BRITISH LIBRARY

Christina Belisario
Research Coordinator
Morrison Foerster
12531 High Bluff Drive
San Diego, CA 92130-2040
USA

17 October 2025

Dear Christina

Wireless Home Networking Simplified by Jim Doherty and Neil Anderson – Cisco Press, Inianapolis, 2007. Shelf mark: YK.2007.b.1648

According to our records, this item was receipted by The British Library on **16 January 2007** and would have been available for public use from that date.

A copy of the pages with date stamp indicating the date of availability, title and contents pages has been attached. Also additional pages as requested.

Please note that we can only provide the date that the British Library made this item available for public use; for the actual date of publication, please contact the publisher.

Yours sincerely

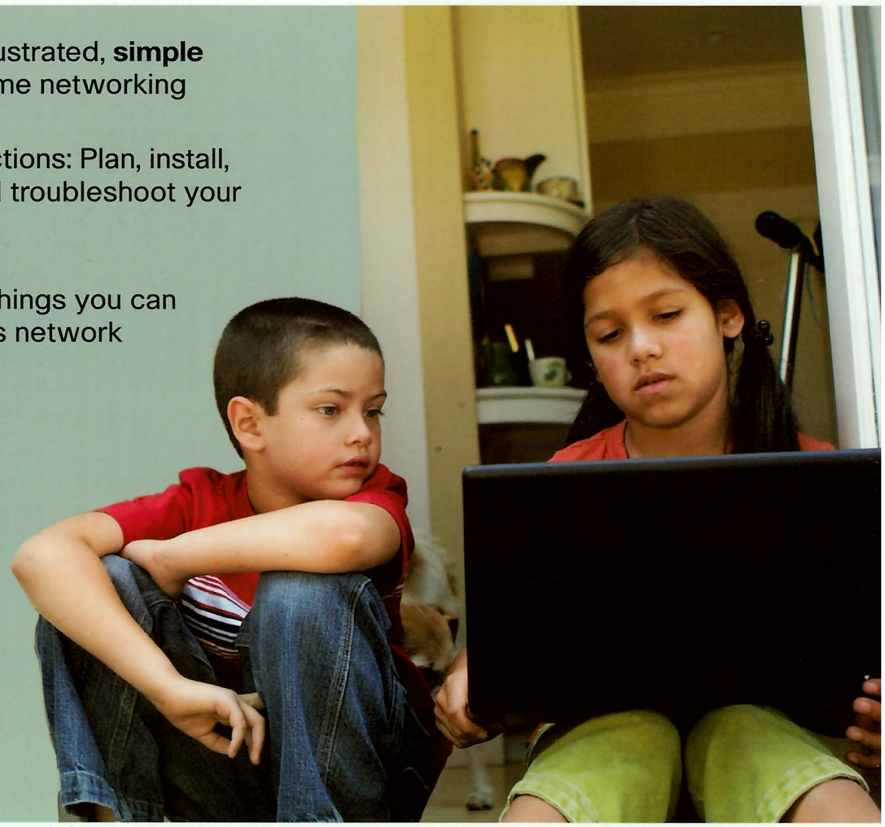
Tony Corsini

British Library Research Service
Tel: +44 (0) 20 7412 7903 bipc-research@bl.uk

cisco

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



ciscopress.com

Jim Doherty
Neil Anderson

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.



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

Amazon EX1038 Page 4

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

Amazon EX1038 Page 5

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

Amazon EX1038 Page 6

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

Amazon EX1038 Page 7

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

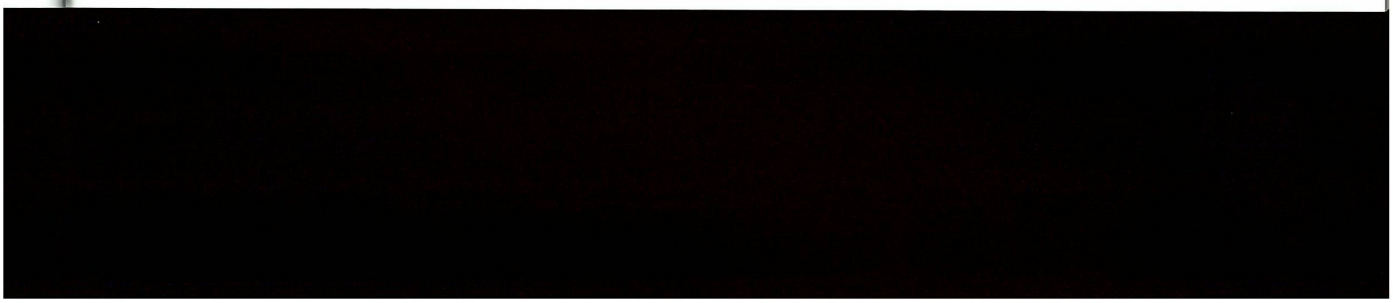
Wireless Connection Made 216

Amazon EX1038 Page 8

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



Amazon EX1038 Page 9

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.

Amazon EX1038 Page 12

CHAPTER 1

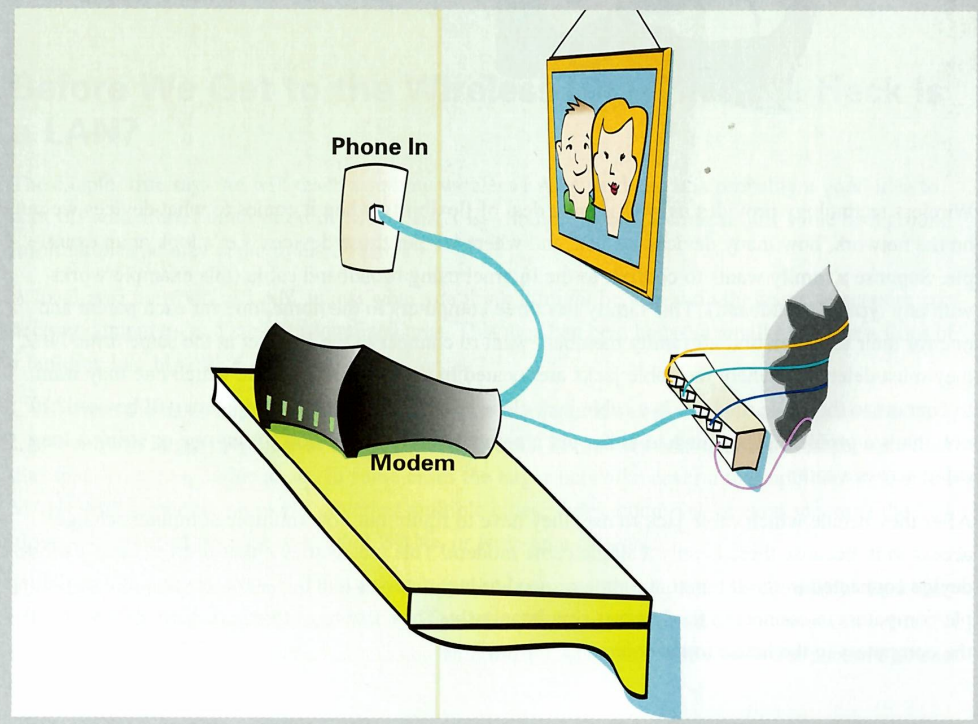
How Wireless LANs Work

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.



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.

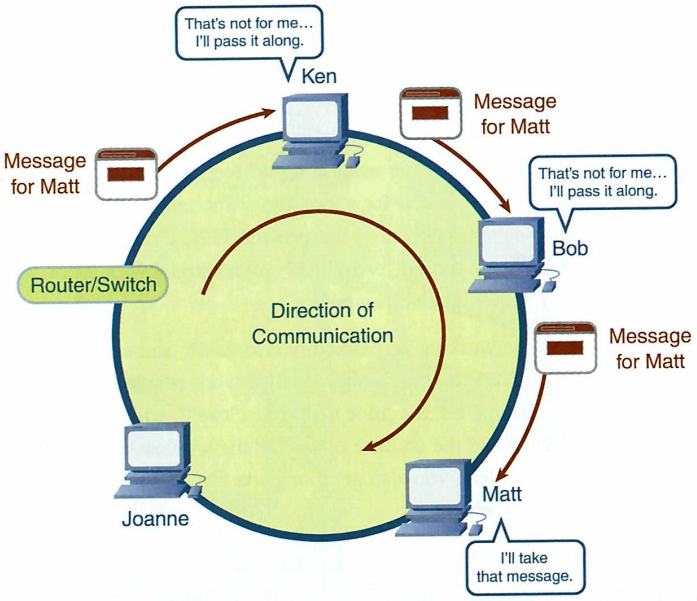
LANs form the basic building blocks of large-scale computer networks. LANs connect to other LANs to form larger corporate or institutional networks. These networks connect to larger networks that span large geographic areas. In some cases the larger networks cover a metropolitan area, called MANs. Still 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.

Amazon EX1038 Page 14

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).

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

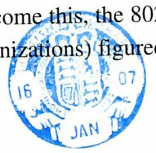
- **Interference**—Because many other devices use the open frequency bands (including cordless phones and baby monitors), anything using these bands is prone to interference from other devices.
- **Power and range**—The rules for the open frequency band limit the power of transmissions. The problem here 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



Amazon EX1038 Page 16

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.

Amazon EX1038 Page 17

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

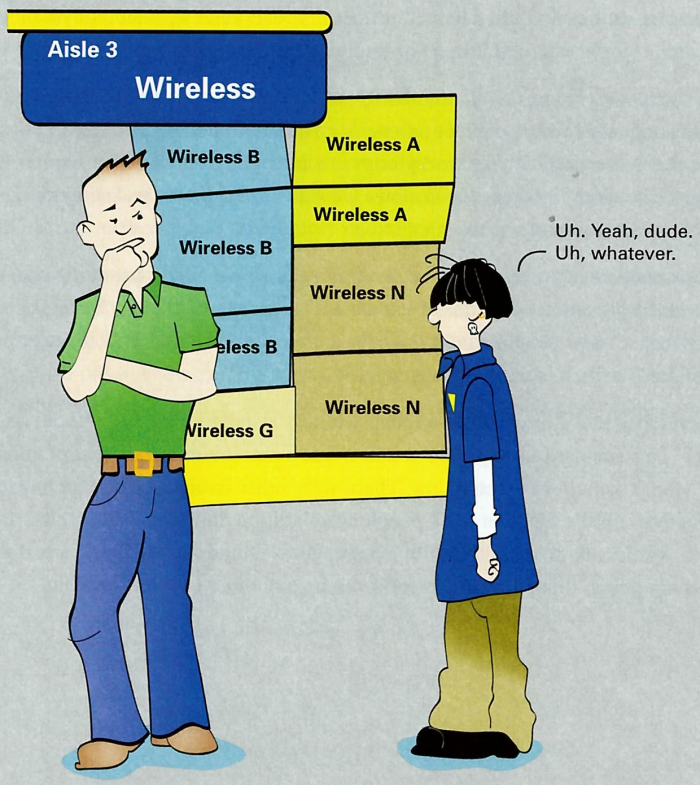


Table 2-1 802.11a Summary

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.

Amazon EX1038 Page 19

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.

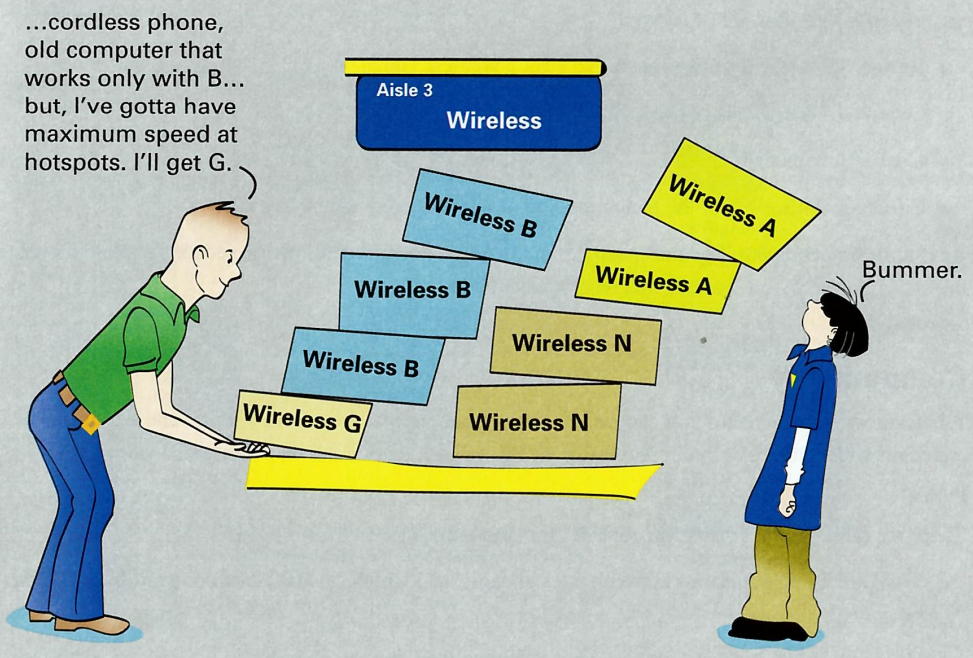
Therefore, we recommend you stick with one of the standards and be wary of proprietary manufacturer extensions.

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.



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.

Amazon EX1038 Page 22

CHAPTER 4

Planning Your Wireless Network

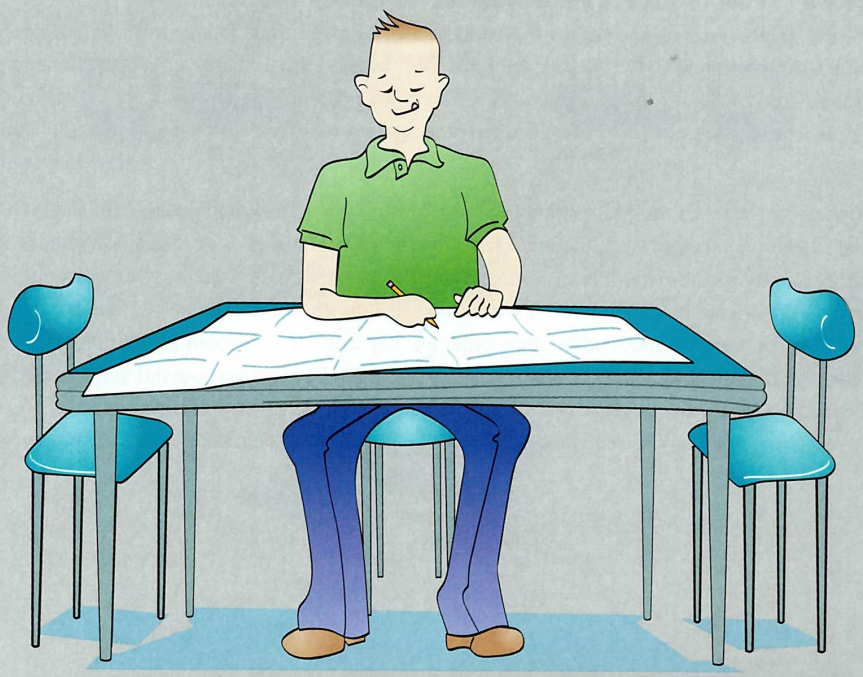
The first step in building your wireless network is to sit down and do some planning. Sure, it's fun to run out and start buying stuff, but a little time spent up front will save you a lot of frustration and rework time later.

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



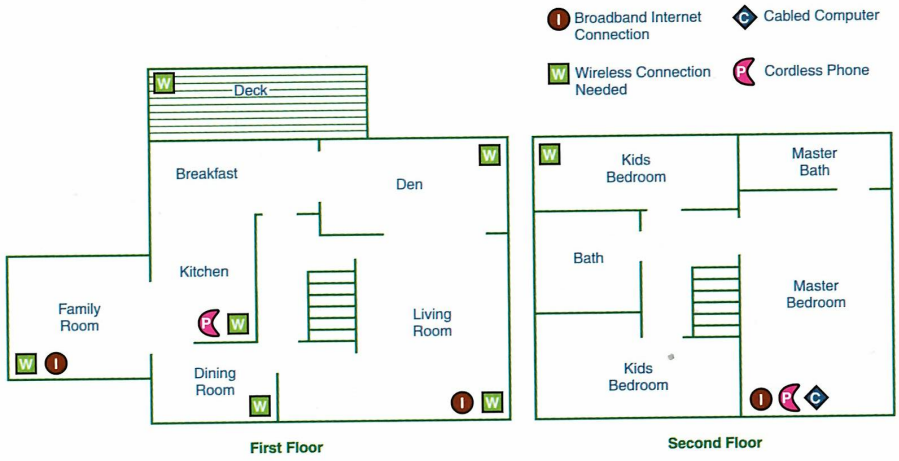
Next, put a mark in the rooms where you are likely to have a desktop computer, or other wired device such as a storage server, or network printer. In Figure 4-3, we used a blue diamond with a *C* in it to denote where we want to have a wired network connection, like a desktop computer.

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



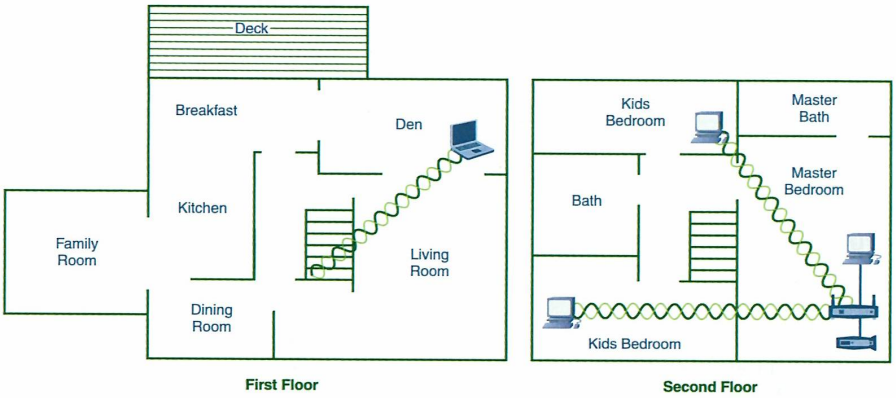
From the sketch, you can make some decisions about where you will put your wireless router, which computers will have wired connections, and which computers will have wireless connections.

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

Amazon EX1038 Page 25

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.

Amazon EX1038 Page 26

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

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.



Figure 7-28 EasyLink Graphical View of Your Network

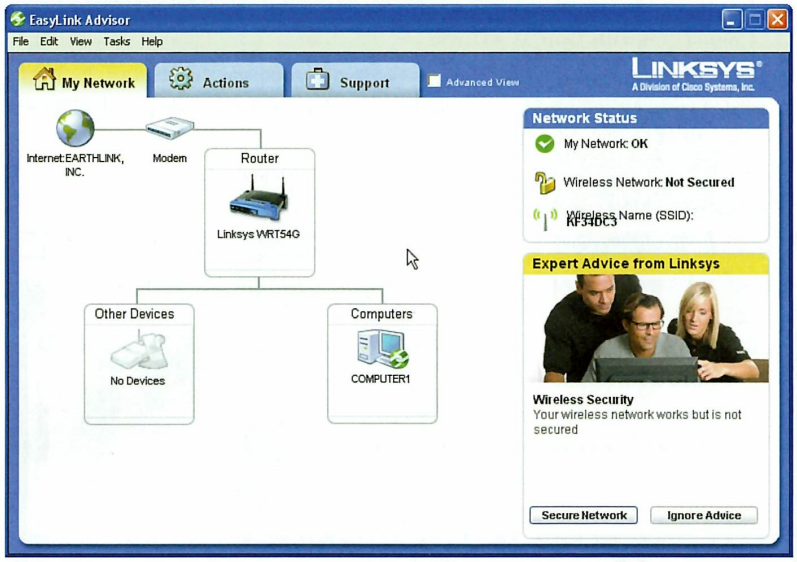
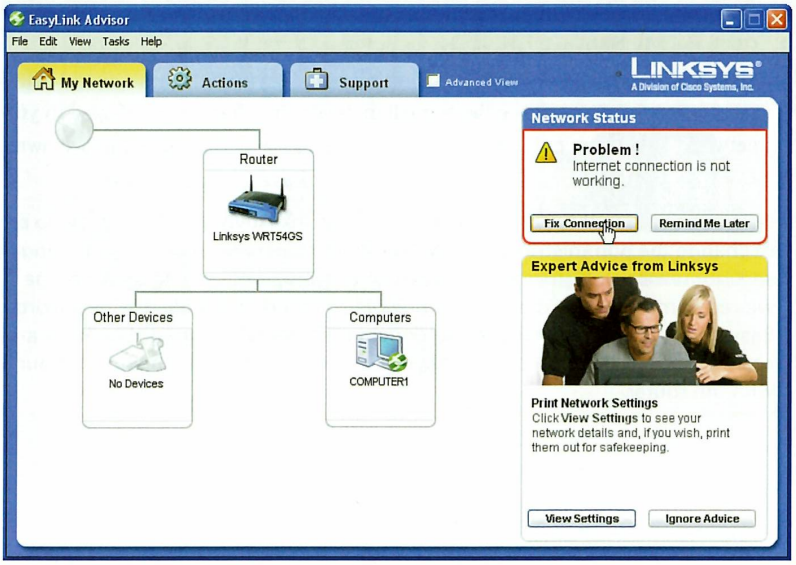


Figure 7-28 shows what the initial network should look like if things are working properly, including connectivity to the Internet. EasyLink Advisor can also help troubleshoot when something is not quite right. If, for example, the Internet connectivity is not working properly, EasyLink tells you, as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

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



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

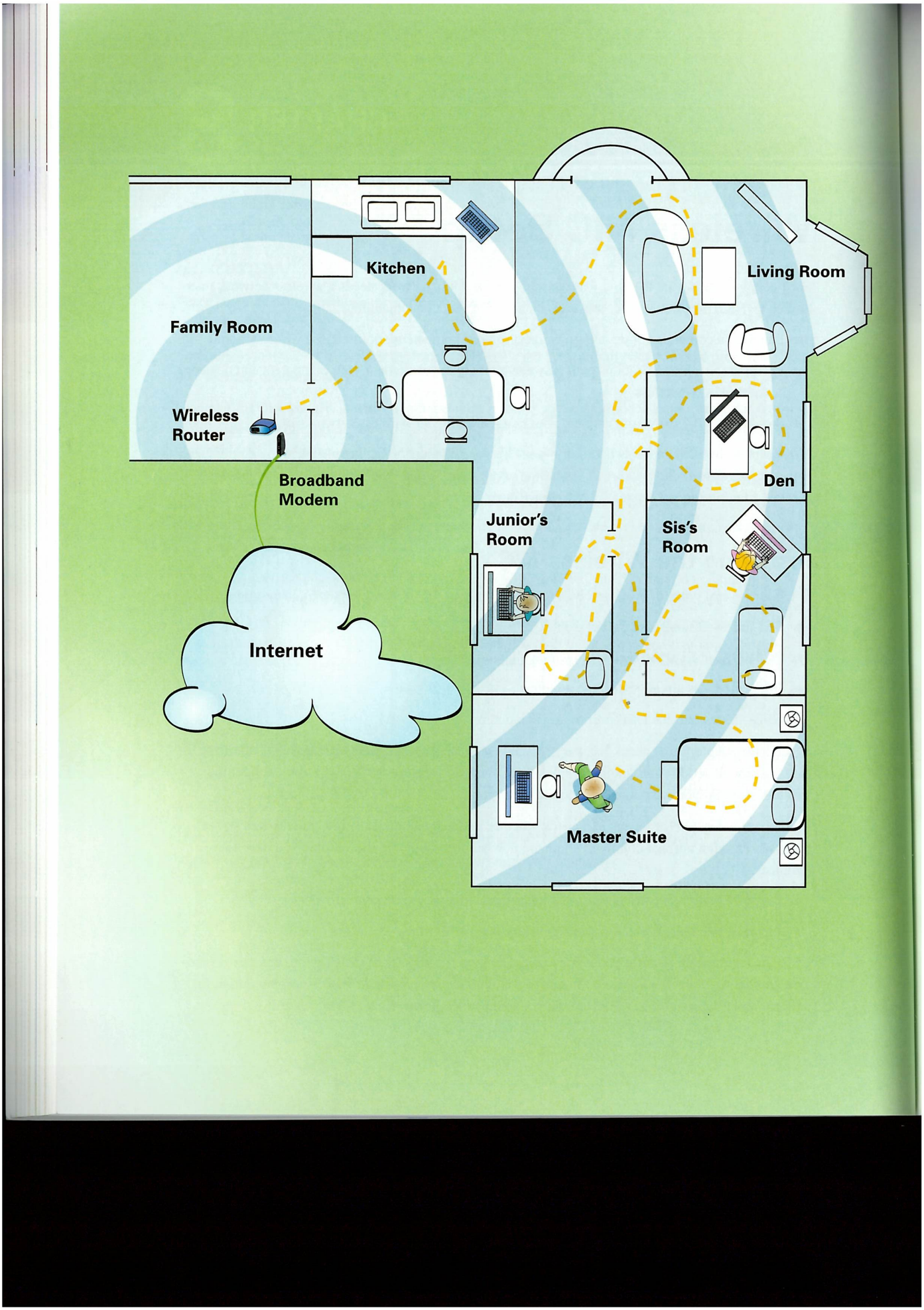
- **PCI card**—Installs inside a desktop PC
- **PCMCIA or ExpressCard**—Plugs into a laptop
- **Integrated**—Is already built into a laptop
- **USB**—Plugs into the USB port of any computer

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

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

Amazon EX1038 Page 32

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.

Step 2 Make sure that only your wireless network profile appears in the Preferred Networks list. If other networks are listed that you do not recognize, delete them.

Step 3 Click the **Advanced** button. Click **Access Point (Infrastructure) Networks Only** and make sure that Automatically Connect to Non-Preferred Networks is *not* checked (see Figure 9-62).

Figure 9-62 Verify Network Access Settings



Step 4 Click **Close** and then click **OK**.

Now, if the wireless NIC sees your neighbor's wireless router, it will not try to connect to it because it is not in the list of preferred networks. Similarly, if we encounter another computer with a wireless NIC that attempts to set up an ad hoc connection, our wireless NIC will not respond to the attempt, keeping our wireless network (and laptop) secure.

MAC Address Locking

One additional wireless security measure that you can take that has not yet been discussed is MAC address locking (often called MAC address filtering). Because each wireless card has a unique identifier called a MAC address, we could instruct the wireless router to accept connections only from the wireless cards that we know. This is called *MAC address locking*.

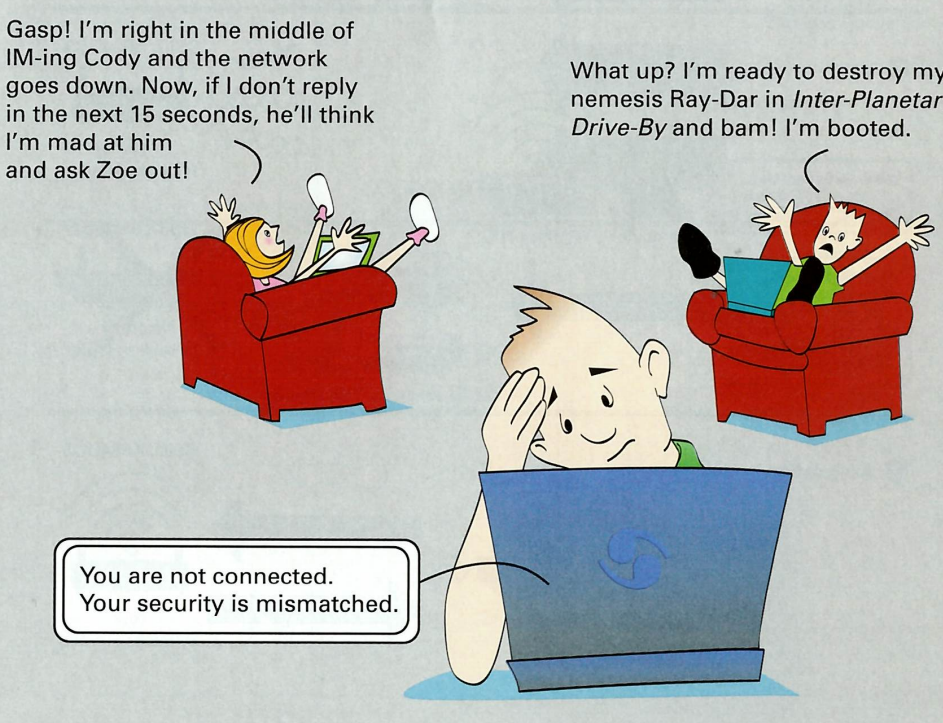
Turning on MAC address locking is not trivial and can be a bit of trouble. Remember, with every security measure enabled, you typically lose some flexibility. For example, with MAC address locking enabled, you need to change the configuration on the wireless router if you buy a new wireless card or device. Also, if you have visitors who want temporary Internet access, you would have to grant them access by adding their MAC address to the permission table. MAC address locking does provide an additional level of protection. If you want to enable it, see Appendix A, "MAC Address Filtering."

CHAPTER 10

Troubleshooting: I Can't Connect at All

Usually, wireless networks are pretty easy to set up and connect to, but, as we said earlier, due to the fast-moving nature of the technology, sometimes the network does not work as it is supposed to. In this chapter we will cover what to do if you cannot get a computer or laptop to connect over the wireless connection to the wireless router. Start here if you cannot get the computer and router to connect at all. If you can connect sometimes but not others, skip to the next chapter.

Before jumping into troubleshooting, let's first take a look at what happens during the steps when your wireless NIC connects to your wireless router and at what can go wrong during that process.



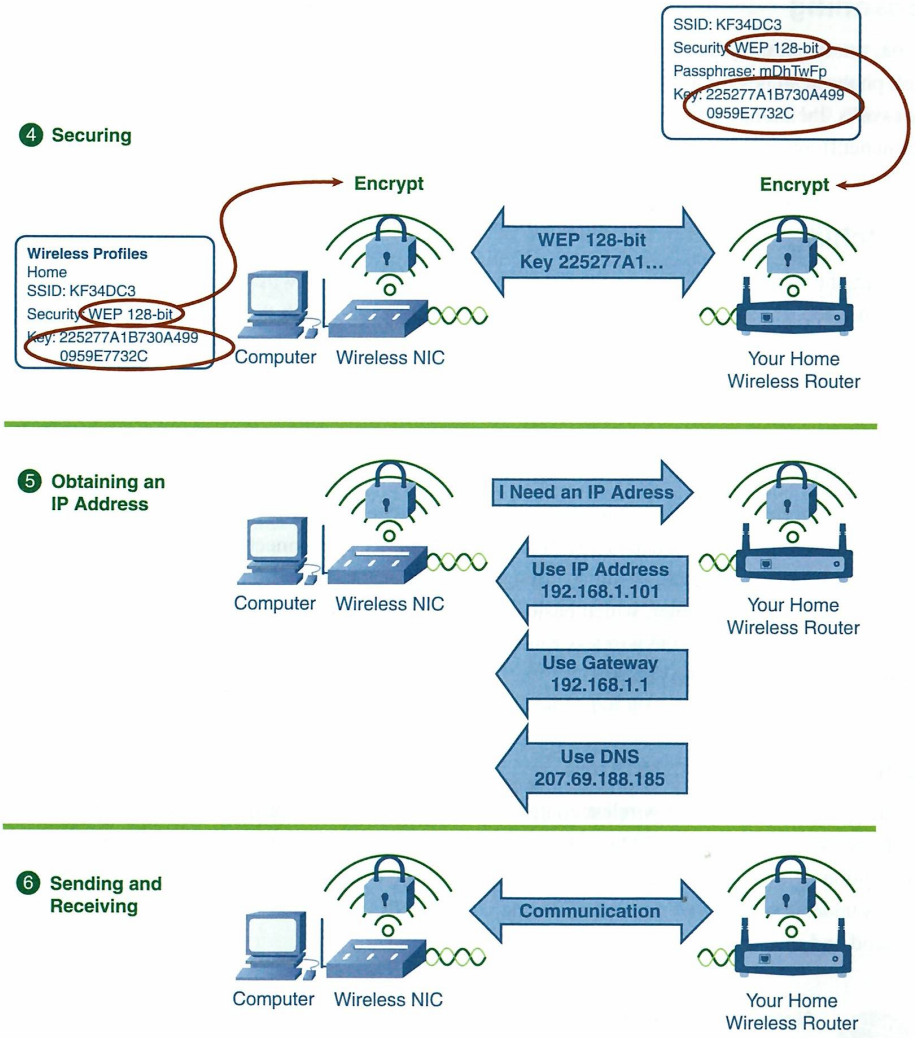
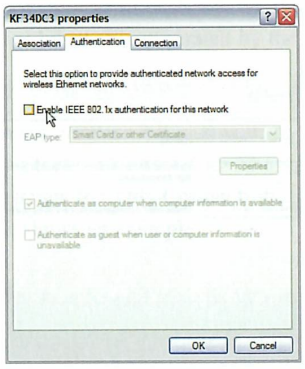

SSID: KF34DC3
Security: WEP 128-bit
Passphrase: mDhTwFp
Key: 225277A1B730A499
0959E7732C
4 Securing
Encrypt
Encrypt
Wireless Profiles
Home
SSID: KF34DC3
Security: WEP 128-bit
Key: 225277A1B730A499
0959E7732C
WEP 128-bit
Key 225277A1...
Computer
Wireless NIC
Your Home
Wireless Router
5 Obtaining an
IP Address
I Need an IP Adress
Use IP Address
192.168.1.101
Use Gateway
192.168.1.1
Use DNS
207.69.188.185
Computer
Wireless NIC
Your Home
Wireless Router
6 Sending and
Receiving
Communication
Computer
Wireless NIC
Your Home
Wireless Router

Figure 10-43 Verifying the Authentication Setting in Windows XP



IP Address Assignment–Related Issues

After you have confirmed that the wireless NIC is now making a connection properly to the wireless router, including encryption, it's time to move on to the last step in the connection process: obtaining an IP address. Joining the wireless network allows the NIC to send and receive packets to and from the router. To be a part of the home network, the NIC also needs an IP address.



Note: IP addressing is a fundamental networking concept that is not covered in detail in this book. The 30-second description is that each device (computer, laptop, and so on) in a home network needs to have an IP address, which is how the device is known on the network. IP addresses have four numbers, separated by a dot (.). Most home networks use IP addresses in the range of 192.168.1.100 to 192.168.1.149, and the router assigns each device an address from this pool when it boots. This is called *dynamic IP addressing*, or Dynamic Host Configuration Protocol (DHCP). To learn more about how IP addressing works, pick up a copy of *Home Networking Simplified*.

With dynamic IP addressing, or DHCP, enabled on the wireless router, when a NIC establishes a new wireless connection, it then requests an address from the router, and the router assigns the next available one from the pool. The wireless NIC can then use the address until the computer is shut down or the laptop leaves the wireless network.

Why would an IP address not be assigned correctly? There is not really a good reason; let's just say that DHCP does not seem to always work properly. Sometimes a wireless NIC gets "stuck," thinking it already has an IP address (maybe from the last network it joined). Also, in very weak signal conditions, the request could get lost, never reaching the router.

On the router side, it's also possible that all the available IP addresses in the pool have been assigned. This is usually not the case, but, depending on how many devices you have on your home network and the size of the address pool, it could be an issue. Occasionally, if one or more devices are having an intermittent connection issue in which they keep losing the signal and then coming back onto the network, they could be requesting a new IP address each time, and the router could exhaust its pool.

Finally, depending on the wireless NIC, sometimes with WPA encryption, if the WPA key does not match, the NIC will appear to connect to the wireless signal just fine but will not be able to properly

acquire an IP address from the router. In other words, it looks like a DHCP problem, but it's really a mismatched WPA key.

It's important to be able to recognize when a problem with the IP address assignment is happening, and you may be able to take some actions to remedy the problem. The next few sections give some tips.



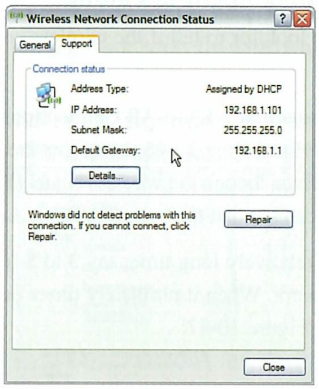
Note: Static IP addressing, which is when you turn off DHCP and assign your home network addresses manually, is quite problematic. Problems include duplicate addresses, errors in manually entering IP addresses, and others. We do not recommend using static IP addressing in home networks. If you do, prepare yourself for some frustration.

Determining if an IP Address Is Assigned

You first need to figure out whether you are getting an IP address assigned. Here is how to tell.

If you are using the Windows Wireless Network Connection utility, choose **Start > Connect To > Show All Connections**. Select the wireless NIC and then right-click and select **Status** from the list. Click the **Support** tab. Figure 10-44 shows an example.

Figure 10-44 Verifying IP Address Assignment with Windows XP



In Figure 10-44, we can see that the IP address 192.168.1.101 has been assigned to the wireless NIC. We can also see that a default gateway IP address has been assigned, 192.168.1.1. This is good. We have both an IP address to use for the NIC and a gateway to which to send requests to access the Internet. This should be a complete connection now for us to access the Internet from the laptop or other computer that is connected over the wireless connection.

If you are using the Linksys WLAN Monitor utility, double-click the icon on the desktop to launch the utility or choose **Start > Programs > Linksys Wireless Card > WLAN Monitor**. Click the **More Information** button on the Link Information tab. Figure 10-45 shows the resulting link information.

Amazon EX1038 Page 38

CHAPTER 11

Troubleshooting: I Can Connect Sometimes

Sometimes, your wireless network works well when you set it up, but then when you try to use your laptop over a wireless connection, say in the living room, it does not always connect. You might be experiencing a wireless signal coverage issue. Before assuming so, make sure you have successfully connected your computer to the router via a wireless connection at least once, even if your computer is right beside the router.

If you have never connected to the wireless router successfully, start with Chapter 10, "Troubleshooting: I Can't Connect at All." If you have connected before but are not able to use the wireless network in locations inside your house where you want to, take a look at the rest of this chapter.

How Wireless Coverage Works

Wireless networks are similar to cell phone networks:

- The more bars of service you have, the better the call sounds.
- When you have very few bars of service, you may be able to place a call, but it probably does not sound very good.
- When you have zero bars of service, you cannot make or receive calls.

Wireless networks operate the same way, as shown in Figure 11-1. When you are within the coverage area of your wireless network and have good signal strength (shown in the green area), you will have a good wireless connection and also have at or near the maximum data rate your wireless router supports (54 Mbps for 802.11g, 108 Mbps or higher for 802.11n, and so on).

Table 11-4 Five Simple Guidelines for Wireless Router Location

Do	Don't
Choose a site for the router in a central location in your house, considering all three dimensions (see Figure 11-9). Note the bigger the house, the more important this becomes.	Put the router in the basement, attic, garage, closet, or other isolated part of your house.
Place the router on a wooden table or desk where the router (and especially the antenna) is not obscured.	Place the router on the floor, in a metal bookcase, in a metal enclosure, or in a drawer.
Keep away from potential interfering devices like microwave ovens, cordless phones, and baby monitors.	Keep a cordless phone base or handset next to the router.
Plug into a power strip with a surge protector, and plug the power strip into an empty outlet.	Plug into an outlet along with other electrically "noisy" devices, such as hair dryers, blenders, toasters, and so on.
Keep the antennas free from obstructions, including wires and cables.	Drape electrical cords or cables over the router or antennas, or wrap extra wires around the antennas.

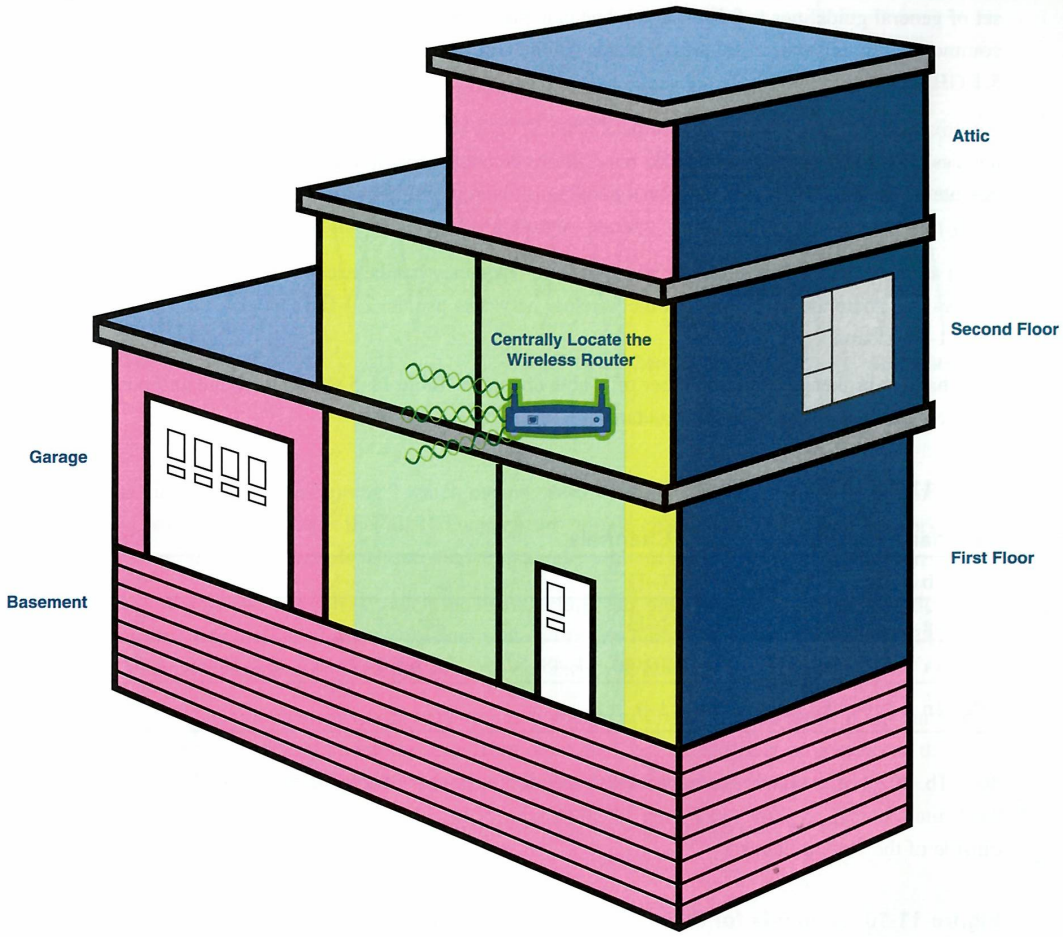


Note: We omitted some pretty obvious guidelines from Table 11-4, but we have heard of these happening, so they are worth mentioning. The funny part is, you will probably read this and think we are kidding:

- You have to actually remove the router from the store packaging and plug it in somewhere in your house for it to work. It's not so much the shrink wrap that causes the problem, but the lack of electricity is hugely limiting.
- Don't put the router in a wet or damp area. This includes an area where pets are likely to urinate on it. By the way, urination on electrically powered devices, such as routers, can be just as detrimental to your pet as it is to the wireless network.
- Aluminum foil generally does not make a good antenna booster, although there is something to be said for empty Pringles cans, and a lot of "research" seems to have been done in this area.
- Unless specifically designed for use outdoors, the vast majority of wireless routers are for use indoors only, and bad things happen if they get rained on. This is true of most things with an electrical plug, by the way.
- A dark, cool, corner room of the basement or root cellar is a great place to store wine. Great places to store wine are not good places for wireless routers.
- You need to be at *home*, or close by, to use your wireless *home* network. If you are out of state on vacation, it is extremely unlikely you will get a signal from your *home* network.
- You may be tempted to mount your router on the ceiling (like they do in the office), but keep in mind that your office has a false ceiling to allow cable runs and, more importantly, your company has people who do this type of installation for a living. We're not saying it wouldn't be cool to do, but you are signing up for a lot of work (and a mess) if you try this at home.

Amazon EX1038 Page 40

Figure 11-9 Choose a Central Location for the Wireless Router



If you follow the guidelines described in this section, you will get the most coverage from your wireless router. If you do not follow them, and do something like putting the wireless router in a metal bookcase or computer desk cubby hole, no amount of tuning is going to help.

Next, let's move on to some other tips to help you get the most from the wireless network coverage.

Trying Different Channels

Wireless networks operate today in what are called *unlicensed frequencies*. The U.S. Federal Communications Commission (FCC), or the equivalent in your country, manages who uses which radio frequencies for what purposes. For example, television broadcasters, FM radio stations, police and fire radios, and cellular phone companies all must be licensed by the FCC to use a particular set of radio frequencies. If the FCC did not regulate this, no one would be able to rely on such services because everyone would be transmitting all over each other, and none of the services would work very well.

However, the FCC designates certain sets of radio frequencies as unlicensed, and as long as a certain set of general guidelines is followed, anyone can build devices that operate at these frequencies. The common public unlicensed frequency bands (in the United States) are 900 MHz, 2.4 GHz, and 5.1 GHz.

Approximately 5 to 10 years ago, cordless phones, baby monitors, and many other home wireless devices commonly used the 900-MHz band. More recently, most home wireless devices are built to operate in the 2.4-GHz band, somewhat because of overcrowding of the 900-MHz band. Finally, many new devices are being built to operate in the higher 5.1-GHz band.

There are not a lot of differences or advantages to frequency bands, except the number of other devices that share the band. Most home wireless networks use the 2.4-GHz band, with a few built for the 5.1-GHz band.

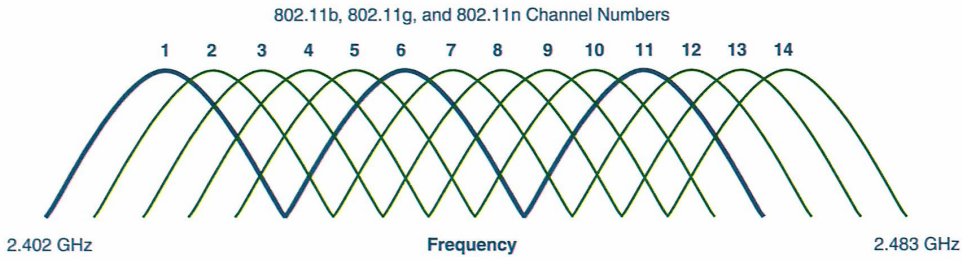
Each band is broken up into a number of usable channels. Table 11-5 shows the band and possible channels for each of the wireless standards.

Table 11-5 Possible Wireless Channels

Standard	Band	Channels	Default
802.11b	2.4 GHz	1–11	6
802.11g	2.4 GHz	1–11	6
802.11a	5.1 GHz	36, 40, 44, 48, 52, 56, 60, 64, 149, 153, 157, 161	52
802.11n	2.4 GHz	3–9	5

802.11b, 802.11g, and 802.11n networks all operate in the 2.4-GHz band. There are 11 channels (in the United States), as shown in Figure 11-10 (Channels 12, 13, and 14 are valid in a few countries outside of the United States.)

Figure 11-10 Channels for 802.11b, 802.11g, and 802.11n Standards



These channels are "overlapping," which means that part of the signal for one channel spills over a bit into the channels above and below it. This means there are three unique channels: 1, 6, and 11. If you have one wireless router using channel 1 and another nearby wireless router on channel 2, these channels partially overlap, so they could cause each other interference.

Amazon EX1038 Page 42

CHAPTER 12

Troubleshooting: I Can Connect, but It's Slow

What if you can connect to your wireless network, it stays connected just fine, but it seems like it is slow? To answer that, we first need to understand what to expect from a wireless network. Is it living up to its potential, or is some problem keeping the network from being as fast as it could be?

A wireless network can be slower than expected for a few different reasons:

- Broadband speed limits Internet access speed
- Operating at a slower wireless standard than expected
- Signal degradation due to interference

We explore each of these possibilities in this chapter.

Is the Broadband Internet Connection the Bottleneck?

There is a lot of competition between wireless home networking equipment makers. As a result, faster and faster wireless routers are all the rage. 802.11b started out with 11 Mbps and then 802.11g (and 802.11a) increased the speed to 54 Mbps. Extensions to 802.11g as well as the newest 802.11n standard are increasing the speed even more to 100 Mbps and beyond.

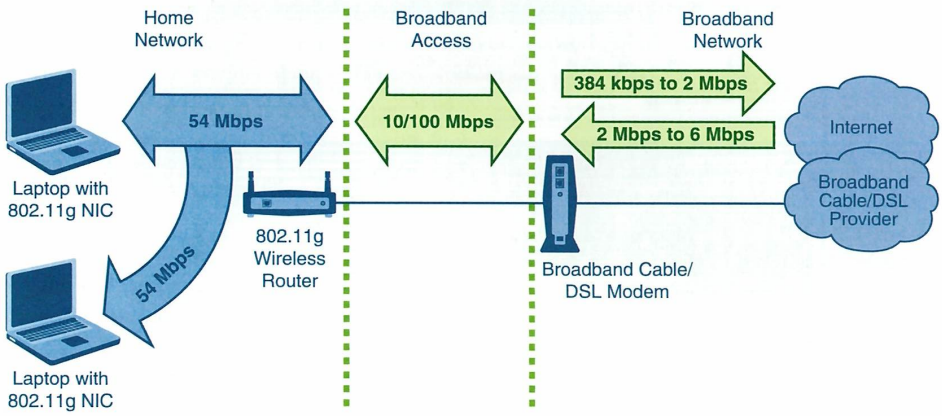


Note: Incidentally, 100 Mbps is the speed of most wired networks today. Some are still 10 Mbps. So wireless networking has caught up to, and in some cases surpassed, wired networking in terms of speed. Wired networking is already starting to move toward 1 Gbps, which equals 1000 Mbps.

So, using a faster router means faster Internet access, right? Well, maybe. The Internet access speed really depends on more factors than just the wireless router speed. Figure 12-1 shows why. We have an 802.11g home wireless network, which provides up to 54 Mbps of speed. This means that within the home network, computers and devices can communicate with each other pretty fast. But when accessing the Internet, the speed is limited by the broadband connection to your house in most cases rather than by your router. The speed between the wireless device and wireless router stays the same, 54 Mbps, but the broadband services today typically only offer in the neighborhood of 384-kbps to 2-Mbps uplink speed (toward the Internet) and between 2-Mbps and 6-Mbps downlink speed (from the Internet).

Amazon EX1038 Page 43

Figure 12-1 Networking Speeds Inside and Outside the Home Network



The point is that buying a wireless router capable of 54-Mbps or 100-Mbps speeds does not mean that you get that speed when accessing the Internet. You are limited by the broadband speed.

Checking the Broadband Connection

Sometimes, you can experience issues with your broadband connection that cause your service speed to be slower than you are paying for. This can be caused by an intermittent connection or wiring problem, as well as just general congestion on the broadband service.

We can check whether the router seems to have a good connection to the broadband service. Linksys routers have a built-in utility called *ping* (Windows XP also has this utility) that you can use to perform a rudimentary connection test.

Access the wireless router using an Internet browser. Click the **Administration** tab and then click the **Diagnostics** subtab, as shown in Figure 12-2. Click the **Start to Ping** button.

The wireless router creates and sends a number of test packets to the address in the IP or URL Address field, measuring the success rate and time it takes to receive a response. The results displayed appear similar to the example shown in Figure 12-3.

CHAPTER 13

Wireless Video and Entertainment

Now that we have a well-functioning, secure wireless network, what do you do with it? Well, lots. You can of course use it to surf the Internet and read your e-mail from the back deck. But there is a lot more you can do.

One general category is wireless video and entertainment, including wireless video cameras, media gateways that can display pictures and send music to your TV entertainment system, online gaming, networking your digital video recorder (DVR), and wireless digital jukeboxes.

We cannot begin to cover all the things you can do with your wireless network here, but let's take three pretty cool things to do and see how you would set up and use them:

- Wireless video cameras
- Online gaming
- Networking a DVR, like a TiVo

The network capacity (or bandwidth) within your home network is much greater (three times or more) than the fastest upload/download speeds you will get from your high-speed connection to the Internet. All this excess capacity exists on your home wireless network because many in-home applications—including the three described in this chapter—typically require more bandwidth than is required for Internet browsing or e-mail. This chapter shows you how to set up these three options in your network.

Wireless Video Cameras

Once limited to very expensive closed-circuit television (CCTV) systems, video cameras for fun or for surveillance are now pretty affordable. If you already have a wireless network in your home, a decent wireless video surveillance system costs you only $100 or so. (We say "only" because a basic CCTV system costs more than $1000.)

Wireless video cameras have all sorts of practical uses, including home surveillance for security and nanny cams.

Finding Uses for Wireless Video Cameras

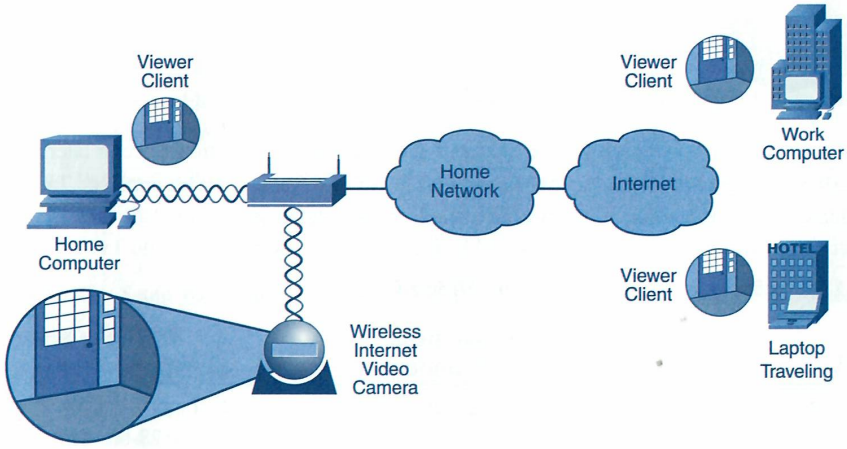
Video cameras that attach to computers are very common, usually used for communicating with other people that have similar video cameras. Also popular recently have been very inexpensive wireless cameras that can be placed anywhere in your house.

The ability to use either of these video cameras for live surveillance while you are not at home is limited. However, newer products like the Linksys wireless Internet video cameras have several distinct advantages:

- No computer is required for them to operate, so they can be located anywhere in your house (or outside, for that matter) where there is an electrical outlet.
- Images from the camera are viewable with any computer from inside your house, or from anywhere outside your house where there is Internet service.

In Figure 13-1, we placed a wireless Internet video camera in a house with a view of the front door.

Figure 13-1 Home Surveillance Using a Wireless Internet Video Camera

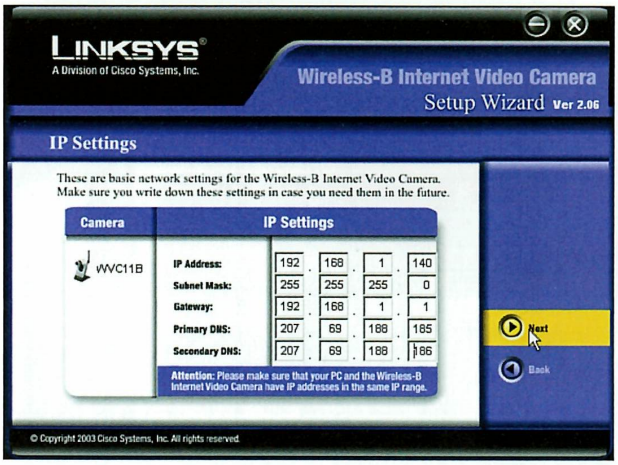


Now, we can use a viewer client to view the real-time video feed. So from upstairs, we could check who is at the front door. We could also use the viewer client on a computer at work to periodically check the residence or to see that the kids got home at the expected time from school. In a similar way, you could even use your laptop to check on the house while traveling on business.

To avoid the need for constant surveillance, you can set up the camera to act as an automated sentry, and notify you only when there is something worth seeing.

You can program the camera to send a signal to a pager, cell phone, or e-mail account to notify you if motion has been detected. You can even have the camera send you a video clip that it captures of the event.

Figure 13-5 Configure the IP Address Settings





Note: The IP address you choose needs to be in the range of IP addresses for your home network. In Chapter 7, "Wireless Router Setup," we set up the router to use the address range 192.168.1.2 through 192.168.1.254 for our home network (.0, .1, and .255 are reserved). In addition, we set up the router to dynamically assign IP addresses in the range 192.168.1.100 through 192.168.1.149 to computers and devices requesting an address.

The IP address just needs to be unique on the network and within one of these ranges. We chose 192.168.1.140 for this example. Whatever address you choose, write it down, because this will be the address needed when accessing the camera. If you forget the address, you probably have to do a factory reset and start over.

Step 9 The next wizard page asks if your network is ad hoc or infrastructure (meaning based on a wireless router). Select **Infrastructure** and click **Next**.

Step 10 Enter the SSID for your wireless network (see Figure 13-6). For this particular example, the home network is using an SSID of J59wgh21MX. Click **Next**.

Step 11 Set the wireless security setting to **WEP 128 Bit Keys** (or the encryption you are using), as shown in Figure 13-7. Enter the WEP passphrase for your wireless network. In this example, the WEP passphrase is 64Gx3prY19fk2. Click **Next**.

After completing these steps, you can reach the video camera from outside the home network.



Note: You can also use the Linksys Viewer Client to view video images over the Internet. The details of this process have been omitted here to save space. The procedure is very similar to using the Viewer Client from within your home network, as previously described. The major differences are

- Click **Internet** instead of **LAN**.
- Specify the Internet IP address.
- Specify the port number (for example, 63333).

Problems with Viewing Video over the Internet

There is one other potential issue with viewing your video over the Internet. The broadband networks typically assign a dynamic IP address to your broadband service. *Dynamic* means the IP address can change, typically only if you power off and on your broadband modem. This is usually not an issue because, typically, you will be assigned the same IP address for a long period of time.

If the IP address of your broadband modem does get reassigned, the new address may not match the address you wrote down for the camera. Then, when you try to access the camera, you will get an error message from the Internet browser saying "The page cannot be displayed." In this case, you need to access your wireless router, click the **Status** function, and write down the new Internet IP address.

If you rely on accessing your camera over the Internet, and the IP address changes too often, here are a couple of solutions:

- Subscribe to a dynamic DNS service that automatically tracks your home network's IP address. Linksys offers a pay service called SoloLink. This service automatically tracks the address used to reach your video camera. (See http://www.linksys.com/sololink/. Further detail on dynamic DNS services is beyond the scope of this book.)
- Inquire with your ISP about upgrading your broadband subscription to a static IP address, which means that you pay a little extra per month, but your address never changes.

Using the Video Camera as a Motion Detector

Another very useful feature of the Linksys wireless Internet video camera products is the ability to act as a motion detector for active surveillance. Watching a video feed for hours waiting for something to happen is tedious. Depending on the reason for the video camera, it can be more effective to trigger on motion detected and then perform a notification action. Setting up the motion detector is pretty easy:

Step 1 Access the video camera using the administrator account. Click **Setup** and then click **Advanced**. Check the **Send E-Mail Alert when Motion Detected** check box (see Figure 13-22). Select a length in seconds for a video capture (2–5 seconds). Select the minimum time between e-mail alerts (2–30 minutes).

Amazon EX1038 Page 48

CHAPTER 15

The Future of Wireless Networking

The future of technology is always difficult to predict. Usually you get some pretty generic statements that do not really tell you anything, or wild predictions that are usually wrong and provide little insight for those trying to figure out if the $400 worth of stuff they just bought is going to be useless a year from now.

In this chapter, we try to give you some points to think about regarding where this technology is going in the near future (which we see as being 2 to 5 years out). We hope to avoid being too generic or making any wacky predictions. We see wireless networking evolving as follows:

- Wireless networks will be faster.
- Wireless networks will go farther.
- Wireless networks will be in more places.
- Wireless networks will move with you.
- More devices will connect to wireless networks.

This chapter explores each of these, including how it will affect your network and the stuff you just bought.

Wireless Networks Will Be Faster

There is no doubt that wireless users are addicted to speed. With perhaps the sole exception of security improvements, speed is where most of the R&D and engineering dollars get spent in companies that provide wireless equipment. The interesting thing is that most people's high-speed Internet connection is slower than the slowest wireless standard currently on the market (which is being phased out because consumers are demanding the faster standards).

Paying for extremely high speeds doesn't make sense unless you are using wirelessly enabled computers where the connections are faster (perhaps at the office or Internet cafés) or if you are using bandwidth-intensive applications within your network, such as music or video servers or head-to-head video or computer games. The funny thing is that most wireless users are not doing this, but folks are addicted to speed whether they are on the road or on their own network.

So, how fast will wireless home networks get? We are already up to 100 Mbps. That is as fast as most corporate wired computer networks have been for a couple of years. The next big jump would

Amazon EX1038 Page 49

By the way, some airlines (such as Germany's Lufthansa) offer Internet access on their flights today via satellite link, and more are expected to follow.

More Devices Will Connect to Wireless Networks

Probably the most significant change impacting wireless networks will be the number and types of devices that connect to it. A number of new devices have already come out, but these are network-specific types of gear like print servers and such.

In the next wave, we see all types of devices connecting to the network, including some obvious devices such as TVs, stereos, and digital recording devices (DVRs), but also appliances, home security systems, and electronics that can control home lighting, sprinkler systems, air conditioning, and answering machines.

Connecting these devices will have some pretty important implications on security and processing requirements for your wireless router. Because most routers are underutilized today, the processing power required should not be an issue. Even if processing power were an issue today, it wouldn't be an issue in 3 to 5 years given the pace of technology. Security is particularly important because in this scenario a hacker could really mess with you.

Having a handle on how this technology really works is also important. If you think it was annoying when the clock was blinking 12:00 on your VCR for 5 years, just wait until you have to upgrade the firmware on your toaster. That said, as manufacturers make it easier to connect, secure, and use this technology with tools such as EasyLink Advisor, adoption will increase.

Summary

This chapter provided not so timid but not too crazy predictions on where wireless networks are going. The capability for everything we mentioned in this chapter exists today. The issue is that the technology is too expensive. Technology costs are dropping all the time, however.

The real determining factor with wireless (and all technology for that matter) is its usefulness to the average consumer or business user. It is a rare event when a technology is broadly adopted within 5 to 10 years of its discovery. In fact, the history of fax machines, cellular phones, and the Internet suggests that the new technology adoption time frame is closer to 25 years than to 5. There are a lot of great "solutions" out there waiting for the right problem to come along. The day that the public demands wireless networking that is faster, goes further, exists in more places, moves with you, and connects to more stuff is the day someone will be standing there with a box that does it.

Where to Go for More Information

The Michael Grebb article for Wired is called "Cities Unleash Free Wi-Fi." You can find it at Wired.com: www.wired.com/news/technology/technology/wireless_special/0,68999-0.html.

Amazon EX1038 Page 50