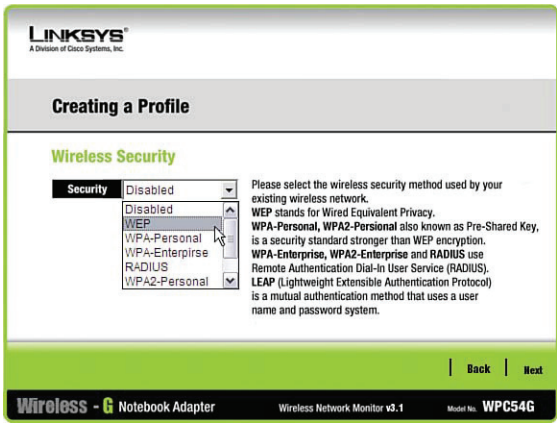
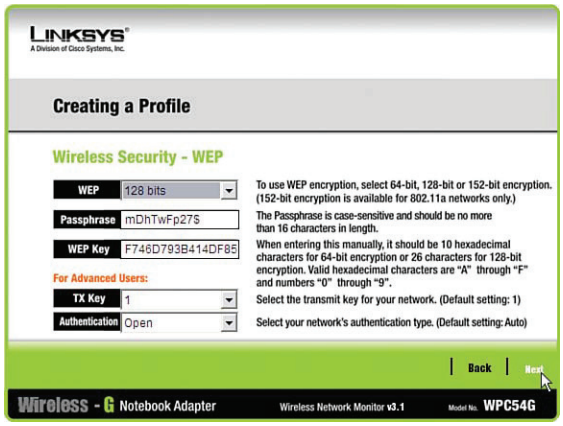


Figure 9-10 Choose WEP as the Security Type



Step 9 A second Wireless Security settings window appears (see Figure 9-11). From the WEP field, choose **128 Bits**.

Figure 9-11 Enter the WEP Key



Step 10 In the Passphrase field (also shown in Figure 9-11), enter the passphrase exactly as you entered it earlier when you enabled WEP on the router (mDhTwFp27$ for this example). You will see the WEP key being built as you enter the passphrase. After you enter the complete passphrase, click **Next**.

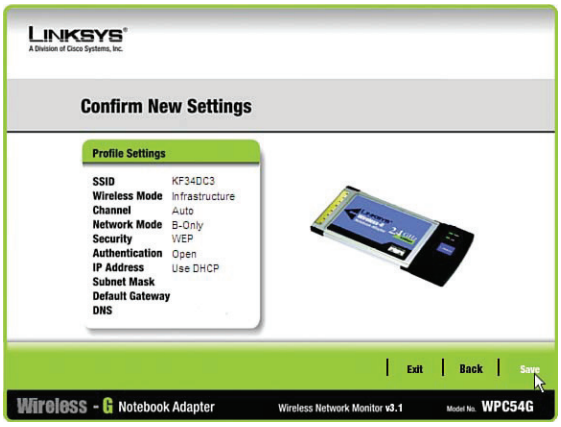


Note: Make sure to enter the passphrase exactly as you did on the wireless router. Lowercase *a* is different from uppercase *A*. The two keys (on the router and on the wireless card) must be identical. If the passphrases on the router and the NIC do not match, then the computer and the router will not be able to communicate.

Also, remember that when you use a passphrase, the first key (of the four created) is the one that will be used by default.

Step 11 A confirmation window appears (see Figure 9-12). Double-check the new security settings and click **Save**.

Figure 9-12 Confirm the New Settings



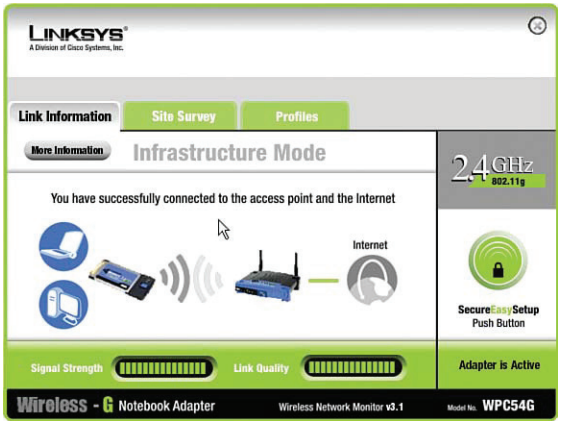
Step 12 A Congratulations window appears (see Figure 9-13). Click **Connect to Network**.

Figure 9-13 Activate Your New Settings



Step 13 Click the **Link Information** tab. If you entered everything correctly, the Signal Strength and Link Quality should reappear as green bars (see Figure 9-14).

Figure 9-14 Successfully Connected



The green bars may or may not be solid the whole way across. It depends on the strength of the wireless signal and how far away you are from the wireless router, much like a cell phone.

If the link information shows no connection, you probably entered something incorrectly. Repeat the steps and double-check the settings, particularly that the passphrase is typed in exactly the same on the router and the wireless NIC. Also see Part IV of this book, "Honey, This Stupid Wireless Thing Is Not Working," particularly Chapter 10, "Troubleshooting: I Can't Connect at All."

You can further test the connection by trying to browse the Internet. Launch your web browser (such as Internet Explorer) and see if you can browse a web page.

Enabling WEP Encryption Using Windows XP

Now let's look at an example of enabling WEP encryption using the Windows Wireless Network Connection utility to configure the USB wireless NIC we installed in Chapter 8 (Linksys WUSB54G). The steps to enable encryption are as follows:

Step 1 Choose **Start > Connect To > Show All Connections**. Select the USB wireless NIC in the right side of the dialog box and then click **Change Settings of This Connection** on the left side (see Figure 9-15).

Step 2 Click the **Wireless Networks** tab (see Figure 9-16). You will see a list of wireless network profiles. Locate your wireless network in the list. The SSID you chose should be displayed (in our example, we used KF34DC3). Select the SSID and click **Properties**.

Figure 9-15 Locate the Wireless NIC

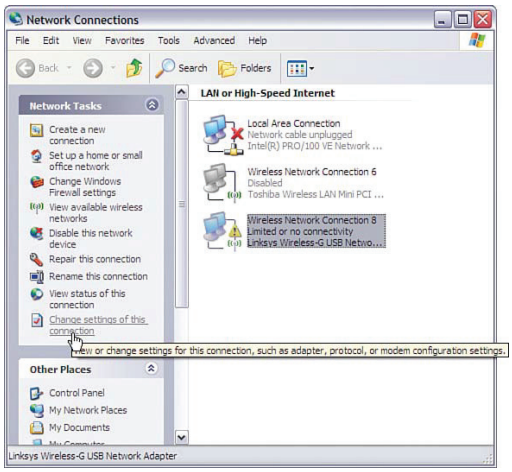
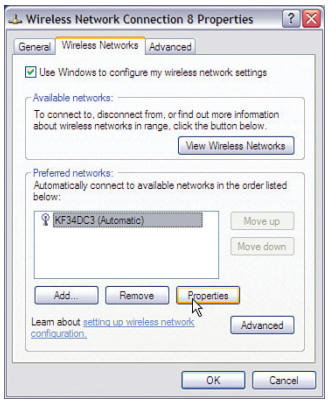
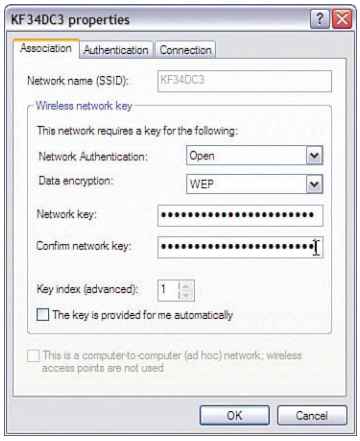


Figure 9-16 Open the Wireless Connection Properties



Step 3 Choose **Open** as the Network Authentication type. From the Data Encryption field, choose **WEP**, as shown in Figure 9-17.

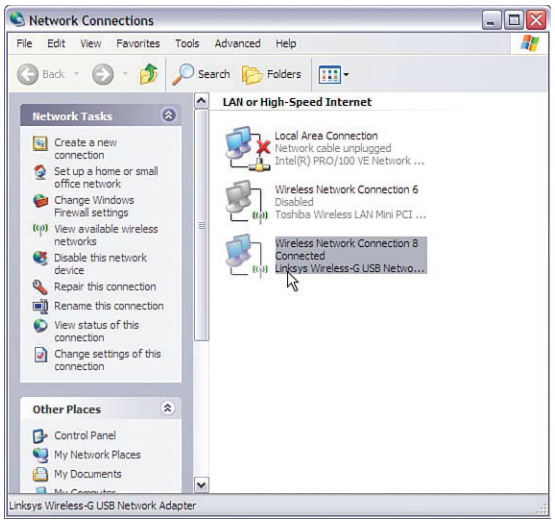
Figure 9-17 Confirm Connection to an Unsecured Wireless Network



Step 4 In the Network Key and Confirm Network Key fields, enter the 26-character WEP key (not the passphrase). Type in the whole key that you wrote down when you enabled WEP on the router (F746D793B414DF85E53008B93E in our example). You cannot generate the key from the passphrase; you need to manually enter the key itself on both lines. Leave the Key Index field set to 1. When you are done, click **OK**, and then click **OK** again.

Step 5 The NIC will reassociate to the wireless router, this time using the WEP key. In the View Available Wireless Networks dialog box, the status will change to Connected, as shown in Figure 9-18.

Figure 9-18 Connected to Wireless Network



You can test the connection by trying to browse the Internet. Launch your web browser (such as Internet Explorer) and see if you can browse a web page.

WPA Encryption Example

To compare enabling WEP encryption to enabling WPA encryption, let's take an example of WPA. Enabling WPA encryption is similar to enabling WEP encryption, with three main differences:

- With WPA you do not choose a passphrase or generate a key. Instead, you choose a preshared key (PSK). A PSK looks a lot like a passphrase: It's a series of random letters and digits that you create that acts as a password for joining into your wireless network. Only wireless NICs that have the PSK can join your network.
- With WPA you must choose whether to use the TKIP or AES mode for WPA encryption. If your wireless router and all wireless NICs support AES, use it, because AES is more secure than TKIP; otherwise, use TKIP. You cannot mix modes. In other words, you can't set some NICs to use TKIP and others to use AES. All NICs must use the same mode.
- With WPA you must decide what length of time an encryption key can be used before a new key is assigned, which is called a *key renewal period*. The shorter the period, the less time a hacker has to try to "crack" the key. For example, if you set the time period to 1800 seconds (which is

30 minutes, for you non-math majors), a key is used for 30 minutes, and then the wireless router and wireless NIC create a new key. If a hacker "cracks" the key within 30 minutes (which is pretty tough to do), the key is valuable only for the remainder of the 30 minutes, after which it is switched to an entirely new key, and the hacker would have to start all over.

- With WPA, if a longer WPA preshared key (more characters) is used, there is an added security benefit (whereas WEP keys are fixed length and WEP passphrase length does not directly impact the strength of the key). Some security experts recommend choosing a WPA PSK of at least 20 characters.



Note: So how long should you set the key renewal period? There is no great answer, although if you have the value set too low (1 to 2 minutes, for example), it could cause connectivity issues for some NICs. We recommend following manufacturer recommendations (or defaults).

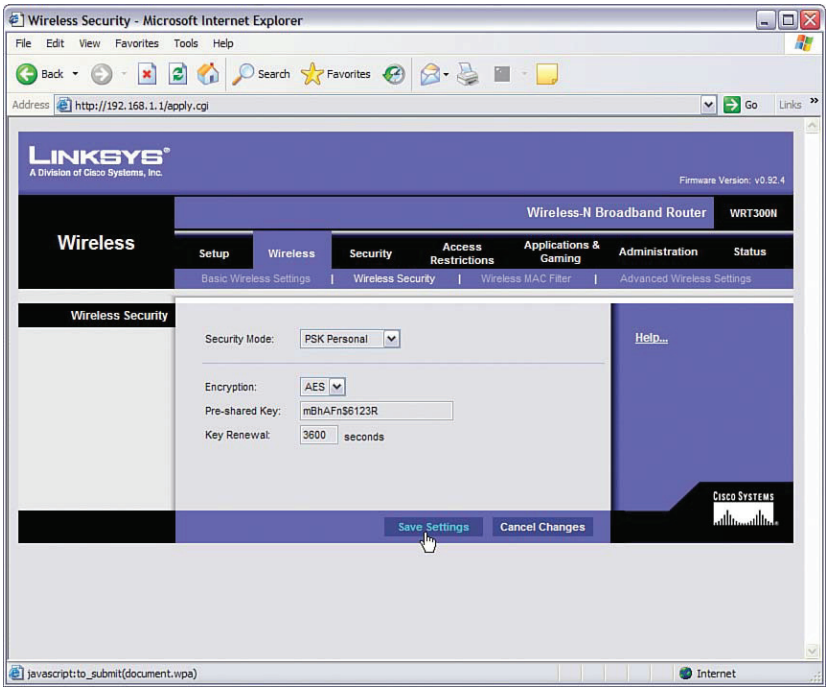
Again, we must set the security settings to be identical on both the wireless router and the wireless NIC. The next couple sections show an example of how to set up WPA.

Enabling WPA Encryption on the Wireless Router

First, we need to set up WPA on the wireless router:

Step 1 On the Wireless Security subtab (see Figure 9-19), from the Security Mode field, choose **PSK Personal**. (On some Linksys products, the choice is called WPA Pre-Shared Key.)

Figure 9-19 Enabling WPA Encryption on the Wireless Router



Step 2 From the Encryption field (see Figure 9-19), choose either **TKIP** (for WPA1) or **AES** (for WPA2). If your wireless router and all wireless NICs support AES mode, choose it, because AES is more secure. If any of them does not, choose TKIP. You cannot configure some with TKIP and some with AES.

Step 3 In the Pre-Shared Key field, enter the preshared key you made up (in our example, mBhAFn$6123R).

Step 4 In the Key Renewal field, enter the number of seconds that you want the key to be used before changing it. We chose 3600 (60 minutes) for this example.

Step 5 Click **Save Settings**.

Enabling WPA Encryption on the Wireless NIC

With WPA, we also then need to tell the super-secret password to each of the devices with wireless cards so that they know how to decode the conversations with the wireless router. Here is an example for a PCMCIA laptop NIC (Linksys WPC54G) managed with the Linksys WLAN Monitor utility:

Step 1 Launch the Linksys WLAN Monitor by double-clicking the icon on the far right of your Windows taskbar (the example shows a computer running Windows XP). If you do not see such an icon, try going through **Start > Programs > Linksys Wireless Card > WLAN Monitor**.

Step 2 Notice that there is no connection to the wireless router (the signal bars are not "lit up"). This is normal since we enabled encryption on the wireless router but have not yet enabled it on the wireless NIC. (See Figure 9-20.)

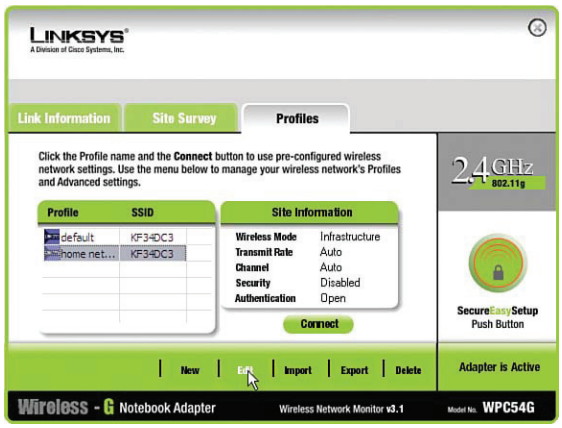
Step 3 Click the **Profiles** tab.

Figure 9-20 Launch the WLAN Monitor Utility



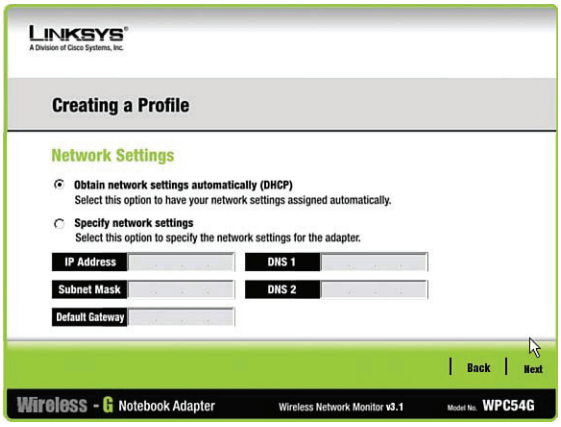
Step 4 Select the profile for your home wireless network and click **Edit** (see Figure 9-21).

Figure 9-21 Select and Edit the Wireless Profile



Step 5 No changes are needed to the network settings (see Figure 9-22). Click **Next**.

Figure 9-22 Network Settings Stay the Same



Step 6 The Wireless Security window appears, as shown in Figure 9-23. Choose **WPA-Personal** (on some Linksys wireless NICs, the option may be listed as WPA or WPA Pre-Shared Key). Click **Next**.



Note: As mentioned earlier, you will see several options in the list, including WPA-Enterprise, RADIUS, and LEAP. These are options for corporate networks, not home networks, so just ignore them.

Step 7 A second Wireless Security settings window appears, as shown in Figure 9-24. From the Encryption field, choose **AES** (or **TKIP**, whatever you selected on the wireless router).

Figure 9-23 Choose WPA-Personal as the Security Type

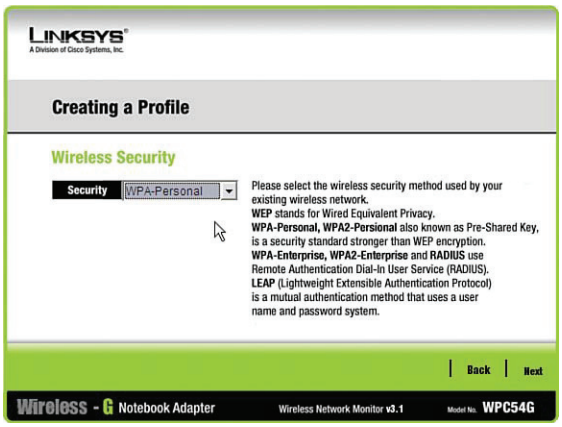
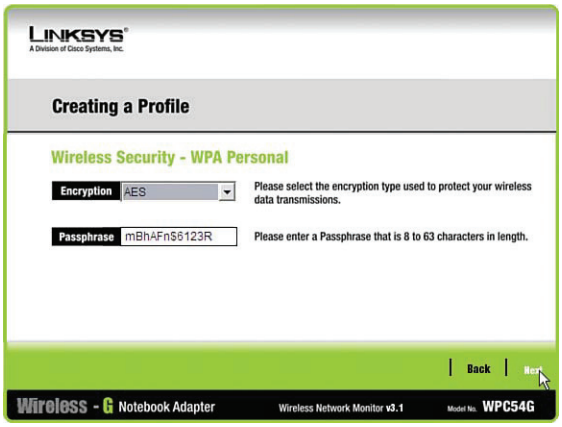


Figure 9-24 Enter the WPA Mode and Preshared Key



Step 8 In the **Passphrase** field, enter the WPA preshared key exactly as you entered it earlier when you enabled WPA on the router (mBhAFn$6123R for this example). Click **Next**.



Note: Make sure to enter the PSK exactly as you did on the wireless router. Lowercase *a* is different from uppercase *A*. The two keys (on the router and on the wireless card) must be identical.

Step 9 A confirmation window appears (see Figure 9-25). Double-check the new security settings and click **Save**. A Congratulations window appears (which is the same as Figure 9-13). Click **Connect to Network**.

Step 10 Click the **Link Information** tab. If you entered everything correctly, the Signal Strength and Link Quality should reappear as green bars (see Figure 9-26).

Figure 9-25 Confirm the New Settings

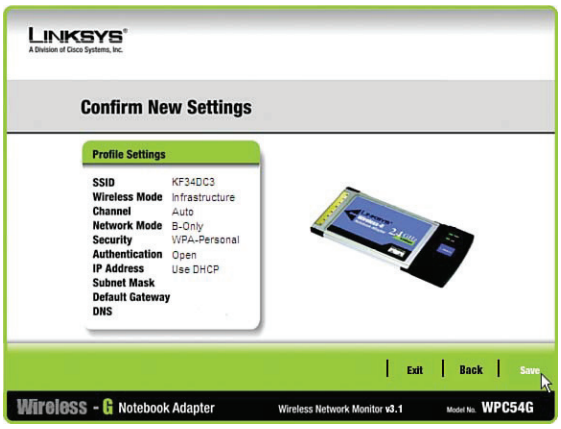
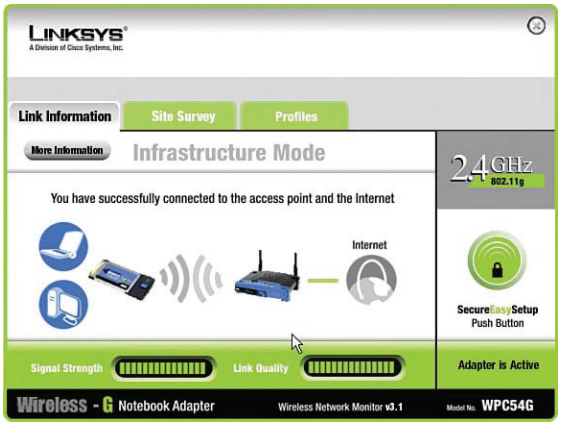


Figure 9-26 Successfully Connected



Continue setting up each NIC with the super-secret password, each time checking to see whether the connection is re-established to the wireless router.

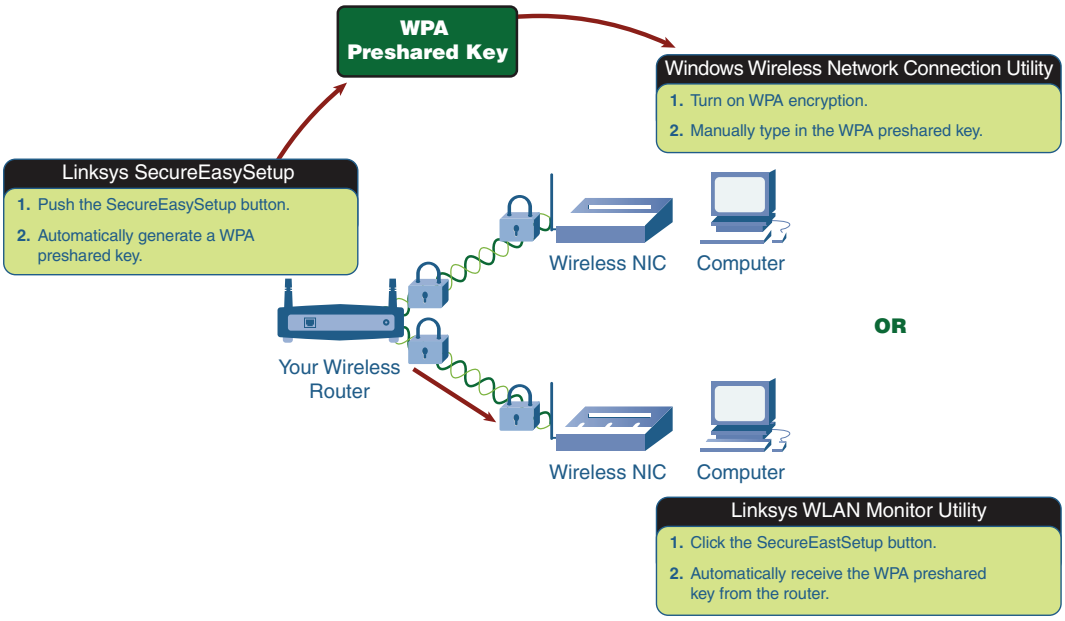
Setting Up Wireless Encryption with Linksys SecureEasySetup

To try to simplify the process of setting up a secure wireless network, Linksys released a feature called *SecureEasySetup (SES)*. SES provides a push-button setup process that can automatically set up a secure connection between the wireless router and wireless NICs.

The SES process works as shown in Figure 9-27. When you invoke SES on the wireless router, it automatically creates a WPA PSK. The router then starts accepting new wireless NIC connections.

You then invoke SES on each of the wireless NICs, which automatically receive the WPA PSK directly from the wireless router. There is no need to manually program the WPA key into the wireless NIC yourself.

Figure 9-27 Setting Up Wireless Encryption with Linksys SecureEasySetup



This truly is a push-button approach to wireless security. However, there are some very important limitations to consider:

- SES is supported on only a subset of Linksys wireless routers and Linksys wireless NICs. Consult the Linksys website at http://www.linksys.com to see which products support SES.
- Only Linksys wireless NICs can be set up using SES. NICs from manufacturers other than Linksys have to be set up manually or using a utility provided by that manufacturer.
- If you have a wireless NIC that you manage with the Windows Wireless Network Connection utility, such as one that is built in to a laptop, you have to manually program the NIC to join the wireless network, because SES cannot be used.
- SES automatically configures wireless security based on WPA and the TKIP mode. If you want to use another security mode, such as WEP, WPA with AES, or WPA2, you cannot use SES.
- For guests visiting your home or for non-Linksys devices, you need to write down the SSID and WPA key that SES creates, and enter them manually to allow them to join your wireless network.

Limitations aside, if you are setting up a new wireless network and have mainly Linksys products (in other words, a Linksys wireless router and Linksys wireless NICs), and the products all support SES, SES can be an easy and effective way to get your network started quickly, and secured.

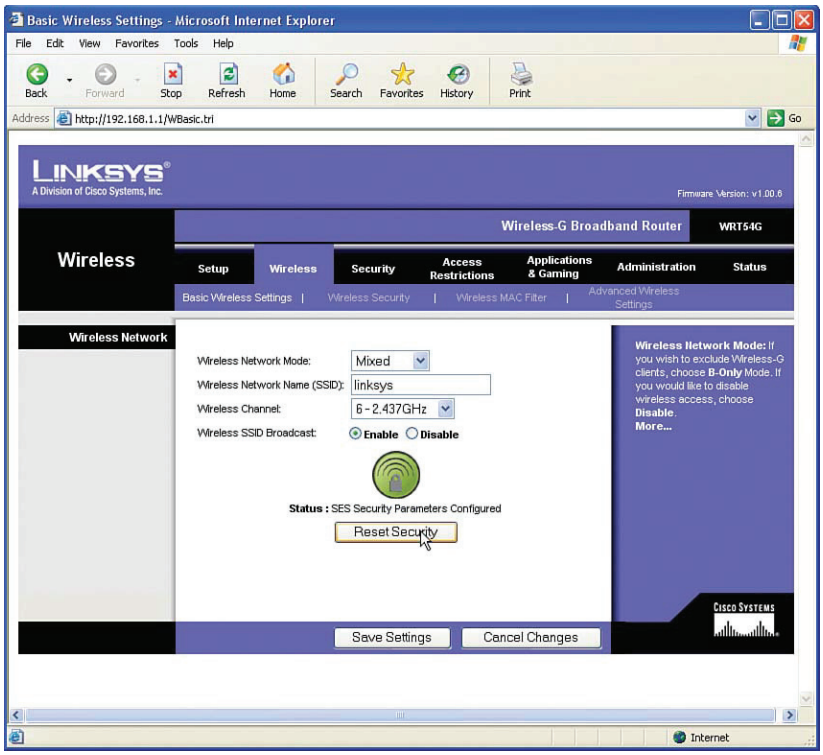
The steps to set up a network with SES are shown in the next two sections.

Linksys SecureEasySetup on the Wireless Router

First, we need to set up SES on the wireless router:

Step 1 Access the wireless router using your Internet browser. Click the **Wireless** tab. Click the **Basic Wireless Settings** subtab (see Figure 9-28).

Figure 9-28 Access the Linksys SecureEasySetup Activation



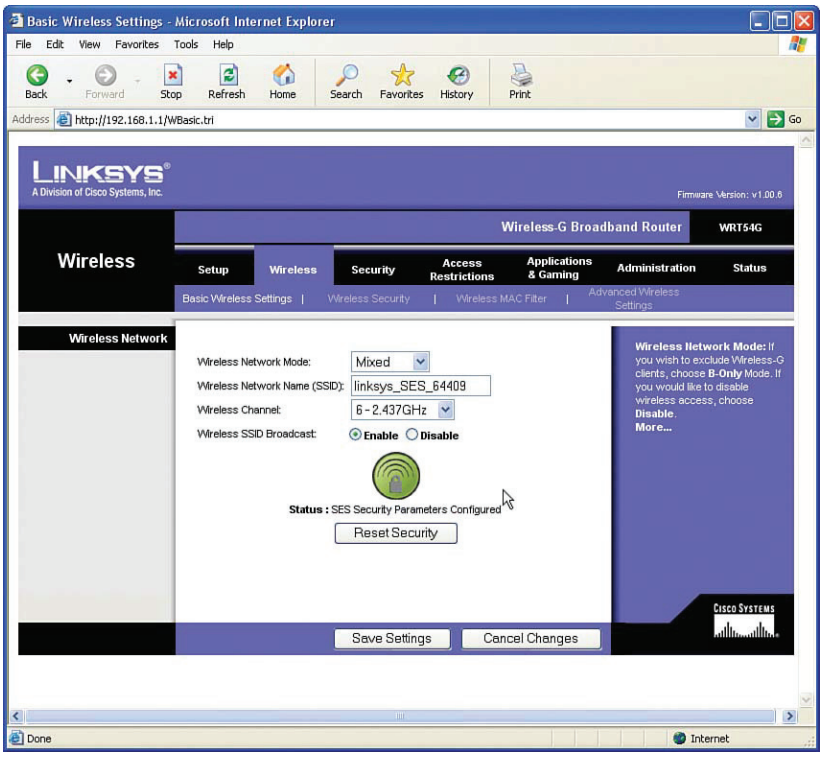
Step 2 You should see a green icon with a padlock on the menu. If you do not, the model of wireless router you have may not support SES. Click **Reset Security**.



Note: You need to reset the security settings only once for your network, not each time you add new wireless NICs. Resetting the settings assigns a new SSID and WPA preshared key, so wireless NICs that were previously set up and connected to your wireless router will lose their connections.

Step 3 Notice that SES has generated a new SSID (linksys_SES_64409 in this example) for your wireless router (see Figure 9-29). Write it down; you will need it when you have to program wireless NICs that do not support SES.

Figure 9-29 Linksys SecureEasySetup Assigns a New SSID



Step 4 Click the **Wireless Security** subtab (see Figure 9-30). You see that SES has set the wireless router to use WPA Personal (on some Linksys routers, this may be WPA or WPA Pre-Shared Key) and TKIP mode. You also see that SES has generated a random WPA preshared key (2iwitleatw9yphq2 in this example). Write it down; you will need it when you have to program wireless NICs that do not support SES.

Step 5 Click the **Basic Wireless Settings** subtab again. You are now ready to trigger the router to accept new wireless NICs using SES. When you are ready (you may want to jump to the section "Linksys SecureEasySetup on the Wireless NIC" before proceeding), click the green padlock icon to begin the SES process. A confirmation dialog box appears, as shown in Figure 9-31, stating that the SES process has been started. Click **OK**.

Figure 9-30 Displaying the WPA PSK Generated by Linksys SecureEasySetup

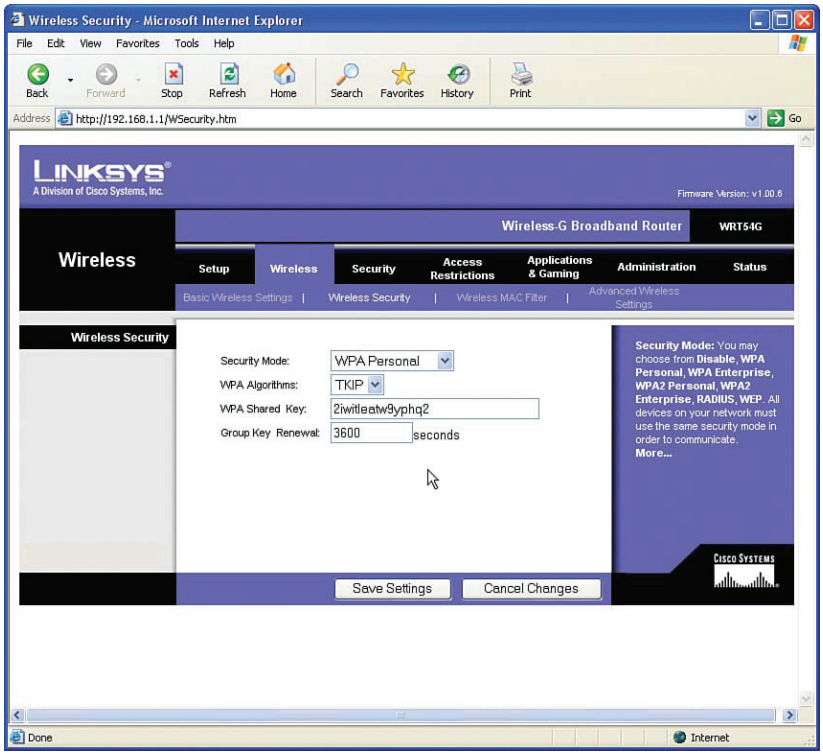
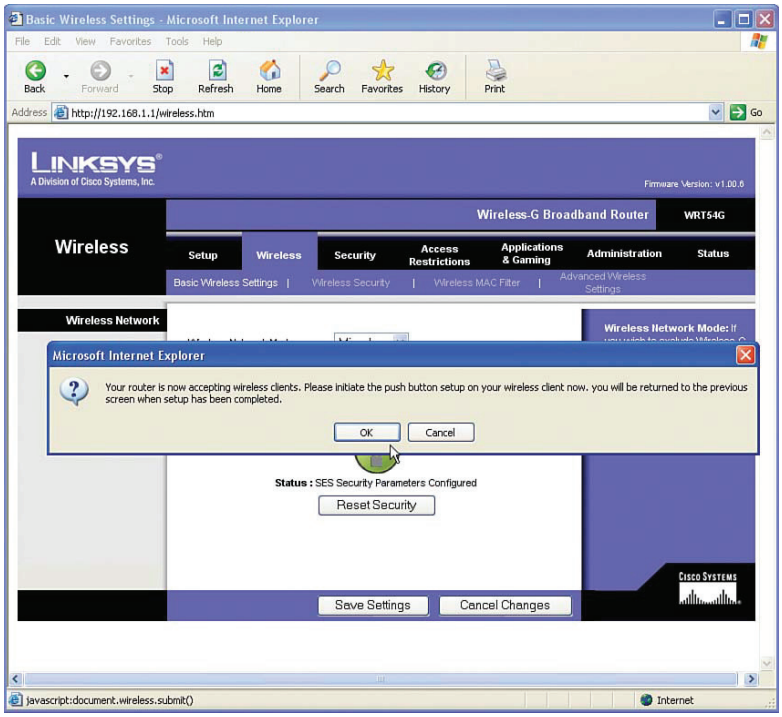
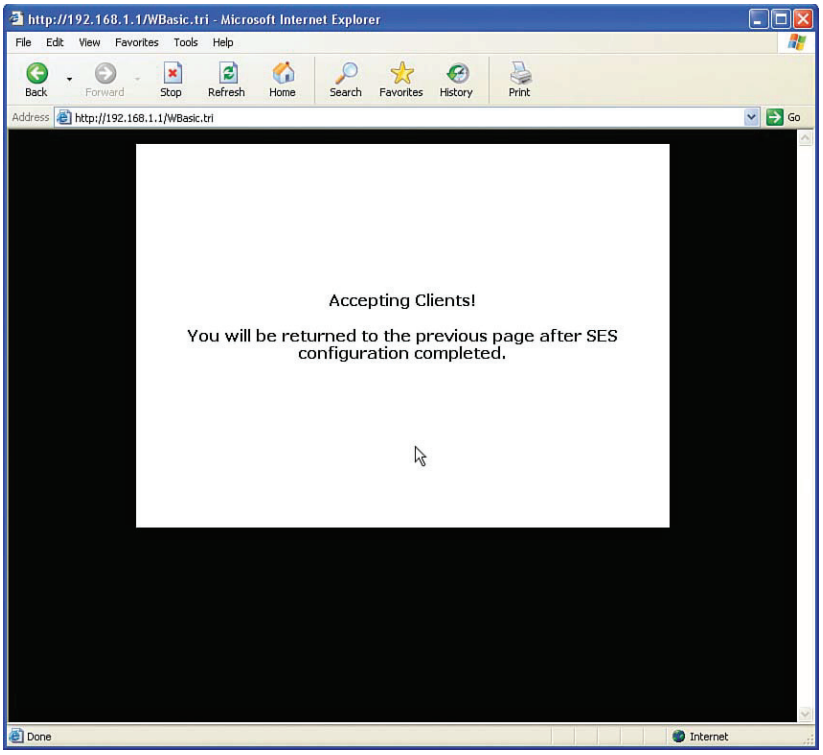


Figure 9-31 Linksys SecureEasySetup Is Enabled



Step 6 The wireless router will now accept new connections from wireless NICs for about a minute or two. During the acceptance period, the message shown in Figure 9-32 is displayed. When the router returns to the main menu, the SES acceptance period has ended.

Figure 9-32 Wireless Router Is Accepting New Connections



It's important that you synchronize the steps on the wireless router and wireless NIC you are connecting. You need to make sure the wireless router is accepting new clients at the time that you trigger the NIC to associate itself (see the next section).

You can repeat Steps 5 and 6 as many times as necessary to connect a wireless NIC to the wireless router. At a future time, if you need to add a new wireless NIC to your network, you can go straight to Step 5. You should not start with Step 1 in this case, because Steps 1 through 4 are needed for your network only when you initially set it up, not every time you add a new device.

As a caution, though, if you repeat starting from Step 1, you will reset all the security settings for your wireless network and therefore have to repeat Steps 5 and 6 with each computer in your network to obtain the modified settings.



Note: Alternatively, to enable SecureEasySetup to accept a new wireless device, you can press the Cisco logo or the green circle with a padlock icon on the front of the wireless router instead of following Steps 5 and 6. The logo or icon will start flashing, indicating it is accepting new NIC clients. When it stops flashing, the acceptance period has ended. By the way, you will see the icon flashing if you follow Steps 5 and 6 also.

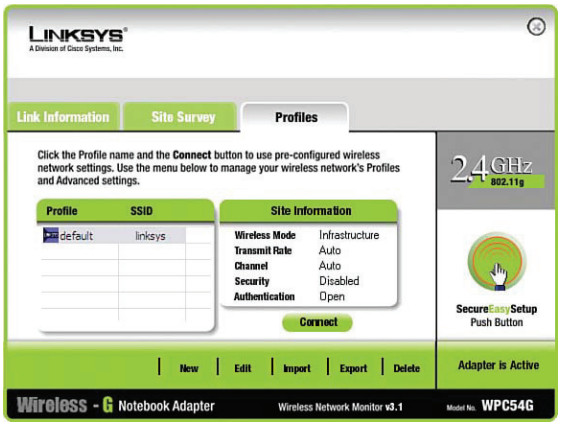
Linksys SecureEasySetup on the Wireless NIC

With Linksys SES, the wireless NIC obtains the WPA key (and SSID) directly from the wireless router. To use SES, you need to first execute the steps in the preceding section for the wireless router, up through Step 4. When you execute Step 5 in the preceding section, you need to execute the SES process on the wireless NIC. Here is an example for a PCMCIA laptop NIC (Linksys WPC54G):

Step 1 Launch the Linksys WLAN Monitor by double-clicking the icon on the far right of your Windows taskbar (the example shows a computer running Windows XP). If you do not see such an icon, try going through **Start > Programs > Linksys Wireless Card > WLAN Monitor**.

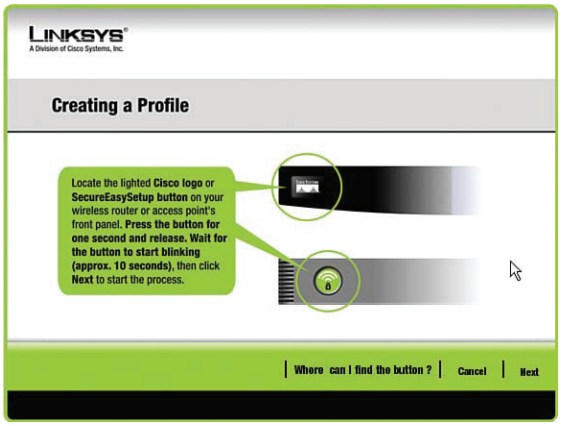
Step 2 Click the **Profiles** tab (see Figure 9-33).

Figure 9-33 Launch the WLAN Monitor Utility



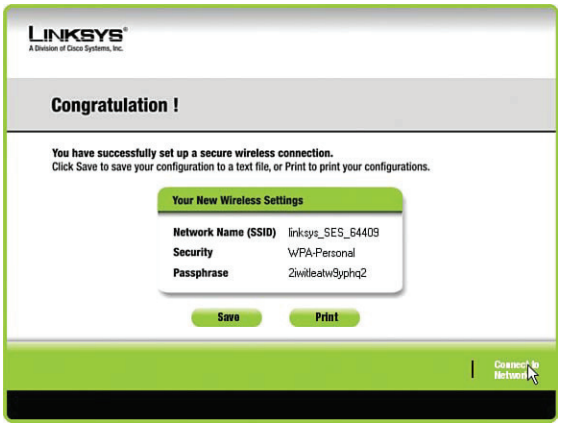
Step 3 Click the green circle with a padlock icon on the right side of the dialog box (refer to Figure 9-33). A dialog box appears telling you it is time to initiate SES on the wireless router, as shown in Figure 9-34. Follow Steps 5 and 6 in the previous section at this point and then return here.

Figure 9-34 Trigger Linksys SecureEasySetup on the Wireless Router



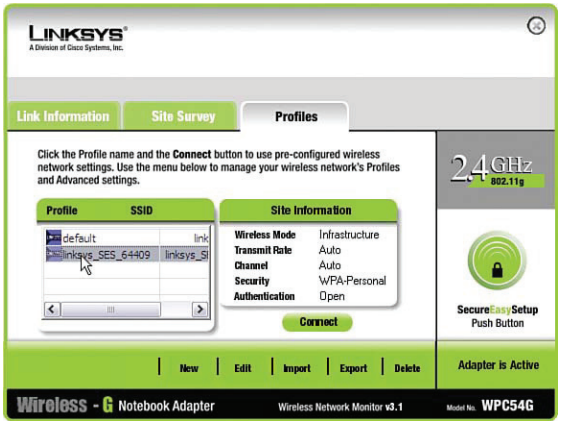
Step 4 Click **Next** on the WLAN Monitor utility. The wireless NIC retrieves the WPA pre-shared key (and SSID) from the wireless router. Figure 9-35 shows a successful result, where you can see that the random WPA key that was created by the router is now programmed into the NIC (2iwitleatw9yphq2 in this example). Also notice that the SSID has been reassigned to the one provided by the router as well (linksys_SES_64409 in this example). Click **Connect to Network**.

Figure 9-35 Wireless Security Settings Are Retrieved



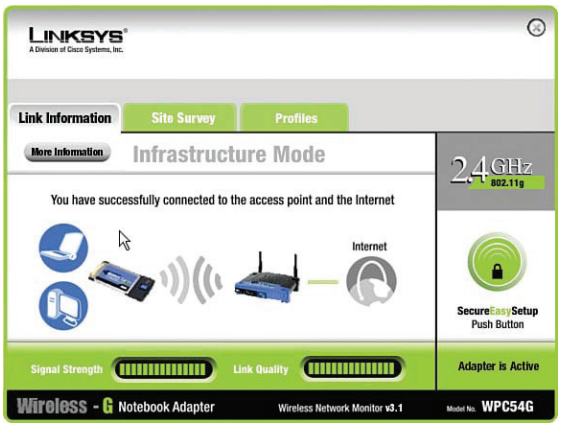
Step 5 A new wireless profile is created automatically by SES for the wireless network just programmed using SES (see Figure 9-36). You can rename the profile to something more recognizable if you want.

Figure 9-36 New Wireless Profile Created



Step 6 Click the **Link Information** tab. The Signal Strength and Link Quality should show green bars, indicating a connection to the wireless router (see Figure 9-37).

Figure 9-37 Successfully Connected



You can repeat this process with each wireless NIC, each time triggering SES to accept clients on the wireless router and then triggering SES on the wireless NIC to retrieve its wireless security settings from the router. In other words, you need to follow this procedure for every NIC that is capable of being set up using SES.

Each time you add a new NIC, check to see whether the connection is established to the wireless router.

Setting Up Wireless Encryption with Linksys EasyLink Advisor

As discussed in Chapters 7 and 8, there is a new software setup utility for Linksys routers (under development at the time of this writing) named EasyLink Advisor. EasyLink provides a simplified way to set up wireless routers and add wireless computers to the network.

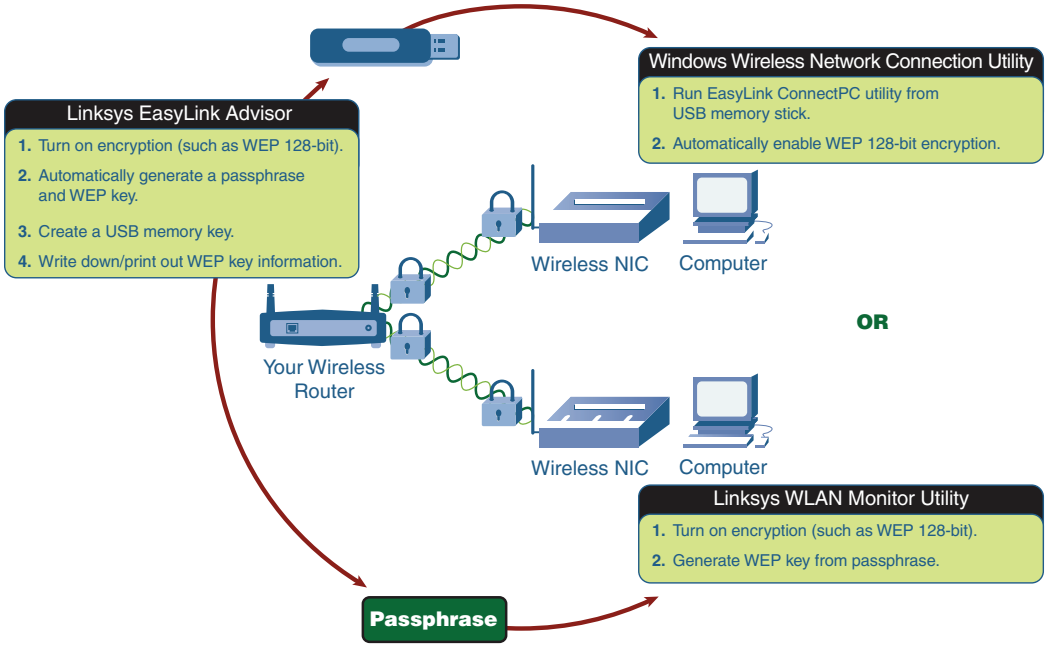
You also can use EasyLink to aid in the setup of wireless security. Before starting, you need a USB memory stick. Similar to Chapter 8, if the computer runs Windows XP and higher, we can use EasyLink to create a wireless profile on a USB memory stick, including the wireless security settings (see Figure 9-38), and then simply plug that USB memory stick into the computer we want to join the secure wireless network, automatically updating the wireless profile with the security settings.



Note: In Figure 9-38 you see that 128-bit WEP is being referenced. At the time of this writing, 128-bit WEP is the encryption option that Linksys EasyLink Advisor supports. Newer versions of EasyLink may support additional encryption types.

Also at the time of this writing, using a USB memory key to set up wireless security using EasyLink Advisor works only for computers running Windows and higher, and only when using the Windows Wireless Network Connection utility. It does not work if a separate program utility is required to manage wireless NICs, including the Linksys WLAN Monitor program or other manufacturers' wireless connection manager programs.

Figure 9-38 Setting Up Wireless Encryption with Linksys EasyLink Advisor



If you are using an older version of Windows (for example, Windows 2000 or 98SE), the EasyLink program helps you print out the wireless profile security settings you need. Then, you have to use the printout to manually configure the wireless security settings on your wireless NIC using a wireless connection manager program, like the example shown earlier in "Enabling WEP Encryption on the Wireless NIC" for the Linksys WLAN Monitor program.

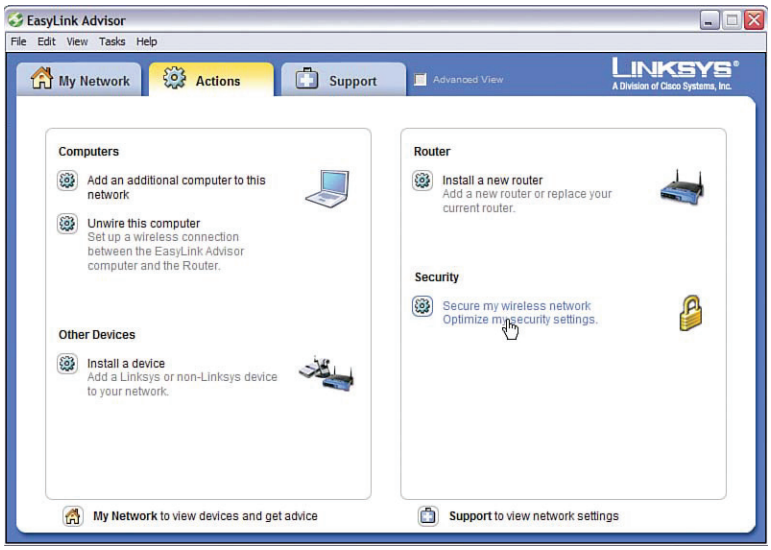
We will continue the example started in Chapters 7 and 8, with a Linksys WRT54G wireless router and two computers with wireless NICs, both running Windows XP.

Linksys EasyLink Advisor on the Wireless Router

When you are using EasyLink Advisor to manage your home network, the first step to setting up encryption is to set up the wireless security parameters on the wireless router. The steps for doing so are as follows:

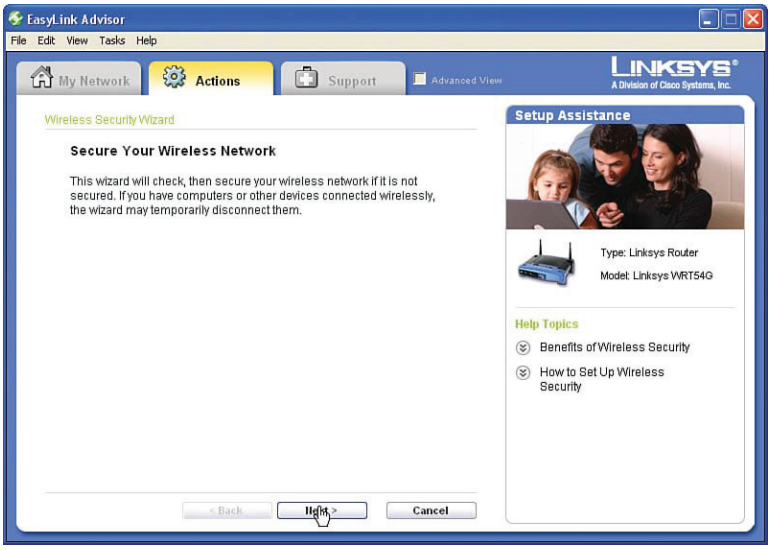
Step 1 On the computer with Linksys EasyLink Advisor installed, launch the EasyLink Advisor program by double-clicking its icon on the running tasks taskbar or by choosing **Start > Programs > Linksys EasyLink Advisor**. You should see the network. Click the **Actions** tab and then click **Secure My Wireless Network**, as shown in Figure 9-39.

Figure 9-39 Secure Wireless Network with Linksys EasyLink Advisor



Step 2 The Wireless Security Wizard starts up, as shown in Figure 9-40. Click **Next**.

Figure 9-40 Start the Wireless Security Wizard



Step 3 Click the **Override Current Wireless Settings** radio button, as shown in Figure 9-41. Click **Next**.

Step 4 The Wireless Security Wizard turns on 128-bit WEP on the wireless router, creates a random WEP passphrase, and generates a WEP key from the passphrase. When complete, the dialog box shown in Figure 9-42 is displayed. Click the **Yes, I Have Computers or Other Devices That Are Wireless** radio button and then click **Next**.

Figure 9-41 Secure the Wireless Network

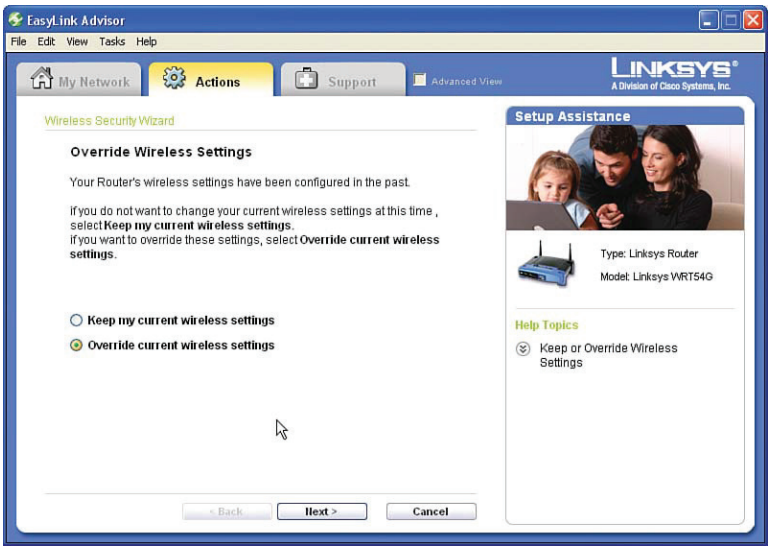
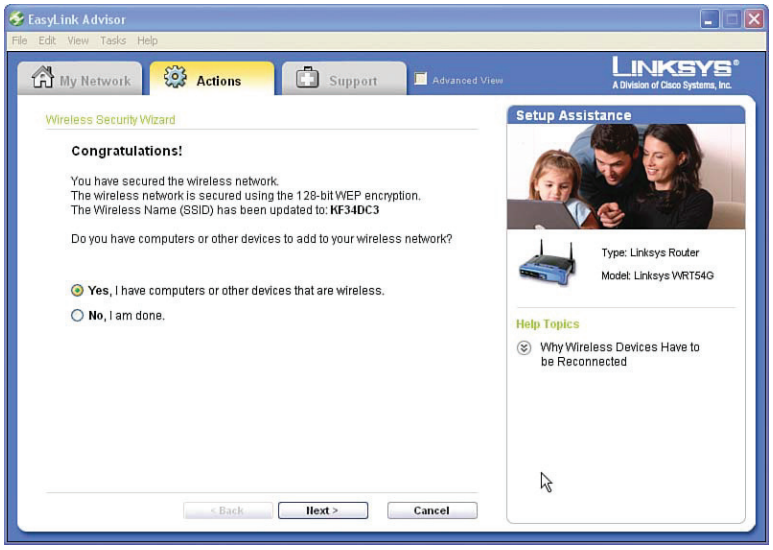


Figure 9-42 Prepare to Propagate Wireless Security Settings to Other Computers



Step 5 The Wireless Security Wizard displays the wireless security settings it created, as shown in Figure 9-43. Write them down in your notebook and print them out. Click **Next**.

Step 6 The Wireless Security Wizard asks if you have an additional computer to add, as shown in Figure 9-44. Click **Yes, I Have an Additional Computer to Add** and then click **Next**. Even though you already said Yes in Step 4 to add computers, you must say Yes again in Step 6.

Figure 9-43 Write Down and Print Out the Wireless Security Settings

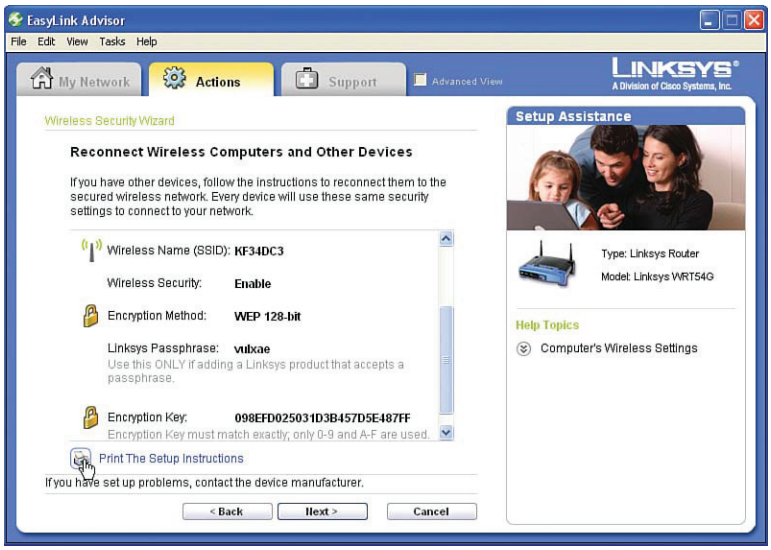
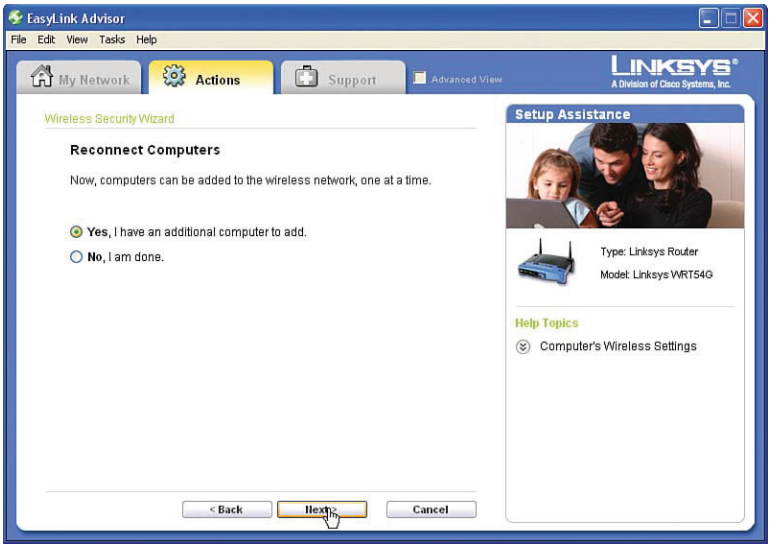


Figure 9-44 Yes, We Want to Add an Additional Computer



Step 7 The Wireless Security Wizard asks you if the additional computer is wired or wireless, as shown in Figure 9-45. Click **Wireless** and then click **Next**.

Step 8 The Wireless Security Wizard then asks you to plug in a removable media device, as shown in Figure 9-46. Plug a USB memory stick into an open USB port on the computer running EasyLink and click **Next**. The Wireless Security Wizard confirms the location you want to save the wireless profile to (on the USB memory key, in this example E:/). Click **Next**.

Figure 9-45 Yes, It Is a Wireless Computer

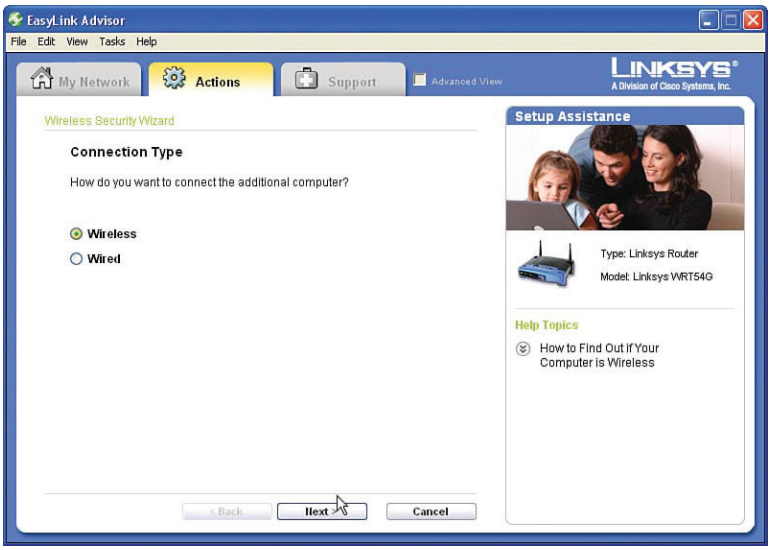
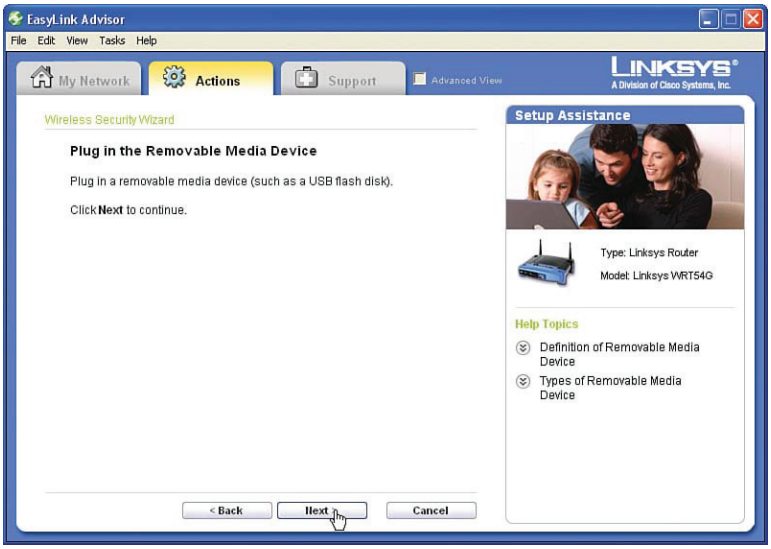


Figure 9-46 Wireless Security Wizard Requests to Plug in USB Memory Key



Step 9 The Wireless Security Wizard saves a program file to the USB memory key, as shown in Figure 9-47. You can now remove the USB memory key and take it to the computer you want to add to your wireless network.

Step 10 If you click the My Network tab (as shown in Figure 9-48), you will notice that only the wired computer appears on the network diagram, not the wireless computers. This is normal, because we changed the wireless security settings but have not yet changed the corresponding settings on the computers.

Figure 9-47 Wireless Profile Program Saved on the USB Memory Key

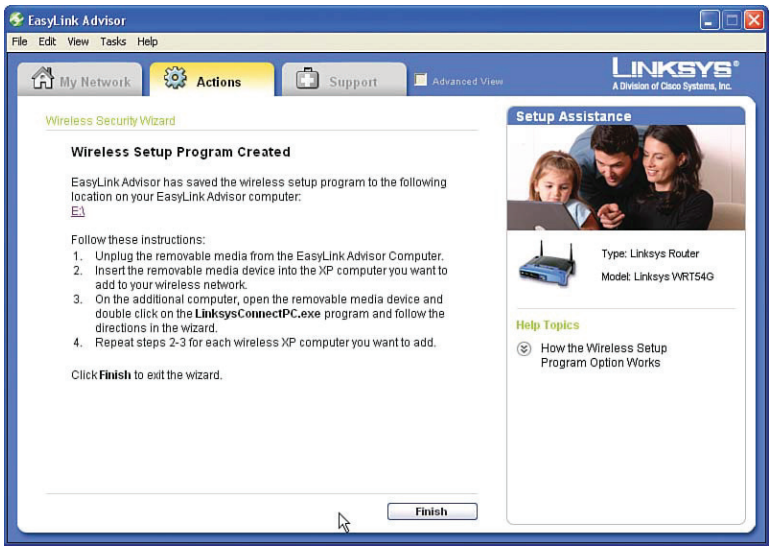
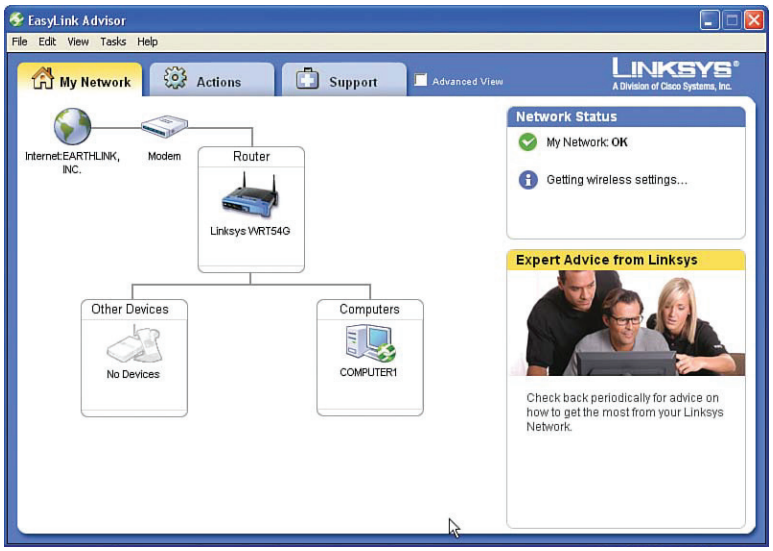


Figure 9-48 Wireless Connected Computers No Longer on the Network Diagram



Using EasyLink Advisor to Add Encryption to Wireless NICs

As discussed in Chapter 8, you can manage the wireless connection in each of your computers in a couple of different ways, including with the Windows Wireless Network Connection utility or the Linksys WLAN utility. The same wireless connection manager you use to associate and set up wireless connections is used to also enable wireless security.

The sections that follow show two examples:

- A Windows XP laptop with a built-in wireless NIC that we set up using the Windows Wireless Network Connection utility

- A Windows XP laptop computer with a PCMCIA wireless card that we set up with the Linksys WLAN utility

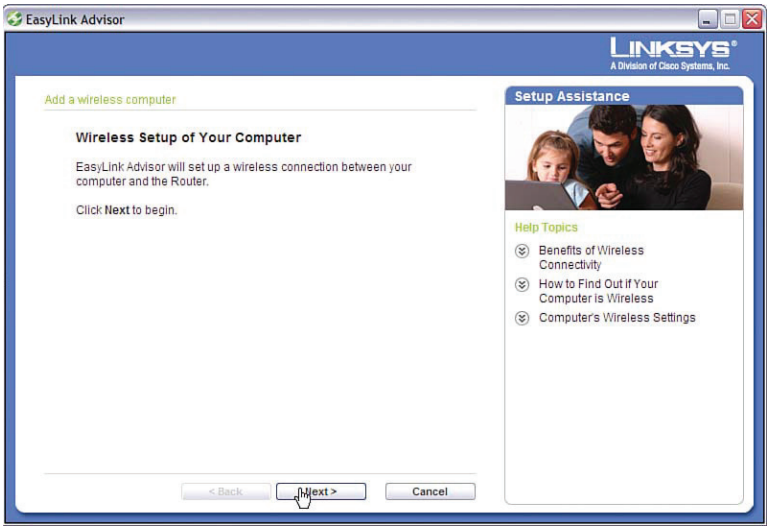
EasyLink Advisor with Windows-Managed NICs

For wireless NICs that are managed with Windows Wireless Network Connection utility, we can easily transfer the wireless security settings from the wireless router to the wireless NIC using a USB memory key. The following steps show how to do so:

Step 1 Plug in the USB memory key to an open USB port. Double-click **My Computer** and then double-click the USB memory key "drive" (E:/ in this example). You will see a program on the USB memory key named LinksysConnectPC.exe. Double-click the program icon to launch the program.

Step 2 A very small version of the Linksys EasyLink Advisor program starts executing on the computer you are adding to the wireless network, as shown in Figure 9-49. Click **Next**.

Figure 9-49 Linksys EasyLink Advisor Wireless Profile Creator Utility Launches



Step 3 The program modifies the wireless profile with the wireless security settings and re-establishes the wireless connection (see Figure 9-50).

Step 4 As shown in Figure 9-51, the program creates a wireless profile using the wireless network information from the wireless router (that it has stored on the USB memory key). Click **Finish**.

Note: The window shown in Figure 9-51 makes a reference to removing the network cable. If you had previously connected the computer to the network with a cable, you can remove it at this point. If this is the first time connecting the computer to the network, ignore the comment.

Figure 9-50 Linksys EasyLink Advisor Re-Establishing the Wireless Connection



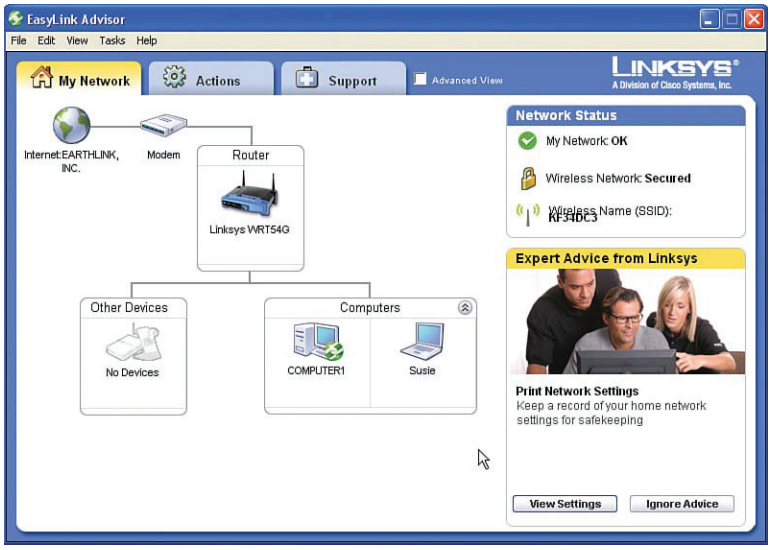
Figure 9-51 Wireless Profile Created



Step 5 Go back to the computer where the (main) EasyLink Advisor program is installed and see if the router now "sees" the computer we just added. Click the **My Network** tab. As shown in Figure 9-52, you can see graphically that there are two computers now connected to the wireless router: Computer1, which is the computer we used in Chapter 7 to set up the wireless router, and now the computer designated as Susie, which is the computer we just re-joined to the wireless network.

At this point the wireless profile should be created, including the wireless security settings, and your wireless NIC should reassociate with your wireless router. Just like in the other examples, start your Internet browser and see if you can browse a web page. You can now remove the USB memory key and take it to the computer you want to add to your wireless network.

Figure 9-52 Computer Reappears in the Network Diagram



Note: The USB memory key you created is valid until you change any of the settings on your wireless network. We recommend keeping it handy; hang it on the side of your refrigerator or in some other easily accessible place. When you have guests staying at your home who want to connect to your wireless network, you can hand them the USB memory key and walk them through creating a wireless profile on their Windows XP laptop.

EasyLink Advisor with Linksys Utility–Managed NICs

Now, let's walk through an example of setting up encryption on a computer running Windows XP, using a PCMCIA wireless NIC (Linksys WPC54G) and the Linksys WLAN utility.

In this case, we cannot propagate the wireless security information automatically using a USB media key like we did earlier. We need to take the printout of wireless security settings from EasyLink Advisor and manually enter the key information. The steps to do so follow:

Step 1 Launch the Linksys WLAN Monitor by double-clicking the icon on the far right of your Windows taskbar (the example shows a computer running Windows XP). If you do not see such an icon, try going through **Start > Programs > Linksys Wireless Card > WLAN Monitor**.

Step 2 Click the **Profiles** tab. Select the profile for your home wireless network, and click **Edit** at the bottom of the screen, as shown in Figure 9-53.

Step 3 No changes are needed to the network settings. Click **Next**. The Wireless Security window appears (see Figure 9-54). Choose **WEP** and click **Next**.

Figure 9-53 Select and Edit the Wireless Profile

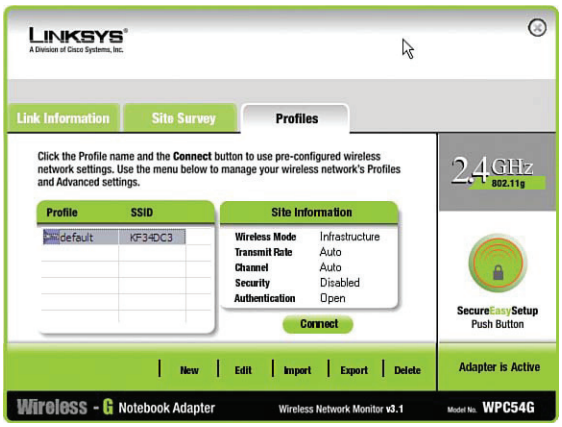
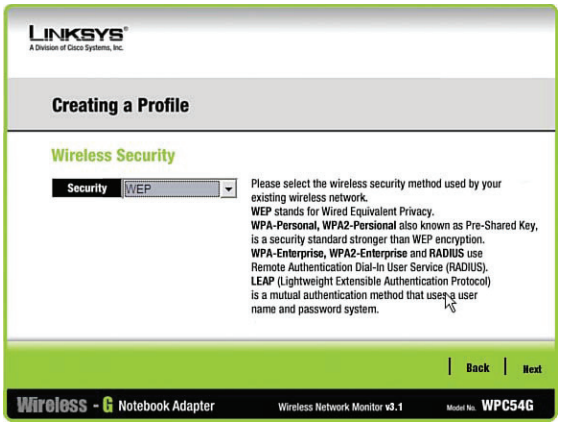
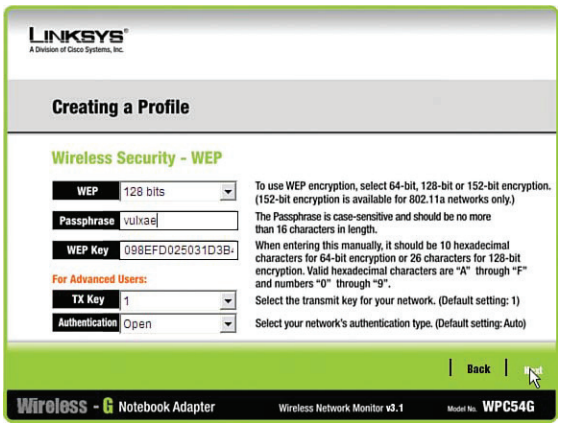


Figure 9-54 Choose WEP as the Security Type



Step 4 A second Wireless Security settings window appears (see Figure 9-55). From the WEP field, choose **128 Bits**.

Figure 9-55 Enter the WEP Key

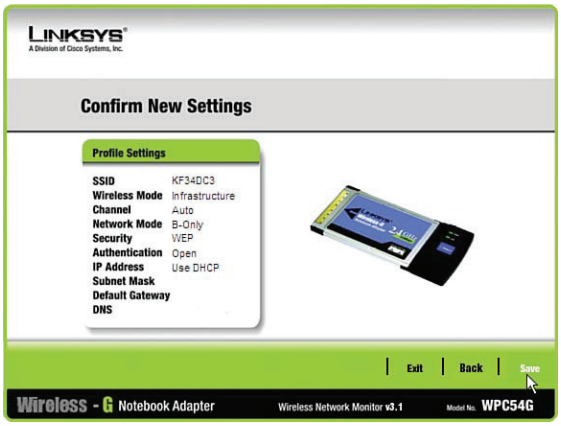


Step 5 Enter in the Passphrase field the passphrase exactly as it appears in the printout from EasyLink Advisor, when you enabled security on the router (vulxae for this example). You will see the WEP key being built as you enter the passphrase. After you enter the complete passphrase, click **Next**.

IMPORTANT NOTE: Make sure to enter the passphrase exactly as it appears on the printout. Lowercase *a* is different from uppercase *A*. The two keys (on the router and on the wireless card) must be identical.

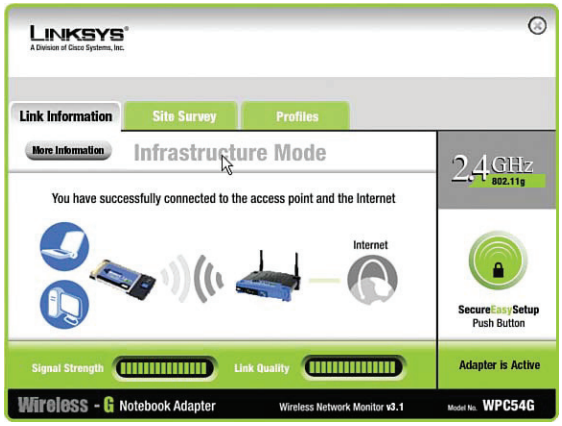
Step 6 A confirmation window appears (see Figure 9-56). Double-check the new security settings and click **Save** (with some Linksys wireless NICs, the option may be **Connect to Network**).

Figure 9-56 Confirm and Activate the New Settings



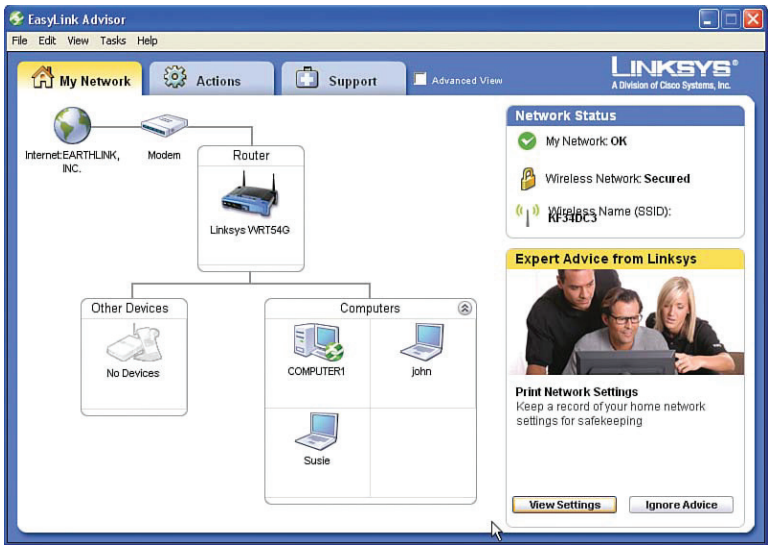
Step 7 Click the **Link Information** tab. If you entered everything correctly, the Signal Strength and Link Quality should reappear as green bars, as shown in Figure 9-57.

Figure 9-57 Successfully Connected



Step 8 Go back to the computer where the (main) EasyLink Advisor program is installed and see if the router now "sees" the computer we just added. Click the **My Network** tab. As shown in Figure 9-58, you can see graphically that there are three computers now connected to the wireless router: Computer1, which is the wired computer we used in Chapter 7 to set up the wireless router, and now Computer2 and Computer3 (which we named Susie and John), which are the computers we just added wireless security to.

Figure 9-58 Computers Reappear in the Network Diagram



Again, the green bars may or may not be solid the whole way across. It depends on the strength of the wireless signal and how far away you are from the wireless router, much like a cell phone. If the link information shows no connection, you may have entered something incorrectly. Repeat the steps and double-check the settings, particularly that the passphrase is typed in exactly the same on the router and the wireless NIC. Also see the troubleshooting information in Part IV of this book, particularly Chapter 10.

You can further test the connection by trying to browse the Internet. Launch your web browser (such as Internet Explorer) and see if you can browse a web page.

More Wireless Security Steps

Enabling encryption is the most critical step to securing your wireless network. With that completed, there are a couple more simple steps you can take to make your wireless network secure. These steps by themselves will not provide bullet-proof security, but they do add to the security you have just implemented and they only take a few moments each to implement. First, we can stop "advertising" to other wireless NICs. Then, we can make sure the firewall function is enabled on the wireless router. Finally, we can make sure our NICs do not unintentionally roam to other wireless routers. These steps are discussed in the next few sections.