Making Everything Easier!™

2nd Edition

Wireless

ALL-IN-ONE

FOR DUMMIES®

8 BOOKS IN 1

- Pulling the Plug
- Planning Your Network
- Configuring Networks
- Security and Troubleshooting
- On the Road
- Networking Technologies
- Home Technology
- Global Positioning Systems

Sean Walberg
Loyd Case
Joel Durham Jr.
Derek Torres

Get More and Do More at Dummies.com®

Start with **FREE** Cheat Sheets

Cheat Sheets include

- Checklists
- Charts
- Common Instructions
- And Other Good Stuff!

To access the Cheat Sheet created specifically for this book, go to
www.dummies.com/cheatsheet/wirelessaio

Get Smart at Dummies.com

Dummies.com makes your life easier with 1,000s of answers on everything from removing wallpaper to using the latest version of Windows.

Check out our

- Videos
- Illustrated Articles
- Step-by-Step instructions

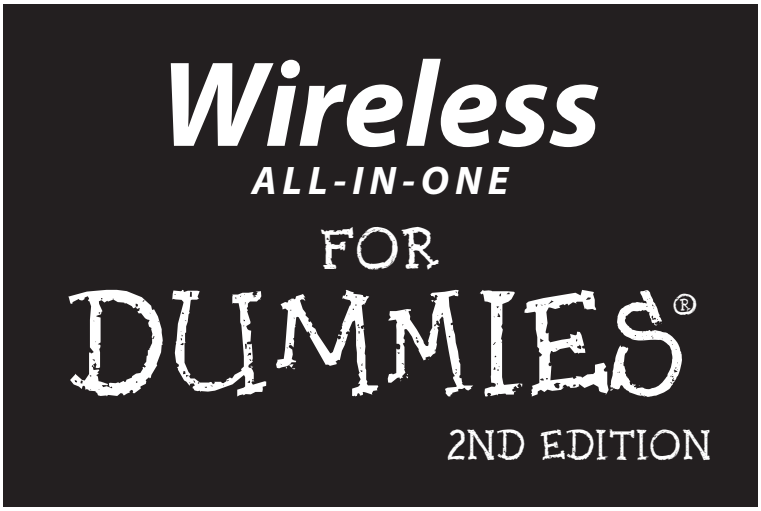
Plus, each month you can win valuable prizes by entering our Dummies.com sweepstakes. *

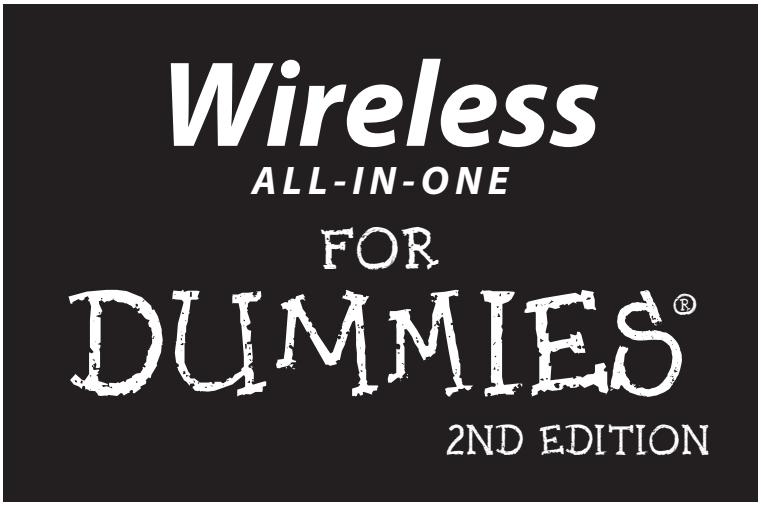
Want a weekly dose of Dummies? Sign up for Newsletters on

- Digital Photography
- Microsoft Windows & Office
- Personal Finance & Investing
- Health & Wellness
- Computing, iPods & Cell Phones
- eBay
- Internet
- Food, Home & Garden

Find out "HOW" at Dummies.com

**Sweepstakes not currently available in all countries, visit Dummies.com for official rules.*


Wireless
ALL-IN-ONE
FOR
DUMMIES®
2ND EDITION



Sean Walberg, Loyd Case,
Joel Durham, Jr.
and
Derek Torres

Wiley Publishing, Inc.

Wireless All-in-One For Dummies,® 2nd Edition
Published by
Wiley Publishing, Inc.
10475 Crosspoint Boulevard
Indianapolis, IN 46256

www.wiley.com

Published by Wiley Publishing, Inc., Indianapolis, Indiana

Published simultaneously in Canada

Library of Congress Control Number: 2009939356

ISBN: 978-0-470-49013-6

Manufactured in the United States of America

10 9 8 7 6 5 4 3 2 1

Dedication

To Rebecca, my wonderful and supportive wife — Sean Walberg

To Pablo, Victor-Emmanuel, and Anne-Claire — Derek Torres

I dedicate my portion of this book to Matt Firme — Joel Durham

About the Authors

Sean Walberg has been a network engineer for nine years. He's been in the information technology field since 1994 and has worked on development, technical support, systems administration, and network engineering.

When not working, you can find Sean playing with his three energetic sons or in the kitchen cooking.

You can find Sean's contact information and links to other writing at `http://seanwalberg.com`.

Derek Torres is an author and technical communicator. He has extensive experience working for software companies in the United States and in Europe. He has authored or coauthored several books on Windows operating systems and, most recently, BusinessObjects XI Release 2 For Dummies. He is currently based in Paris, France.

Joel Durham is passionate for all things technological. Whether it's a multimillion transistor integrated circuit or a really cool mouse, Joel has a deep desire to check it out. This personality trait at various times delights, amuses, and sometimes even infuriates Joel's wife and two children, with whom he lives in upstate New York. Joel worked on this particular book for the simple reason that wires infuriate him. The battle to clear out and ultimately eliminate the nests of thin, black, metal-wrapped-in-rubber snakes behind the desks and tables in Joel's house has become a top priority. The mice that drive the cursors of Joel's computers are wireless, as are the keyboards. Joel's PDA and MP3 players sync sans cables. If he could, Joel would also get rid of video, audio, and even power wires—but that last one appears to be a long way from becoming reality.

Loyd Case is a technology writer and analyst covering PC platform, graphics, digital media and gaming technologies. He's written extensively for a wide array of publications, including Maximum PC, PC Magazine, PC World and others. He began writing for Computer Gaming World back in the 1990s, when no one wrote about technology for gamers. When not working, you can find him playing board games, PC games or behind the viewfinder of his digital SLR. Loyd is married, with two daughters.

Publisher's Acknowledgments

We're proud of this book; please send us your comments through our Dummies Online Registration Form located at www.dummies.com. Some of the people who helped bring this book to market include the following:

Acquisitions, Editorial, and Media Development

Senior Acquisitions Editor: Stephanie McComb

Project Editor: Beth Taylor

Technical Editor: Jason Cross

Copy Editor: Beth Taylor

Editorial Director: Robyn Siesky

Editorial Manager: Cricket Krengel

Business Manager: Amy Knies

Senior Marketing Manager: Sandy Smith

Cartoons: Rich Tennant, (www.the5thwave.com)

Production

Project Coordinator: Katherine Crocker

Layout and Graphics: Joyce Haughey, Melissa K. Jester

Proofreaders: Melissa Cossell, Christine Sabooni

Indexer: BMI Indexing & Proofreading Services

Wiley Publishing Technology Publishing Group

Richard Swadley, Vice President and Executive Group Publisher

Bob Ipsen, Vice President and Group Publisher

Joseph Wikert, Vice President and Publisher

Barry Pruett, Vice President and Publisher

Mary Bednarek, Editorial Director

Mary C. Corder, Editorial Director

Andy Cummings, Editorial Director

Wiley Publishing Manufacturing

Ivor Parker, Vice President, Manufacturing

Wiley Publishing Marketing:

John Helmus, Assistant Vice President, Director of Marketing

Wiley Publishing Composition for Branded Press

Debbie Stailey, Composition Director

Wiley Publishing Sales

Michael Violano, Vice President, International Sales and Sub Rights

Contents at a Glance

Table of Contents

Introduction

I still remember when I got my first cordless phone. Suddenly, I didn't have to run to the kitchen when the phone rang, I just carried the phone with me. I could make a phone call from wherever I was. Wireless meant freedom, and this is just a phone that I'm talking about!

Wireless technology can make your life easier, and it's not just limited to saving you from getting up to answer the phone. You can free up space on your desk with a wireless keyboard and mouse, and you can even move your laptop around the house and stay on the Internet with a wireless network. You can be productive wherever you want to now.

Cellular technology is another area of wireless growth. A phone that once had to be carried over your shoulder now fits on your belt and offers a video camera, location tracking, and Internet access. With Bluetooth, you can have a wireless headset, which eliminates a lot of embarrassing fumbling when a call comes in.

Most types of devices have embraced wireless functionality in some form or another, and given how convenient it is to get rid of wires, you should be looking to do so whenever possible.

This book covers the whole spectrum of personal wireless technology, from your computer to your cell phone, and even your home entertainment system. There's not much we can do about those pesky power cords, but that's what batteries are for! Read on and find out all the ways your life can get easier by using wireless.

About This Book

Wireless All-In-One Desk Reference For Dummies is all about wireless technologies. It covers just about everything, from networking to digital TV broadcasting to cell phones.

If that sounds like a hodgepodge for one book, think again. The book is separated into topic specific minibooks, each written by an author who is an expert in the field.

With this book in hand, you can do all kinds of cool things:

- ✦ Choose the right wireless networking hardware
- ✦ Install and configure a wireless network in your home or small office
- ✦ Troubleshoot your networking hardware

- Configure printers so you can use them across your network
- Plug security leaks and keep them plugged
- Connect your laptop computer to wireless networks while on the road, as well as keep it constantly supplied with power
- Connect and synchronize smartphones and handheld devices with wireless networks
- Purchase, configure, and use a BlackBerry e-mail device
- Choose and use cellular telephones
- Use media servers to play your music and view photos on your home entertainment center
- Set up your own weather station
- Use GPS technology for things like finding your way home and locating cemeteries for genealogy research

The first time a technical phrase is used in the book, it is italicized, so look out for that.

System Requirements

For the sections about wireless networking, we assume you are running Windows XP or Windows Vista (or perhaps you're an early adopter to Windows 7) on your computer. Earlier versions of Windows don't let you connect to a wireless network with the ease of later editions of Windows, so we recommend upgrading to one of these three Windows versions before setting up your network.

We don't cover Mac OS X or Linux in this book. It's not because they aren't wonderful operating systems conducive to wireless networking. Instead, whole books are devoted to both operating systems and wireless networking, so I focus on what most people are running these days. Whatever your view on monopolies, Microsoft still dominates the market.

Not everything in this book is about Windows-based computers. You find chapters on new third-generation smartphones and other handheld devices — and even an entire minibook on GPS. Obviously, you need some of that equipment to get the most from those chapters.

What You Don't Have to Read

Actually, you don't have to read anything if you don't want to. It's a free country. But I bet you didn't pay to not read this book. Assume you want to read everything that's precisely on topic and not a sentence more.

That's okay. You can skip two types of information without losing the big picture:

- Information marked by a Technical Stuff icon, which I discuss a little later in this introduction. This information appeals to your inner geek, but it's not absolutely necessary reading.
- Sidebars. These bits and bytes are off the beaten path. They're interesting (I hope!), but not essential.

Still, these two groups of information make up a small portion of the book. Reading them won't consume that much time. Plus, you will make me happy for having read them. (This book contains a hidden wireless transmitter that reports back to me what you have and have not read, so don't think I don't know.)

How This Book Is Organized

Wireless All-In-One Desk Reference For Dummies contains eight minibooks, each of which focuses on a general wireless topic. We wrote in a way that lets you easily find the topic you want to read about, skipping the others for the time being. For example, one minibook focuses on wireless networking, while another contains information about cell phones and other wireless technologies. When feasible, we've kept an entire minibook about one topic, such as networking or GPS. This is what the eight minibooks contain.

Book I: Pulling the Plugs

I tell you about all the ways to cut your cords and live in a wireless world. Wireless technology has an advantage to its wired counterpart in that you can move anywhere and stay in touch. There's the rub: You're always in touch. Do you really want that? I also talk about some wireless Internet access technologies and how to choose one.

Book II: Planning Your Network

The nitty-gritty starts here, with talk of hardware such as routers and adapters. If and when you're ready to network wirelessly in your jammies, from the safety of your own den, you should take a crack at these chapters. Or at least take a peek. Already there and wrestling with some of your products? Hardware troubleshooting advice to the rescue.

Book III: Configuring Networks

First, I start off with the basics — you've got to crawl before you can walk, so what better place to start than by explaining Windows' wireless networking capabilities. That would, of course, include a look at an old Windows favorite called plug and play technology. From there, we'll learn how to use some of the more advanced networking features, especially Windows Vista's new Network and Sharing Center. We'll also lean how to manage your wireless networks both at home and on the road. Did we forget to mention that we'll cover other important features, such as creating a bridge between wired and wireless networks, as well as how to share a printer? Finally, we'll help you make sure that your network is busy doing its thing.

Book IV: Security and Troubleshooting

This brief but power-packed minibook makes you aware of the dark side of wireless computing and lets you know what you can do to best protect yourself. You can begin by getting a grip on the accounts that are available on your home network, and those instructions are here. These troubleshooting ideas are another way I help you keep your system running smoothly.

Book V: On the Road Again — But Without Wires

This book covers a wide variety of wireless technologies. It starts innocuously enough with your laptop, but moves on to handheld devices. It also covers how to strike the right balance when using your laptop on the road, so that you can take advantage of wireless technology while still thinking about battery life. You'll also learn how to synchronize your wireless devices — both laptops and handheld devices, such as mobile phones and PDAs. Speaking of wireless handheld devices, we'll also take a look at smartphones running Windows Mobile and check in on our old friend, the BlackBerry, and see how it is doing as it is rivaled by high-end mobile phones, including the iPhone. Finally, we'll take a look at how to stay connected on the road, using both hotspots in public places or using a wireless broadband card, which allows you to connect securely from just about anywhere on the planet.

Oh, before we forget, we'll take a look at another cool gadget called the Slingbox. This relatively new gadget allows you to watch your television or DVD player from anywhere in the world — provided that you've got a high-speed connection and your host has the proper Sling Media equipment installed.

Book VI: Other Networking Technologies

Starting with cell phones, this book discusses selecting a service plan and choosing a phone. It also talks about some other important issues, like

health concerns and number portability. A second chapter talks about a similar topic: cordless phones. Which cordless phone technology should you choose? The technologies of both cellular and cordless telephony are evolving, and they're getting better all the time.

Another wireless technology, but one that gets less attention, is the Family Radio Service (FRS). With two or more FRS radios, you can stay in contact with people within a mile or so of each other while on vacation and elsewhere. This book also covers the heavily popular short-range networking technology called Bluetooth and the wider range and infinitely useful Wi-Fi technology. Finally, I go through some wireless peripherals you may want to include on your desk to help get rid of that snake's nest of cords behind your computer.

Book VII: Wireless Home Technology

Wireless in the home means a broad array of gear oriented toward entertainment and leisure activities. We'll show you what it takes to start streaming video and audio that lives on your PC to your living room entertainment center. If all you care about is getting your music where you want it in your house, we show you how to do that, using products like Logitech's Squeezeebox or the Sonos ZonePlayer.

If you want to see HDTV you've recorded on your PC, we show you how to do that as well, using media center extenders and even game consoles.

In today's Web-oriented world, though, you're not limited to media that lives on your local PC. There's a wealth of video and music content available through streaming services on a wide array of Web sites. Watching or listening on your PC is easy, but we show you the hard stuff: watching Web-based TV and listening to Web radio in your living room. We say "hard," but it's easier than you think.

Wireless technology has even invaded that seemingly nondigital technology, reading books. Amazon's new Kindle eBook readers are connected to Amazon.com's online service wirelessly, allowing you to buy an electronic version of a bestseller and be reading it minutes later on your Kindle 2 or Kindle DX — no PC needed.

So while wireless is great for on the go portability and for business, it's also terrific for improving your home entertainment experience. So kick back, get some tunes on, and fire up your eBook reader.

Book VIII: The Global Positioning System

The global positioning system (GPS) is the U.S. government's gift to all of humankind. It's a series of geosynchronous satellites that tell wireless GPS receivers exactly where they are at all times — and exactly how to get where

they are going! Read about the technology behind it and how you can use it, but be sure to check out my tips regarding what to look for and what options to think about when you choose a GPS unit. After that, I describe some common GPS terminology that helps you in your quest, whatever it may be. Finally, you discover a couple of ways to use GPS technology that go beyond simple navigation, including an amazing and growing game called geocaching.

Icons

I point out some issues or topics to you with the use of icons.

A tip is a helpful bit of information that hopefully helps you accomplish a specific task a little easier. By flagging tips with icons, you can quickly find nuggets of helpful information.

Everyone needs a reminder now and then about something that's already been mentioned. That's where the Remember icon comes into play. Sometimes, the icon indicates something that's common sense or that you already know, but I point it out just in case.

Whoa, Betsy! You should know some important things, and I point out these with a Warning icon. Heed these or proceed at your own risk. I keep these to a minimum so that when you see one, you know it really is important.

Are you a geek? There's nothing wrong with that, as geeks now rule the world. If you see a Technical Stuff icon, it's likely the content is something you'll enjoy reading because of its technical bent. Geeks aren't dummies, but Dummies books are for geeks, too. Even if you're not a geek, it can't hurt to discover something new.

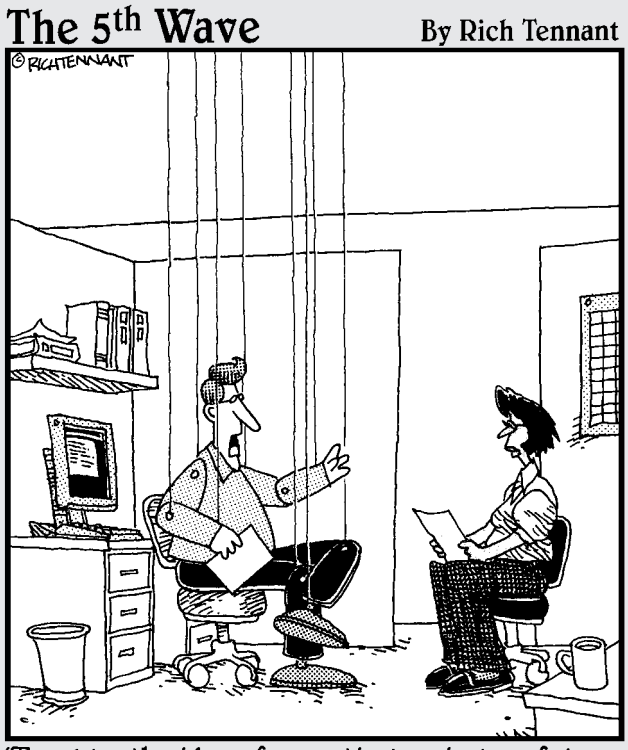
Where to Go from Here

Scissors ready? The next step is to begin cutting the wires that constrain your lifestyle. Instead, embrace radio waves and all things wireless! (Don't actually embrace them, as that effort is futile. They also can fry you; just look inside your microwave oven while it's running. But you know what I mean.) Lie upon the psychiatrist's sofa, as it were, and reject your old, constrained, wired life. Free those demons.

See you in the wireless world!

Book I

Pulling the Plugs



"Frankly, the idea of an entirely wireless future scares me to death."

Contents at a Glance

Chapter 1: Living Without Wires

In This Chapter

- **Saying goodbye to the wired life**
- **Connecting to the world on the go**
- **Dealing with the downside**

Prepare to do away with wires. Technology is terrific, but until recently the term has also been synonymous with *snakes* nests of cables under every table, counter, and desk in the whole darn house. No longer must this be the case.

This chapter introduces you to the ways of wireless. Wires have all kinds of downsides and few positives, and we take a look at the good parts of removing as many cords, cables, and technological tethers as you possibly can and still have your gizmos function the way they should. I cover wireless broadband, clearing cable clutter from beneath your household surfaces, and always knowing exactly where you are with a GPS device. Moreover, I talk about keeping connected to the world while on the go and the wonderful world of Wi-Fi.

There are downsides to living wirelessly, and you can glance at them, too. Wireless stuff is usually "always on," and that can be a hindrance. Find out why, and much more, in this introductory chapter.

Bidding Adieu to Wired Life

When you think about it, wires can be a real hassle. They limit your ability to move freely and to place things where you want them. A very good example of this is the ordinary everyday telephone. If you use a wired telephone, you have to sit at your desk or stand next to the wall phone to have a conversation. If the doorbell rings, you have to tell the person on the other end of the line to hold on while you go see who's at the door. If you're using a cordless phone or a cell phone, you can simply continue your conversation while you walk to the door.

A whole world of wireless possibilities

Now multiply the convenience provided by your wireless phone to include the whole multitude of gadgets that fill your home. Just imagine how these additional examples might apply to your situation:

- You're stuck with a slow dial-up connection to the Internet. Broadband is tempting, however, even if you're out of range of your phone company for a DSL connection or cable and fiber connections are unavailable. Consider a satellite connection. Even though the latency of such a hookup is worse than that with the aforementioned broadband solutions, you can still download big files, stream rich multimedia content, and perform other bandwidth-intensive tasks far more efficiently than you could with dial-up.
- You're pretty much solo at your computer. By adding a wireless network to your home, you can share files, printers, your Internet connection, music you've downloaded, and multiplayer games without the hassle of running wires. If you want to move a PC from one place to another, you can do it and not worry whether a handy network outlet is nearby. Why, you can even take your wireless laptop out into the backyard and surf the Internet in a lawn chair under your favorite tree.
- You're stuck at home waiting on messages and phone calls. With a wireless PDA, you are within reach of e-mail at your favorite coffee shop — you don't have to worry about missing that important message from a potential new client. You may even listen to an Internet radio station, so you don't have to listen to the rants from a fanatical talk radio show host. Figure 1-1 shows an example of a text message using a Pocket PC. Book V talks more about PDAs.

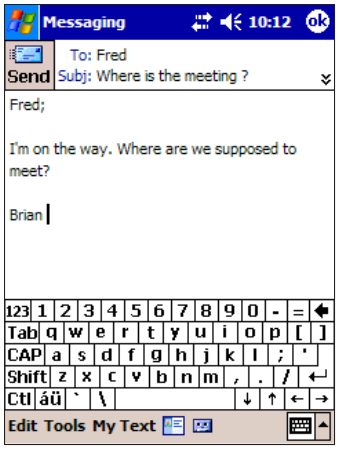


Figure 1-1: My wireless Pocket PC can send and receive messages with the built-in messaging application.

- You're sans cell phone. It's hard to imagine another device that can help you keep in touch nearly as well as a cell phone. With it, you can quickly check to see what someone's scribbled notes on your shopping list really mean. Don't take a chance that what looks like sour cream in someone's poor handwriting is actually whipping cream!

- You're sick of the wiry clutter at your desk. Cutting the wires to your keyboard, mouse, printer, and other devices sounds like a sure way to kill your computer, but wireless peripherals are simply so much more convenient than their wired counterparts — especially if your desk is such a mess that you haven't seen the top of it in years. You can use a proprietary wireless standard, Bluetooth devices, or even the forthcoming WUSB (wireless universal serial bus) to connect peripherals without wires.
- You're a home entertainment technology junkie. Now, you can set up one computer to hold all of your music from your CDs or from Internet downloads, and play that music on your home entertainment system without putting an ugly PC in the living room and without running another tangled mess of wires.
- You love radio but hate commercials, and the terrestrial stations don't play the type of songs or talk shows you enjoy. With satellite radio, the choices are much more numerous, and many shows are commercial-free!
- Your family vacations seem more like battles over who can or cannot read a map. You're going to love how GPS technology can keep you from ever having to ask directions again. Figure 1-2 shows my GPS receiver as it determines my exact position.

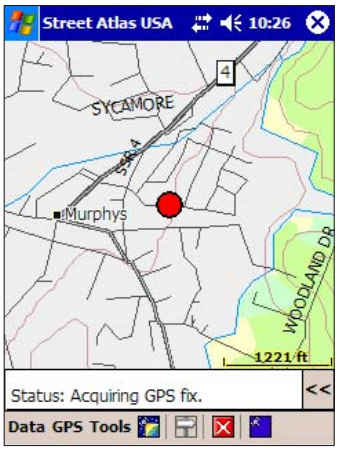


Figure 1-2: With a GPS receiver you never have to wonder where you are.

I guess if that list doesn't have you thinking about the possibilities for a wireless life, nothing will — but even this list only scratches the surface.

Cutting the cords

Now that you've seen some of the ways that you can go wireless, what's next? Actually, that depends. You probably have to do some shopping, either to replace existing wired equipment or to add wireless equipment. In either case,

it helps to plan ahead because so many different types of wireless equipment exist, and you want to make sure the things you buy work together. That's where this book helps.

Consider the example of the wireless home computer network. As you discover in Book III, home computer networks adhere to several different standards, and it's important to make sure that all the equipment you buy for your home computer network works with the same standard. As you discover in Book VII, the type of equipment you choose for your home computer network can have a great impact on how useful your network is in supplying entertainment options.

When buying wireless equipment, go for the highest performance you can afford. That way you won't close off your future options because the equipment you bought can't handle the demands of the need to process more data. Also, you can postpone the inevitable need to upgrade your equipment in the future.

Keeping your options open

Once you get the wireless bug, it can be awfully tempting to want to get rid of every cord. As tempting as that may be, just remember that you probably want to keep your options open. You might, for example, want to make sure that you have at least one wired phone in your home because cordless phones typically won't work if there is a power failure — unlike wired phones, which generally don't need a separate power supply. (Even though the handset on a cordless telephone runs off rechargeable batteries, the base station that it uses to connect to the phone line must be plugged into a power outlet to function.) Of course, if you have a digital cable phone system, all bets are off; the cable system needs power to supply phone service whether or not your phones are corded.

Remember, too, that just because some of your old, existing equipment is wired doesn't mean that it no longer serves any purpose. Sure, you probably prefer the convenience of playing music through your home entertainment system, which is connected to your computer, but that won't do you much good if you want to listen to some old, vinyl records. (I've never seen a PC with a built-in turntable.)

Don't forget to stock up on batteries when you go wireless. While some wireless devices come with built-in rechargeable batteries, others don't. Some wireless devices run through batteries at an amazing rate; consider buying a battery charger and rechargeable batteries for your devices. They're expensive at first, but they certainly save money in the long run. You may want to check out iGo (`www.igo.com`) or Batteries.com to find just the battery you need.

Connecting to the World on the Go

Wireless devices really do open up a whole new world for you, and not just when you're at home, either. Sure, it's pretty obvious that a cell phone enables you to connect to the world when you're on the go, but other wireless devices offer plenty of on-the-go options, too.

Connecting your PC on the go

To successfully communicate with someone, you generally have to both be using the same language. It doesn't really matter what language that happens to be, as long as you both understand it.

Likewise, computers need to use a common language to communicate. Modern wireless home networking equipment uses one of several standardized methods of communication that were developed to enable different brands of computers and networking equipment to successfully interact. You may have heard of these standards — especially if you've tried wading into the sometimes confusing world of wireless networking. These standards go by names like 802.11n, 802.11b, 802.11g, and 802.11a, but they also are known by the slightly less precise Wi-Fi label.

Even though the Wi-Fi label is applied to all four wireless networking standards doesn't mean those standards are identical. Of the four, 802.11b is the slowest but also the least expensive when you're buying hardware. 802.11g and 802.11a are rated for similar speeds (about five times as fast as 802.11b) but are incompatible with each other because they operate on different radio frequencies. 802.11b and 802.11g are generally compatible with each other, but can only communicate at the slower 802.11b speed. Just how fast are these different standards? That's impossible to say because your results vary greatly, depending on dozens of factors (which you discover in Books II and III). Then, of course, there's 802.11n, the newest and fastest standard, which is still emerging as this book is being written.

What does all of this have to do with connecting your PC on the go? Wi-Fi isn't limited to use on home networks. Wi-Fi is also for wireless office networks and is becoming widely available in other places, too. Want some Internet along with your coffee? Every Starbucks coffee shop now offers customers a Wi-Fi connection. (This type of connection is often called a hotspot.) If you'd rather have a Big Mac and fries while you surf, head on over to McDonald's — most of their stores have free Wi-Fi connections, too. Look for hotspots in airports, book shops, and lots of other places as well.

Head on over to the Wi-Fi-FreeSpot Directory (`www.wififreespot.com`) to find free high-speed Internet access hotspots.

Wi-Fi hotspots generally have a very limited range. In most cases you need to be within the building to get a reliable connection (and some hotspots are specifically designed to limit the range so that you can only connect if you're inside, where you are expected to be patronizing the store). Even those hotspots specifically set up to cover a broader area typically only spread their signal a few hundred feet from the hotspot's antenna, though, so Wi-Fi isn't a good option if you can't settle in one place close to the hotspot.

What can you do if you want a wireless Internet connection but aren't always within range of a Wi-Fi hotspot? One option is an AirCard from Sierra Wireless (`www.sierrawireless.com`). The AirCard comes in several models — each one designed for a specific type of service. Some models connect via the Sprint PCS Network, some with the AT&T Wireless Network, and some with other flavors of cellular service, too. Generally you should do your homework, choose the service plan that's right for you, and then buy the AirCard that works with that service. Sometimes cellular service providers even offer special pricing on the AirCard because they know that once you're hooked, you're probably going to spend a lot of money on your monthly service plan.

Connecting for voice and messages

Even though most people think of computers when they think about connecting on the go, sometimes a PC is overkill. Sometimes all you need is simply the ability to send and receive text messages. A couple of different types of wireless devices easily handle this duty:

- Wireless PDAs, including some models of the Palm and the Pocket PC, can easily send and receive text messages.
- The BlackBerry is a wireless device specifically designed for various types of electronic messaging, including e-mail and instant text messaging. It has a small, but serviceable keyboard for entering messages.
- Most cell phones now support short messaging service (SMS) so you can send and receive text messages. Apple's iPhone is a very popular PDA/smartphone.

You read more about connecting on the go in Book V.

Addressing the Downside: You're Always On

If the wireless world has one big problem, it's that always being connected means that people can contact you at any time. Sure, it's convenient to flip open your cell phone to quickly ask someone a question, but don't forget that it is just as convenient for someone to dial your cell phone number and interrupt whatever you're doing.

But once again, you shouldn't limit your concerns simply to the fact that anyone can call your cell phone at any time — that is, unless you're on vacation and you're trying to get away from it all!

Your wireless network is always on

Wireless home networks are awfully convenient because you can simply fire up your PC anywhere within range and connect. This convenience has its dark side, too. As long as your wireless network is working, a neighbor or a stranger driving by can conveniently try to connect to your home network. Remember, the fact that your wireless network doesn't require someone to connect using a physical network cable means it's much easier for someone you don't want on your network to gain access.

You can, of course, apply some security measures to make it harder for people to break into your wireless home network. In fact, it's not only possible, but it's also essential that you enable your wireless network's security features if you don't want to run into serious problems. See Book IV for more information on this very important topic.

Your wireless gadgets are probably open, too

Imagine how difficult it would be to keep your automobile safe if the manufacturers were in the habit of delivering cars without locks because they felt that locks were too complicated for the average driver. In most major cities you'd probably be able to measure in minutes (or hours, at the most) the time before your car was stolen.

Unfortunately, the manufacturers of many wireless devices do something similar to building cars without locks. Rather than building in advanced security features (or, as is the case with wireless home networking gear, leaving the security features turned off by default), manufacturers often opt for dumbing down their products so they work as soon as you take them out of the box. Bluetooth-equipped cell phones present an easy target for snoopers for this reason. (See Book VI for more information on Bluetooth technology and the security risks that are involved.)

In reality, the manufacturers probably are correct; so few people bother to read the technical sections of their product manuals that enabling features that increase security would result in many calls for help from new users. Or, even worse from the manufacturer's perspective, it could result in products being returned to the stores because "it doesn't work."

You can go a long way toward protecting your wireless world by taking a few minutes to understand (and use) whatever security measures are offered by your wireless devices. Remember, the harder you make it for a thief or a snoop, the more likely he'll move on and find an easier target. Even the simplest security measures often deter thieves unless they're specifically

looking to get at your data. Thieves looking to score any data, or leech any Internet connection, typically skip the security-enabled devices and continue on their way.

Taking back control

Yes, going wireless does make life more convenient, and often a lot more fun, too. Keeping things in perspective is important, as well as making sure that the convenience isn't overshadowed by letting the wireless devices control your life, rather than the other way around. You do have the ultimate weapon if you're willing to use it, and that's the on/off switch.

Chapter 2: Choosing Internet Access

In This Chapter

- **Using satellites for Internet access**
- **Microwaving without food**
- **Maximizing access with WiMax**

You probably connect to the Internet using DSL or cable modem service, both of which deliver data over fat broadband connections, meaning they feature fairly wide bandwidth and allow data to download fairly quickly. (If you're going online via a dial-up connection, I hope you're considering switching to broadband access before venturing much farther into this book. Speedier broadband access is practically required for connecting to the Internet nowadays, if you don't want to spend your life in front of your computer, waiting for Web pages to load and programs to download.)

But what if you live in an area that doesn't have either DSL or cable modem broadband service? What's a computer user to do? (Thank goodness you at least have access to Dummies books!) If you live someplace where the local telecommunications providers haven't gotten around to offering broadband service, or if you live too far out of range of them to be able to offer you a high-bandwidth pipe, you can always turn to at least one other option.

In many cases this option is satellite Internet access. In some areas, you might be able to subscribe to something called fixed wireless, which means the company broadcasts a signal directly to your home (and you back to them). Both of these options can be expensive, but they are options.

In even fewer areas, entire cities or city centers are covered by Wi-Fi access, a topic I also talk about in Book V, Chapter 5.

I cover another wireless Internet technology that uses the cellular telephone network elsewhere in the book. You can find information about cellular-based packet data networks in Book VI, Chapter 1. In addition, some cellular carriers have launched so-called 3G (third-generation) networks that provide mobile data services, and 4G is on the way. I cover this in Book VI, Chapter 1, too.

Using Satellite Service

Just like satellite TV services deliver television programming directly to your home, satellite Internet providers provide you with broadband access that you can use to do anything you would do on the Internet over DSL and cable modem services.

Satellite service is great for folks who are off the beaten path (or don't even have a path nearby). The service might also be an alternative if you simply dislike your current DSL or cable modem provider, but beware some downsides:

- ✦ You need a clear view to the south, as that's where the satellite is in geosynchronous orbit — right over the equator.
- ✦ Bad weather can slow or cut off your Internet access, just like heavy rain and snow tend to disrupt satellite TV service.
- ✦ Trees that grow in your satellite path are not your friends. And as I learned the hard way, don't set up service in winter, when the trees have no leaves. As soon as spring comes, those leaves will grow back and obstruct your once-great, clear view to the south.
- ✦ Expect more latency than you experience with a typical cable, DSL, or fiber broadband connection. It takes time for the signal to get from the satellite to a receiver/transmitter dish, and a similar amount of time for the signal to get from the dish to the satellite. Thus, some time-sensitive Internet activities such as gaming and VOIP (voice over internet protocol) don't work well with a satellite connection.

StarBand by Spacenet

StarBand by Spacenet satellite service is available throughout the entire United States (yes, even Alaska and Hawaii), Puerto Rico, and the U.S. Virgin Islands. It's a two-way, always-on broadband service similar to DSL and cable modem service. It works with PC and Mac, Linux, and Unix, although tech support only provides help with Windows 2000 Professional, Windows XP Home, and Windows XP Professional and Mac OS X — that's according to the FAQ on the company's page.

Traveling with connections

StarBand evidently used to have a service that let you mount a satellite antenna on your RV so you could stay connected no matter where you traveled in the United States. Now, according to the FAQ on the Web site, that's not possible. The antenna both transmits and receives information to and from the satellite, and such a connection requires too precise an installation to allow travel.

Fair use policies

Both StarBand and HughesNet employ something they call fair use or fair access policies. In a nutshell, the policies may limit how much bandwidth you can consume in a given time period. They're designed to keep a small number of users from monopolizing the services.

StarBand "reserves the right, and will take necessary steps, to prevent improper or excessive consumption of bandwidth used," according to its fair access policy. It does, however, relax the policy during the wee hours of the morning. As for HughesNet, it too relaxes its fair access policy in the middle of the night. "Currently, you can use your HughesNet service for several hours during the middle of the night (the "Download Period") with relaxed application of the Fair Access Policy. The hours of unrestricted use shall begin no later than 2:00 AM and end no earlier than 7:00 AM eastern time."

Monthly service fees start at $69.99 for Nova 1000, a tier with download speeds up to 1 Mbps and upload speeds up to 128 Kbps. A one-time equipment fee includes the satellite dish and satellite modem, and that costs $299.99. An installation fee also applies, as StarBand requires that a professional install the equipment. Self-installation is not allowed.

A second tier of service, called Nova 1500, offers download speeds up to 1.5 Mbps and upload speeds up to 256 Kbps, and it starts at a monthly rate of $99.99 (plus equipment and installation charges).

HughesNet

HughesNet, formerly DirectWay, which itself was formerly called DirecPC, offers a satellite Internet service very similar to StarBand's. For its home package, it advertises up to 1.0 Mpbs for download and 128 Kbps for upload.

The service provider also limits to 22 the number of concurrent Internet connections. Unlikely a problem for simple Web surfing, but once you have a Web browser, e-mail program, music download software, and other Internet applications working all at the same time, the 22 connections begin to want for more.

HughesNet has many pricing plans, offering Home, Pro, ProPlus, Elite, and more, each of which has different tiers of bandwidth both upstream and down. Furthermore, you can choose whether to purchase or lease the necessary equipment. The sheer number of possibilities makes it impossible to list all the prices you might pay for HughesNet service, but expect to pay between $99 and $299 upfront for equipment and $59 to $349 monthly for bandwidth.

Maxing Out with WiMax

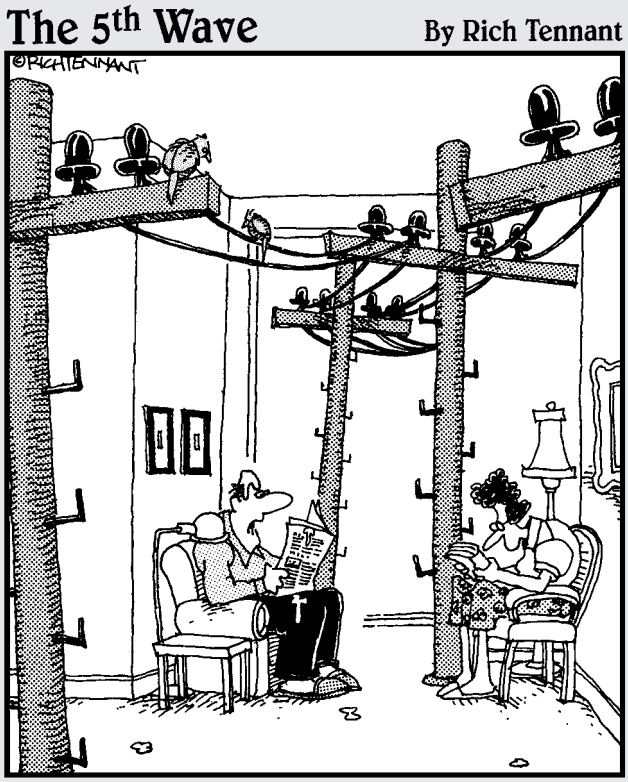
A lot of people in the wireless arena are asking, "Whatever happened to WiMax?" WiMaxstands for world interoperability for microwave access. It's a broadband wireless service that has the capability to provide service for people who get around.

One firm predicted that by 2009, more than 7 million subscribers worldwide would be using the fixed version of WiMax (not including mobile uses). What's so great about WiMax is that it's like having ubiquitous Wi-Fi access. Whether you're in your home, in your backyard, or in your car, you would have constant Internet access. Somehow, WiMax didn't jump into the center of the arena like many people thought it would.

WiMax had, and still has, the possibility of providing fast Internet access throughout a metropolitan area (unlike a local multipoint distribution system, which I describe next). Think about cell phones and how they continue to work as you move around. You don't have to turn off your cell phone when you leave your house and then turn it on again when you get in your car, so why should you have to do that with wireless Internet access? If WiMax ever makes the kind of splash that pundits once predicted, you won't need to do that.

WiMax requires new access adapters in desktop and laptop computers because it's incompatible with Wi-Fi technology. While it's been slow to catch on, there are a few WiMax devices on the market — it will be interesting to see if they take off or simply fizzle out.

Book II
Planning Your Network



"That's it! We're getting a wireless network for the house."

Contents at a Glance

Chapter 1: Getting Started

In This Chapter

- **Figuring out your needs**
- **Surveying your wireless network**
- **Understanding radios**
- **Making a shopping list**

Just five years ago, wireless networking was expensive and difficult to set up. Fortunately advances in technology have lowered costs and increased features, resulting in something that's both affordable and easy to set up. In fact, it's hard to ignore wireless networking now because it's everywhere!

Wireless networking has many benefits, including:

- **Mobility:** If you can drag your computer somewhere, you can get on your network from there. You don't even have to shut it down! Take your computer from the kitchen to the bedroom without having to close your work or tell your chat buddy "BRB" (that's "be right back" for those who were wondering).
- **Fewer cables:** Technically, there's only one less cable, but I've found that the network and power cables are the most bothersome. Now all you have to worry about is power, and I'm sure you've got more power outlets than network drops in your house.
- **Expandability:** Adding a computer to a wireless network takes a few mouse clicks. Adding a computer to a wired network often takes a drill and a lot of cable. Plus, you have to make sure you've got enough network ports. Guess which is faster to get up and running?

This chapter gets you started building your own wireless network. First, you need to determine what it is that you want to get out of your wireless network. Next, you find out how wireless networks work, and apply this to finding any potential trouble spots in your house. Finally, we get you ready to go shopping!

Figuring Out What You Want to Do

Before you even think about how to build your wireless network, take some time to figure out what you want to do with it. Hey, maybe you don't even need wireless. Would this be a bad time to mention your bookstore's "no refunds" policy?

When it comes down to it, networks connect people. You might connect to gain access to a service such as e-mail or the Web, or you might connect to share some files between two computers. Wired or wireless, a network's value is in the connections it provides.

You can do pretty much anything on a wireless network that you can on a wired network. Your requirements affect the kind of equipment you need, so it's important that you think about what you want to do before you open your wallet.

Think about which of the following you'd like to be able to do:

- **Access the Internet.** The Internet's a big place, and to see it you have to connect your network somehow.
- **Share files.** Do you have more than one computer in your home? Do you want to be able to get files between the two? Or maybe you're looking for a separate device to store files on, and you need to connect to that. Are these small files, large files, or huge files? Even though USB key fobs are cheap, you can't beat the convenience of being able to copy files by the drag-and-drop method.
- **Watch video.** Services are available that let you watch video over the Internet. You may also have a device that will let you watch TV over your home network. Either way, video introduces some demands that not every piece of wireless equipment can accommodate.
- **Play video games.** If you're a gamer, then you know how network conditions can affect your game. You can't control much on the Internet, but you can make sure that your network's not the problem.
- **Print.** Printers are coming with wireless capabilities now, so you can put your printer wherever you want, or move it whenever you need.

Give some thought to devices you have that may already be wireless capable. They may need an upgrade, or alter your plans slightly, depending on their age. You don't want that old PC you got from your aunt dragging down the speed of your network if you can avoid it.

Finally, think about where in your house you want to use your computer and wireless peripherals. We get into the details about range shortly, but a wireless solution for a living room will be different for a 30-room mansion, especially if you also need Internet access down in the guest mansion. What's that? Your guest mansion's empty? When can I move in?

Going the Distance

Just like your favorite radio station, the radio waves from your wireless network can't travel forever. And even if they could, your computer doesn't have the power to talk back.

Unlike your favorite radio station, the distances involved are much smaller. A radio station's coverage is measured in miles; your network is measured in feet.

Why, you ask? Isn't all radio the same? Not by a long shot! A radio station's power output is around 100,000 watts; your wireless devices are under a tenth of a watt. Frequency plays a part in it, too — higher frequencies travel shorter distances. Your wireless network's frequencies are at least 20 times as high as your radio's.

The wireless engineers at the IEEE are constantly updating their standards to give you faster speeds and better distance. (Incidentally, IEEE used to stand for Institute of Electrical and Electronics Engineers, but taking a page from a famous fried chicken chain, they have rebranded themselves just as IEEE, which is pronounced "Eye-triple-E") These standards are supposed to ensure that if you buy two products from two different vendors, they can work together.

IEEE standards for wireless have a name starting with 802.11 and ending with a letter. Each letter is a different standard that may or may not be interoperable with other standards. We talk about the standards in the next chapter, but just so you have an idea, here are some of the ranges of the various standards.

Table 1-1 shows ranges you can expect in a typical indoor environment. Note the use of the word typical. Depending on your hardware, your environment, and where you place your devices, you may see better or worse distances.

Table 1-1: Comparing Wireless Radio Ranges

Standard	*Typical Indoor Range*
802.11a	100 feet
802.11b	150 feet
802.11g	150 feet
802.11n (draft)	300 feet

It's Wireless, Not Magic!

In the previous section, you learned that your wireless network has a limited range, and that it's hard to place a finger on what that range will be. In this section, you find out what kind of things cause problems with wireless signals.

A simple wireless network consists of a central radio, called an *access point,* that connects to a wireless transmitter/receiver in your computer, game console, or portable device. The access point is responsible for everything on the wireless network, so it's important that your equipment and the access point have no problems communicating.

Wireless isn't magic. It's a radio wave. Radio waves follow the laws of physics, some of which have the end result of damaging radio signals to the point where they can't be decoded. A signal that can't be decoded is useless to all involved; the result is a slow (or nonexistent) network.

In general, wireless problems fall into two categories: interference from other radio waves, and interference from physical objects.

Interference from other radio waves

Whatever country you're from, your government likely regulates which wireless frequencies can be used, by issuing licenses to people for certain parts (bands) of the radio waves. The governments do this in part to make sure that multiple people don't try to use the same frequency and step all over each other. (They also do it because they get large sums of money out of the deal.) Have you ever played with remote control cars when two people pick up a transmitter with the same frequency? Oh, what fun that is, when the single car tries to respond to two sets of commands.

Wireless network devices operate in unlicensed bands. Unlicensed bands are free for anyone to use as long as they abide by the rules the government set out. These rules, for one, limit the power output of a device so that your transmitter doesn't interfere with your whole block.

Anything transmitting in the ranges that wireless radios use (2.4 GHz and 5 GHz) is a potential source of interference. Other wireless networking devices can cause problems. This is why the IEEE specified several channels within the 2.4 GHz and 5 GHz bands. These channels are on slightly different frequencies so that two devices can coexist. We go over a lot more information about adjusting your channels later in this chapter, but for now, remember that having two access points on the same channel is a bad thing.

Microwave ovens emit interference in the 2.4 GHz range, which as you now know is the same as what your computer's trying to use. Playing with your access point's channels is not going to do much here, because microwave ovens interfere with all of them.

Your best bet for dealing with microwave ovens is to get them as far away from your computer and access point as possible. For example, I've got my microwave oven in one corner of the house and my access point on the opposite corner on a different level. This arrangement usually works unless I'm trying to use my computer in the kitchen with the microwave on.

Another source of interference is from cordless phones. Phones generally come in 900 MHz models, and, you guessed it, 2.4 GHz. Cordless phones bounce around from frequency to frequency to try to avoid interference. You'll probably find that the wireless network causes you more problems while talking on the phone than the other way around, though. However, if you're having periodic network problems and can't pin a cause on it, you might want to check and see if someone's talking on a cordless phone at the time.

Interference from other items

Radio waves can be interrupted in flight by almost any solid object. Walls, doors, furniture, and even glass can degrade your wireless signal.

Walls are likely to be your biggest concern. In general, the bigger and thicker the wall, the worse it's going to make the signal. Simple drywall walls may not cause a problem, but brick or stone walls, or metal (such as a concrete wall reinforced with rebar), are going to cause problems.

If your house has several levels, then try to determine what kind of material is between the floors. In a house, it's usually wood, which is only a mild barrier to radio waves.

The easiest approach to dealing with interference is to place your access point as close as possible to the places you want to use wireless. If you find some dead areas, you can try moving your access point. In the worst case, you buy a second access point or a repeater to give service to the dead zone. It's a lot cheaper than knocking down walls, after all.

Radio engineers have also found other problems caused by walls and furniture that have to do with the way radio waves bounce off of things. The 802.11n standard has features to deal with these.

Preparing to Shop

When wireless standards were first introduced, the cost of wireless was obscene. Access points ran in the thousands of dollars and were marketed to big companies with buckets of cash. Unsurprisingly, the technology was much slower and difficult to manage.

The technology life cycle

If you've followed any area of technology, you'll know that stuff keeps on getting better. Cameras get smaller, computers get faster, and televisions get bigger. You might expect that you'd have more options and be able to choose how fast you want your computer to be, but that is rarely the case.

When making parts for electronics devices, it's in the manufacturer's best interest to make as few versions as possible. Over the past couple of decades, Intel has made chips for computers that run from 4 MHz to over 3 GHz. Digital cameras started out well under a megapixel but have now blown past 12 megapixels. USB memory keys started out at megabyte, and now they're replacing your hard drive. But try to go to a store and find the full array of products? Not going to happen.

Part of it is that people are buying the higher end gear, but it's also that it costs more to make the old stuff. Chip-making machines have already been retooled for the newest chips. The chips to make a computer's wired network card run at the original 10 megabits per second cost a lot more than the ones that let them run 100 times faster.

At the same time, manufacturers shoot for certain price points. In the 1980s, a new computer cost around $2,000. The next model was faster and had more space, but it still cost around $2,000. Once the old model was sold out, it wasn't being made anymore.

This $2,000 price point carried on for a while. Then the introduction of the Internet drove demand for computers up, and advances in manufacturing (and the increased demand) drove the manufacturer's cost down. Now that $2,000 price point is much closer to $400.

The same goes with cellular phones. The price of phones has stayed the same, but you just get more features. Phones now have cameras and built-in MP3 players and can play video games. It's hard to find a basic cell phone now. The demand is low, and it's getting so cheap to add the phone or MP3 player that it makes more economic sense to not offer the bare-bones version.

Every so often something disruptive comes to a product that makes the current technology less desirable. Plasma and LCD televisions made older tube televisions cheap, for a while, as manufacturers tried to get rid of their parts inventory and to make a profit off their soon-to-be obsolete technology while they could. When a new wireless standard is on the horizon, the current technology drops in price. The popularity of wireless made the price of wired network equipment take a nosedive as manufacturers tried to keep the sales coming in.

Now, competition in consumer-grade computer equipment has driven down prices, and advances in manufacturing have allowed engineers to do more with less.

Prices in consumer electronics tend to follow an interesting pattern. First, the cost is high as a new technology is introduced. As the technology gains ground, the price drops as competition enters the market. This should not be a surprise.

However, as the technology matures, the cost stays within the same range; you just tend to get something that's smaller, faster, or more feature rich than the device that came out the month before. Instead of staying on the market, older equipment just goes away as it gets replaced. Prices fall only after something really innovative happens, usually because the manufacturers want you to stay with that technology instead of the new thing.

Within the price range of a particular technology, you find that the latest and greatest model costs the most. If you want to save a fair bit of money, you can get something with 90 percent of the features and speed of the device that happened to be new just a little while ago. You can also go really cheap and get a knock-off device made by a company you've never heard of. Each has their advantages and disadvantages.

All that said, the next section has a list of the types of equipment you'll be looking at, along with the expected price range.

Putting Together Your Shopping List

Here's where you get familiar with the types of equipment you might need and devise the list of what you need.

- A wireless access point connects your wireless network to your wired network. The access point's job is to manage the wireless network and relay messages between the wireless and wired devices. An access point costs between $50 and $150, depending on the technology.
- A wireless router is really a few devices in one box. It's a firewall that connects your network to the Internet and provides some network services and safety along the way. We go over these features later. The router also has a built-in access point. Optionally, the router can have a few wired network ports.

  Wireless routers, like the one in Figure 1-1, go for $50 and up, depending on what extra features are on them and how fast they go. Most quality routers are in the $100 range, though. A wireless router can also be used only as an access point by plugging it in a certain way and not configuring all the features.
- A wireless range extender (shown in Figure 1-2) is used to boost a wireless signal for areas where the signal is weak. These, too, are like access points (some can double as an access point). As long as the extender can receive the signal well, it can rebroadcast at a higher power to extend the range. You should be able to find range extenders for $50–$100.

Figure 1-1: A wireless router.

Figure 1-2: A wireless range extender.

- On the computer side of things is the wireless NIC. For laptops that don't have wireless built in, you need a notebook adapter, sometimes called a PC card for your computer. These devices cost from $50 to $150, depending on features and the standards the card supports. Figure 1-3 shows such an adapter.

Figure 1-3: PC card adapter.

- If you are upgrading a desktop machine, you have a couple of options. You may buy either a PCI card that goes inside the computer or a USB-based one that plugs into a free USB slot. Note in Figure 1-4 that the PCI-based card has an external antenna, which is helpful in obtaining the best signal, especially if your desktop is in a tight spot.

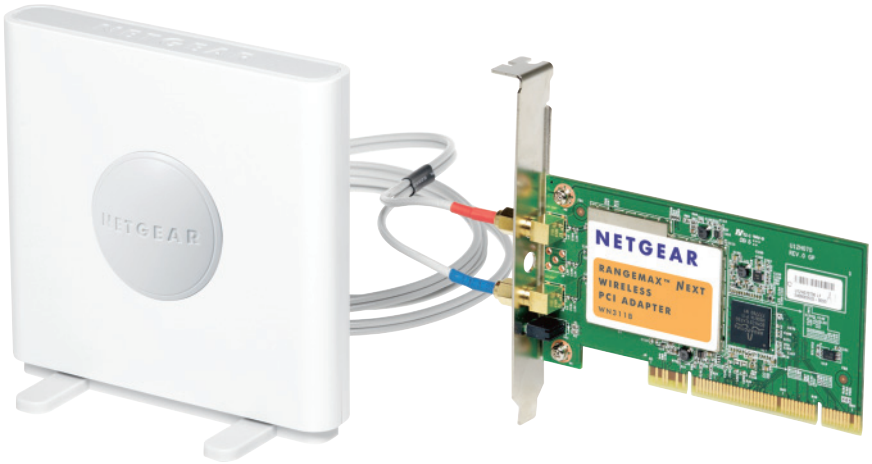


Figure 1-4: PCI wireless adapter with external antenna.

Nothing says you can't use a USB adapter with a laptop. You'll find the PC card is probably more convenient because part of the card is inside your computer.

Wireless cards for PCs cost about the same as their laptop counterparts, though you may pay slightly more for the benefits of an external antenna.

To get your shopping list started, you'll want an access point or a router, plus a wireless card for each device you want to get on the network. Take stock of your existing computers; they may already have a wireless NIC built in.

Don't pull out your wallet just yet. We've yet to get into the various options you have underneath the wireless umbrella. There are different radio standards, frequencies, antennas, and routers . . . I'm getting excited just thinking about the possibilities!

Chapter 2: Choosing Hardware

In This Chapter

- **Choosing your Internet connection**
- **Making sense of wireless standards**
- **Choosing equipment**
- **Expanding your network**

Browse the aisles of your favorite electronics store, and you will find a dizzying number of equipment choices at all price levels. You've got to choose between the various 802.11 standards, whether you need a router or an access point, which brand to buy, and which optional features you want. Did you need wired ports? So many choices, what do you do?

In this chapter, you find out what hardware you need to get on the Internet and to build your wireless network. After you read this chapter, you can confidently make a purchase. You'll also want to make sure your Internet connection is up to par. You are likely to have a few Internet access options available to you, so you'll want to make sure you know what each option offers.

The information in this chapter can help you form the foundation of your wireless network, so the best place to start is where the Internet meets your house.

Exploring Your Options: DSL or Cable

If you watch television for a while, you can see lots of ads for Internet access. Several companies are vying for your business, and they're all offering something slightly different. How do you cut through this noise and buy the right product for you?

Before you get much further on the topic, though, your decision might already be made for you. Maybe you're in a location where you've only got one option. Maybe you already have something. In that case, feel free to skip this section, or read on if you're interested.

Look at the flyers that come in your mailbox or newspaper. Look at your telephone and cable bills. Chances are you're being offered a choice between digital subscriber line (DSL) and cable. Usually both options are called "High Speed Internet," or some flavor of that. But read the fine print,

it's probably one of those. If it comes from the phone company, it's DSL. If it comes from the cable company, it's cable.

Depending on where you live, you might be offered a satellite service, or even a fiber-based service. You also should have the option of dial-up. So many options! My head is spinning!

All other things being equal, your decision comes down to comparing speed and cost. How fast do you need your Internet to be, and how much do you want to spend?

Sharing the road

Even though the term *information superhighway* died a merciful death many years back, it's sometimes helpful to think of the Internet as a road system.

When you browse the Web, or receive e-mail, your computer sends information in the form of *packets* to the other end, which can be a Web server or an e-mail system. The other end looks at these packets and sends the response back to you in a new series of packets. These streams of packets are often called *traffic*.

It might help to think of these packets as cars on a road. Your Internet connection is a small road that can carry so many cars. This road connects to bigger roads that eventually lead to superhighways that are many lanes wide. Depending on who you're trying to talk to, they may be located right off the highway in the case of a busy Web site, or they may be on a road much like yours in the case of a small Web site or home user.

Just like cars on a road, Internet traffic sometimes gets congested if too many cars try to use the road. Only so many cars can fit on a single lane, which means information takes longer to get between the two sides.

Dealing with DSL

DSL is an Internet service that is delivered over your regular phone line. The frequencies that make up voice fall within a small range, so a DSL modem throws the Internet signals into the space that's left. At the phone company, these Internet signals are pulled out by a device called a DSLAM (what it means isn't important, but it's one of the coolest acronyms in the networking field).

The Internet goes on the higher frequencies, which means every phone jack in your house needs a filter placed on it so that you don't hear the noise generated by the high frequencies, and your phone doesn't affect the quality of the data transmissions.

You can choose from a wide variety of DSL, and only your Internet service provider knows which ones are being used. You can find that you usually get the appropriate DSL modem provided as part of the service, so don't worry

too much about buying one of your own. However, do make sure this is the case if you are looking at DSL. You then plug your network into the DSL modem.

The advantages of DSL are that you have a dedicated connection between your computer and the service provider, rather than sharing it with your neighbors. However, your Internet traffic eventually merges with your neighbors in the provider's high-speed core, anyway. DSL offers good speeds, and because it's delivered over your phone line, you can usually get a price break by bundling your DSL and phone service.

DSL is usually offered in different grades, such as 1 Mbps down and 384K up. This means you can download files at 1 million bits per second, or roughly a compact disc's worth of files in an hour and a half. The upstream speed isn't as important because the bulk of your Internet usage is downloading. Having 1 Mbps down is adequate for Web browsing, but having 3–5 Mbps is more desirable. (It goes up from there, so if you plan on downloading a lot of files, then look at higher plans.)

Contemplating cable

Cable-based Internet uses some TV channels for sending and receiving the Internet signals. A cable modem plugs into your TV jack, you plug your network into the cable modem, and you're off to the races.

Cable is a shared medium, so the connection between you and the service provider is shared, usually with your neighborhood. Cable is capable of higher speeds than DSL, so this tends to even out.

Like DSL, you require a modem (but not a DSL modem). The usual practice of cable companies seems to be to charge a rental fee for the modem or to allow you to buy your own. Cable modems tend to follow only one standard called DOCSIS, so finding a compatible cable modem is easier. If you want to go down this road, ask your cable company for a list of supported modems and follow it to the letter!

Cable, too, is often sold in various grades. These grades are likely to be faster than DSL, but remember, you are sharing your connection. Usually the basic package is good enough to get you started, and you can easily upgrade later.

Don't forget to ask about bundling opportunities if you're a cable subscriber.

Debating dial-up

I only mention dial-up in here to tell you to avoid it. It's slow. It doesn't cost much less than a basic high-speed DSL or cable package. You can't use your phone when you're on the Internet because your computer is using it, which defeats the purpose of wireless. Did I mention it's slow?

Just remember that both DSL and dial-up are delivered over the same phone service. Dial-up requires you to use a modem in your computer to make a call to another modem at your provider, while DSL injects the Internet signals on top of your voice calls (which you don't notice). DSL is good, dial-up is bad.

Oh, yeah, and dial-up is slow.

Exploring FIOS or FTTH options

Depending on where you live, you might have the option of getting fiber optic cable delivered to your home. You might see it called FIOS (Fiber Optic Service) or FTTH (Fiber to the Home). Pronouncing the two might get messy, though.

Fiber optic cable can deliver a lot of speed. It's reliable, too. This extra speed will cost from "slightly more than cable" to "a lot more than cable," depending on how fast you want to go. But, if the option is available to you, it's worth looking at. You will be able to get speeds much faster than cable or DSL. Depending on the provider of the fiber, you may be able to get better entertainment offerings, such as high-definition television and video on demand over the same fiber.

Going over the Letters

Getting set up with Internet access (if you don't have it already) takes a few days, which gives you time to think about the kind of wireless network you want.

The eggheads . . . I mean engineers . . . at the IEEE have been improving wireless standards to make them faster and more reliable. The IEEE 802.11 standards describe how wireless signals are transmitted and decided and in traditional geeky fashion have names such as 802.11a, 802.11b, and so forth. Over 20 standards exist in the 802.11 family, although consumer products only advertise support for a handful of them.

The Original — 802.11

The first one didn't have a letter after it, but it provided 1 or 2 megabit service at 2.4 GHz. It worked, but given the state of industry in 1997, it was expensive and bulky. They were the size of a shoebox!

The other standards out there are amendments to 802.11.

Improving on things — 802.11a and b

Despite coming out at nearly the same time, 802.11a and 802.11b are very different. The 802.11b improves on the original standard by giving up to 11 megabits over the same 2.4 GHz frequency. This increase in speed drove

adoption of 802.11b networks, which pushed manufacturers to build smaller and cheaper devices.

802.11a on the other hand runs at 54 megabits per second, and at the 5 GHz frequency. You get a lot of noise at 2.4 GHz, so the IEEE thought it best to get out of that band. There's also more room up there, which means you can have more radios operating in the same area without stepping on each other. The downside is a slightly decreased range; indoor networks are usually rated at around 100 feet for 802.11a and at 150 feet for 802.11b. Needless to say, unless your gear has both a and b radios in them, you have to choose one or the other.

Mass market appeal and low prices made 802.11b the winner here, so you won't find much 802.11a gear out there. The market for 802.11a is mostly companies that are willing to spend some extra money for the benefits of 802.11a.

802.11b has been superseded by 802.11g. You can still find some 802.11a gear out there if you're buying for a company, but you're likely not going to find it on the shelves of a store.

Giving you 1999 speeds in 2003, it's 802.11g!

802.11g got the 2.4 GHz radios to the speed of the 5 GHz radios, only a few years later. 802.11g is also backward compatible with the b standard, so you can use an older network card on your g network, albeit at the lower speed.

There is a significant downside to running an older b radio on a g network, though, which is that the whole network's performance is degraded even if one b radio is joined up. In the worst case you get 802.11b performance, so it's worthwhile to upgrade any legacy 802.11b clients if you're going to run 802.11g.

That aside, 802.11g provides good speeds, good coverage, and it's cheap. Despite being released in 2003, this version is still current. If you look at what's on your store shelves, or if you already have a network card, chances are it's 802.11g (or n, but I cover that next).

802.11g is a good choice for the price conscious buyer, or the user that doesn't need anything fancy. At 54 mbps, 802.11g is still faster than your Internet connection, and still lets you shuffle files between computers with ease. If you already have 802.11g adapters built into your laptop, then this is the most straightforward option for you.

802.11n. Or is it pre-n? Or draft 2?

As of the writing of this book, there's no 802.11n. Although 802.11n has been worked on for years, it's still in draft form. But look in the stores, and you'll see 802.11n devices for sale, how does that happen?

A patent problem with a part of 802.11n is preventing the standard from being completed.

In the meantime, an industry group called the Wi-Fi Alliance has developed a certification program for devices to ensure that they comply with draft 2.0 of the 802.11n standard. This means that any device that's branded Wi-Fi CERTIFIED™ 802.11n draft 2.0 is interoperable with another device with the same brand. The logo is shown in Figure 2-1.

Figure 2-1: The Wi-Fi CERTIFIED® 802.11n draft 2.0 logo.

A device that is certified to draft 2 of the 802.11n standard can be upgraded to the final 802.11n standard by only a change in software. I talk about upgrading your router later, but for now, just understand that if you buy a certified product, you shouldn't have to buy anything else to upgrade once those lawyers get finished.

802.11n operates in both the 2.4 GHz and 5 GHz bands, and is backward compatible to a, b, and g radios. It also doubles the range of 802.11g to 300 feet and can operate at speeds of up to 600 Mbps. That's fast!

Behind those impressive numbers, though, is some marketing magic. You only get the benefits of 5 GHz if your equipment has 5 GHz radios (that means both your access point and wireless card). Such devices are labeled *dual band*, meaning that they have both the 2.4 GHz and 5 GHz capability. In the interests of dropping costs, though, many 802.11n devices only have the 2.4 GHz radios.

802.11n gets most of its speed from running larger channels and running them in parallel. For this to happen, the frequency has to be clear and the device has to have multiple antennas. At the 2.4 GHz range you probably have interference from other networks that causes 802.11n to degrade to smaller channels. Most consumer devices have two antennas, which is twice as good as one, but only half as good as the four that are required to get up to 600 Mbps.

It's not all bad news for 802.11n. There are still improvements on 802.11g that make 802.11n faster than g, even in the worst case. If you have a need for speed, then 5 GHz 802.11n is where you want to be.

Another benefit to the dual band radios is that you can run your 802.11n clients in the 5 GHz range and leave the 2.4 GHz band to the 802.11b/g clients. This way you can make sure your speed-hungry devices aren't slowed down by legacy adapters.

Compatibility concerns

Wireless devices are generally downward compatible with other devices in the same frequency. Therefore, you can mix 802.11b and 802.11g because they're both running at 2.4 GHz, but not with 802.11a at 5 GHz.

Keep in mind that just because something's compatible doesn't mean that it's going to run as well as it could. Even with an 802.11g card (54 Mbit/s, remember?), you're limited to 11 Mbps on an 802.11b network.

When your access point's capabilities exceed that of the clients, you still have problems. An 802.11g access point will instruct all clients to operate in a slower compatibility mode if even one 802.11b client is connected. 802.11n has some protections to prevent this problem with legacy clients but still is not as fast as an 802.11n only network.

802.11n will coexist with 802.11a, as long as you've got a dual band network card in your computer. This limitation isn't too much to worry about because 802.11a network cards aren't terribly popular.

Table 2-1 helps you make sense of the information in this section.

Table 2-1: 802.11 Frequencies, Speed, and Ranges

Standard	*Frequency*	*Speed*	*Range*	*Should I Look at It?*
802.11	2.4 GHz	1–2 Mbps	100′	No
802.11a	5 GHz	54 Mbps	100′	No
802.11b	2.4 GHz	11 Mbps	150′	No
802.11g	2.4 GHz	54 Mbps	150′	Yes
802.11n Draft 2†	2.4 GHz	54–300 Mbps	300′	Yes*
	5 GHz	54–600 Mbps	300′	Yes*

If you go down the 802.11n path, do your best to get dual band (2.4 GHz and 5 GHz) equipment.

Make sure any 802.11n gear you buy is certified by the Wi-Fi alliance. Check `www.wi-fi.org/` for the latest version of the standard.

At the moment, 802.11g provides good speed and coverage, and 802.11n expands on that. If speed is a concern, go with n. If your laptops already have a b or g radio, then consider starting out with 802.11g and then upgrading in a year or so after 802.11n is finalized and the gear comes down in price.

Purchasing a Brand Name

Go to the store and you're going to see an assortment of products, all by different manufacturers. The first part of the selection process is finding which of these boxes have the features you want, followed by picking a manufacturer.

You're going to see a few manufacturers, some you recognize, some you don't. I recommend going with a name-brand product instead of a cheap, white, box knockoff, especially if you're choosing 802.11n. Have a look for the following:

- Do you recognize the manufacturer? Do you see the same manufacturer being advertised by different stores? If so, chances are it's a reputable brand that different stores are willing to stand behind. Also consider that an established brand has the resources and desire to maintain the software that makes your wireless card work.
- Does the manufacturer offer a toll-free support line? You may need to call for help at some point.
- Does the deal seem too good to be true? Cheap equipment is made cheaply.
- Do you see certification logos? This is your guarantee that the device will interoperate with other vendors' equipment.
- Do you need to supply other parts? Read the fine print carefully; sometimes items shown on the box aren't inside the box.

A few bucks extra on a name-brand device will almost certainly save you frustration down the road. Talk to some friends, neighbors, or coworkers to find out the brands that they like or dislike.

Routing and Bridging

You're going to have a network in your house, and it's going to connect to your service provider's network. To get between networks, you have to route. These networks are connected by a device called a router. This router is the part that lets you get out on the Internet. Routers also incorporate a firewall, which is a protection mechanism from the bad guys out there on the Internet. Pretty much every wireless router out there has a built-in firewall.

If you're connecting parts of your own network, you want to bridge. Maybe you're making your wired network bigger by adding more ports. Maybe you're adding a new wireless access point to an existing wireless network.

Take a look at Figure 2-2. The connection from the Internet service provider (which is drawn as a cloud, because you can't have a good network drawing with at least one cloud) comes in to the router. Anything to the right of the router is part of the internal network. On the internal network is a device called a *switch*, which allows you to add wired ports to a network. One of those ports connects to an access point, which brings in the wireless computers.

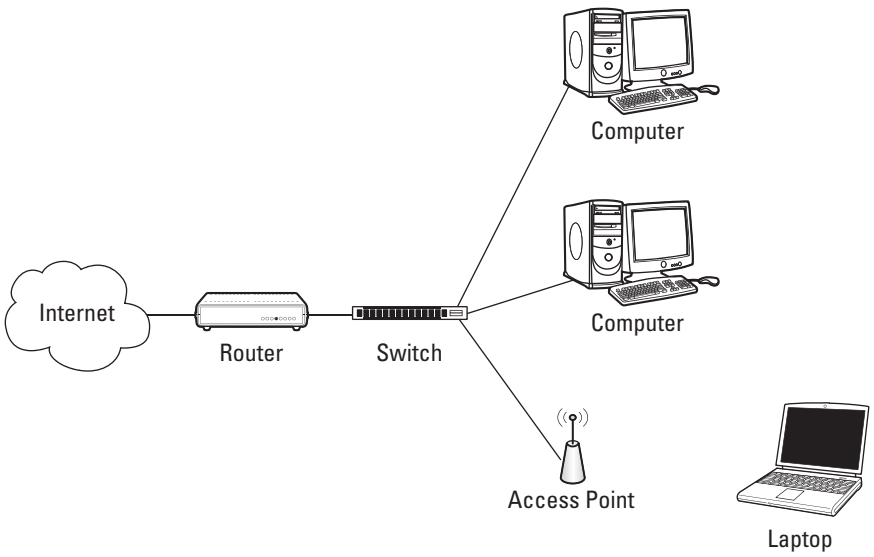


Figure 2-2: Routing and bridging.

The router is routing between the stuff on the left and the stuff on the right. The network on the right is made up of the switch, the access point, and all the computers. The switch and the access point bridge all their connections to each other, which is how a small network grows.

Thankfully, you rarely have to worry about this because most routers you buy combine the router, the switch, and the wireless access point. If you need to connect some wired computers in, then make sure your router has enough ports, or that you've got an extra switch that you can connect to the router to add the ports.

Expanding Your Wireless Network

Before you go thinking "my house is so big, one access point will never be enough," give it a try. You might be surprised at what one access point will do, especially if you're using 802.11n.

If that one access point leaves you with dead spots in your house, try moving the access point around (if you can), to see if that helps. Turning an

access point 90 degrees can make a difference. If that doesn't clean up those pesky dead spots, then you have to look at alternatives.

Upgrading your antenna

Your access point may have removable antennas, in which case you can try to find a better antenna. The short, plastic antennas that are what you probably got with your access point (the highly technical term for these are a *rubber ducky antenna*) are optimized to spray radio energy in all directions such as a big sphere. Other antennas are made to spray in one direction, or in a doughnut shape.

Changing your antenna is becoming a less attractive option as time goes on. Some access points have moved to internal antennae, and with the multiple antennas in 802.11n, replacing several antennae is just a pain. Adding more devices is becoming so cheap that worrying about your antenna is probably not worth it.

Repeaters and range extenders

The easiest approach is to add repeaters, or range extenders, to your network. These devices listen to the existing wireless network and rebroadcast the signal. Because of this, you can expect a repeater to increase your wireless range by about 150 percent in one direction, as shown in Figure 2-3.

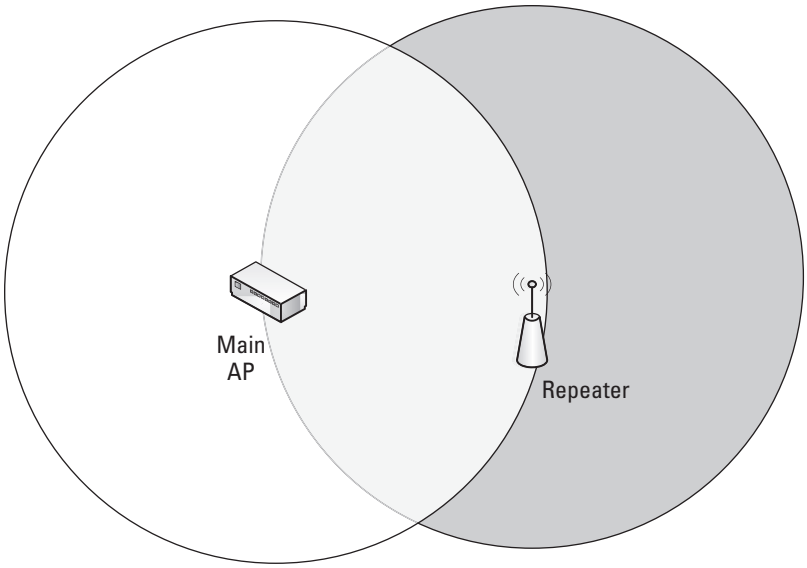


Figure 2-3: A wireless range extender in action.

Wireless range extenders are the easiest way to get what you want, even though they're not the most efficient way about going about it. As you can see from Figure 2-3, the range extender has to be inside the coverage area of the main access point (white circle). This scenario has a fair bit of overlap between the two radios: a large part of the extended coverage area (dark circle) is already covered by the main access point.

When shopping for range extenders, also remember that some wireless access points can be configured as a repeater, which is the same thing. They both do a fine job of extending the signal, but knowing that you have the two options helps you comparison shop.

Creating multiple access points

The solution that gives you the best range is to use multiple access points and then to bridge them together. Figure 2-4 shows how this works.

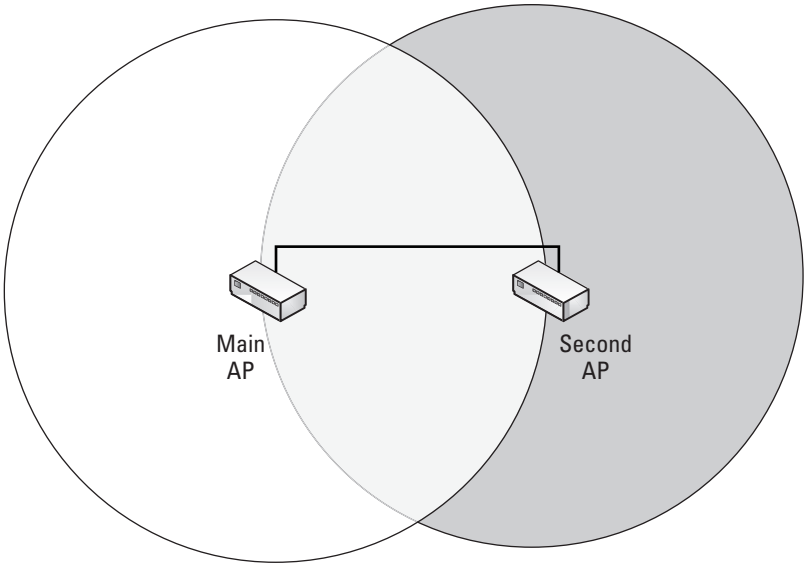


Figure 2-4: How to connect multiple access points.

This option reduces the overlap between the two wireless zones because the two access points don't have to *see* each other over the wireless network. However, the two access points must somehow be connected over the wired network. Given that the benefit of wireless is avoiding wires, this option is cumbersome to set up. Figure 2-4 does show some overlap between the two access points, so that there is no dead zone between the two.

Multiple access points can also be helpful if an entire floor is inaccessible from the main access point. A repeater won't work in your basement if the

signal isn't strong enough, and your only option might be to run a cable between two access points.

Dealing with Wired Devices

After all this talk about wireless, you still have to deal with some wires. You may have a PC or a video game console that doesn't have a wireless adapter.

Consider replacing your computer with one that has built-in wireless capability. But if you can't do that, you got three options:

Wire it, upgrade it, or bridge it.

Wiring a computer

The first option is to simply embrace your device's lack of wireless and run a cable from your router to computer. Your router probably has a switch built in, which is a device that's there to provide several wired ports. Figure 2-5 shows the switch ports on the back of a router.

Figure 2-5: Switch ports on the back of your router.

In theory, wiring a computer is easy. If your computer is in the same room as the router, then run a cable of appropriate length between the two devices, and you're set. If your computer is in another room, you'll have to think of the least disruptive way to get there. The cable simply plugs into one of the switch ports on the router on one end, and into the Ethernet port of your computer on the other.

Run the cable along the baseboard of your wall if you can, or under a strategically placed rug. Avoid bare cable, it just looks bad and people tend to trip over them, especially when carrying fragile things. If you do have to drill, try to drill in closets to avoid an ugly mess.

Speaking of cable, you want Ethernet cable rated at category 5e. You may also see category 6 cable or some fancy thing with connectors coated in precious metals, but for a home network you'd just be throwing your money away. Even better, find a friend with cabling experience to do the work for you in exchange for dinner.

Wiring up your computer works, but you bought a book on wireless networking, not wired networking. Unless your computer is really close to your router, avoid the mess and pick one of the other options.

Upgrading a computer

Most computers have some expansion slots that let you add peripherals, such as network cards, to your computer without having to buy a completely new computer. With this option, you go out and buy the appropriate adapter for your computer, and then install it.

The key here is to make sure that you've got the right adapter for your computer. Computers are getting faster and smaller, and the expansion cards follow the trend.

Desktops

Desktop computers have two options, depending on the capabilities of your computer and how much work you feel like doing.

The traditional method is to install a PCI card (that's peripheral component interconnect, for those of you who need to know these things), which is a card that goes into specially designed slots right on the motherboard of your computer. The slots are aligned such that one edge of your card sticks outside your computer's case, which allows for easy connection of an antenna. (Chapter 1 of this minibook shows a PCI-based network card.)

Most computers that you buy will have a free PCI slot, but the only way to make certain is to check. You should see at least one blank panel on the back of your computer (it's about 4 inches high and slightly over half an inch wide). If you open your case, you can see an empty slot for the card.

Opening the case isn't for everyone, and improvements in the Universal Serial Bus (USB) have made it possible to get the same speeds without the hassle. If your computer has a free USB 2.0 slot then you can buy a USB-based card for around the same cost as an internal one.

Figure 2-6 shows the USB slot from a typical desktop computer.

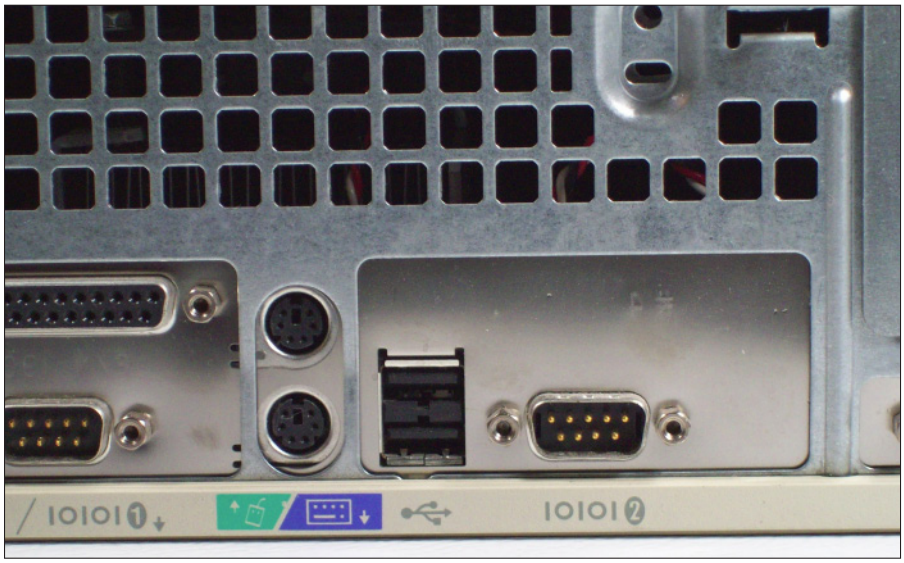


Figure 2-6: USB slot on a desktop.

When buying an adapter for a desktop machine, be it USB or PCI, keep in mind where your computer is and where the antenna would be. An antenna that's buried under a pile of books, or is stuck in a cabinet, will not perform as well as one that's got room to breathe. I'd recommend an external antenna with a cable for PCI cards.

USB adapters are also used with laptops, so are often designed to be small. You can take a USB adapter with an integrated antenna and attach a USB extension cable to it if your desk layout hides the antenna. Your adapter might come with this cable — check the box to make sure.

Laptops

Laptops follow the same idea as desktops; however, the technologies are different. If your laptop doesn't have wireless built in (or it's an older technology and you want to update), then you can go down the USB route, or an adapter.

USB devices for laptops work the same way as they do on desktops, except that you want something that's small and unobtrusive. Before you buy, look at where your USB ports are. If you dock your laptop, consider whether or not you need wireless while docked.

The other option for laptops is a peripheral card, much like the PCI card from a desktop. Laptops are a bit more refined, though; they have standard card types that plug into the side of the computer.

There are currently two popular types of laptop cards — the PC Card (sometimes called CardBus) and the ExpressCard. ExpressCards are a newer (and by newer I mean faster) version of PC Cards. The name is also better, don't you think?

Laptops have been shipping with ExpressCard since at least 2005, so chances are you already have an ExpressCard slot. You might also have a PC Card slot. The two types of cards are available in the same width (and not compatible), so it's not obvious from looking which one you have.

If you look at the pins inside the slot for the card (you might need a flashlight, and will certainly need to pop out the plastic holder), you find that PC Cards have a wide connector, almost 2 inches wide, and have protruding pins. The ExpressCard's connector is slightly over an inch wide and has more of a card interface.

To make things even more confusing, ExpressCards come in two widths. One is the ExpressCard/34 which is slightly over an inch wide (34 millimeters for those of you who understand metric), and ExpressCard/54, which is about 2 inches wide. The connector is the same, but you can't use the 54mm card in a 34mm slot! There should be a plastic guide inside the slot, though, that allows you to use the 34mm card in the 54mm adapter. Figure 2-7 shows the two ExpressCard variants.

Figure 2-7: PC Card and PC ExpressCard compared.

When in doubt, check out the documentation that came with your computer, especially the sales brochure.

Bridging a computer

Bridging is remarkably simple — you buy a device that speaks wireless on one side and has a network jack on the other. This device bridges the wireless to the wired, so that the computer thinks it's on a wired network, but everything it sends goes out to the wireless network.

This option is great for video game consoles, where you may not have flexibility in what you can add. Some models can behave as a bridge for use at home and a standalone access point if you and a bunch of friends decide to get together with your consoles or computers and play multiplayer games.

Chapter 3: Setting Up Routers

In This Chapter

- **Unpacking your hardware**
- **Plugging equipment together**
- **Configuring your router**

If you're ready to set up your router, you likely have all the equipment you need. For most of you, this will be the most foreign part of the whole process. Don't worry! In terms of difficulty, I rank this as easier than setting up a home entertainment system and slightly harder than falling off a log.

In this chapter, I discuss the router. If you bought some network adapters, you can set those aside for now. First, you get acquainted with the equipment, and then I explain how to put it together and get it going!

For those of you with foggy memories, or who skipped ahead, the router is the device that connects your home network to the Internet. The router hides all your internal computers and acts as a firewall, which helps to protect you from the bad guys out there. Your router probably has wireless built in, so it's going to take care of getting your wireless computers connected.

Unpacking the Box

Clear off a table and start unpacking the router box. You should see

- A router (if you don't see this, then pack everything up and take it back to the store)
- A power supply
- A network cable (3-inch to 6-inch long, with a square plug on each end)
- CDs and documentation
- Antennae, depending on the router you bought

Your box might come with some other goodies, such as a network card, if you bought a combination package, or some other odds and ends that the manufacturer threw in.

Handle with care

If your cable or DSL modem isn't in a good spot, then you might consider moving it somewhere better.

Moving a cable modem means that you have to find another cable jack in the house and plug the cable modem into that jack. Be careful, though, especially if you had someone from the cable company come out and set up your equipment. The installers for cable modems optimize your house wiring to give the best signal to the modem, so changing jacks might hurt your Internet speeds. Thankfully, you can just move things back if something goes wrong, or call your provider for a signal check if you're unsure.

For ADSL setups, you can move your modem to any phone jack. You have to make sure that all the other phones in your house have a filter on them, which prevents noise from the phone from interfering with the Internet signal.

Figuring Out Where to Put the Router

The router needs to be placed close to where your Internet service provider's equipment (such as a cable modem or an ADSL modem) is located. Ideally, this area is as close to the center of your house as possible, to maximize the wireless range.

So, you've found a central location with a bit of breathing room for the router. It's near a power outlet, and is out of the way enough that you're not going to trip over it.

Grab some masking tape and a marker before you start setting things up. Tag your cables as you go along so that someone looking for a free outlet doesn't pull your cable modem's plug, or you don't forget which port plugs into what, should they get separated.

Plugging Everything Together

Before you start hooking equipment up, throw together a quick picture of what you're trying to build. Figure 3-1 shows an example of a network.

Starting on the left, you have your cable modem, which is probably already plugged into your phone or cable line. The cable modem hooks into the external side of your router. Your router connects wirelessly to your workstations, and optionally through a wired interface to any devices that need it.

While you're configuring your network, you can connect your PC to the router using an Ethernet cable. After you've set up the router, you can begin using your wireless network.

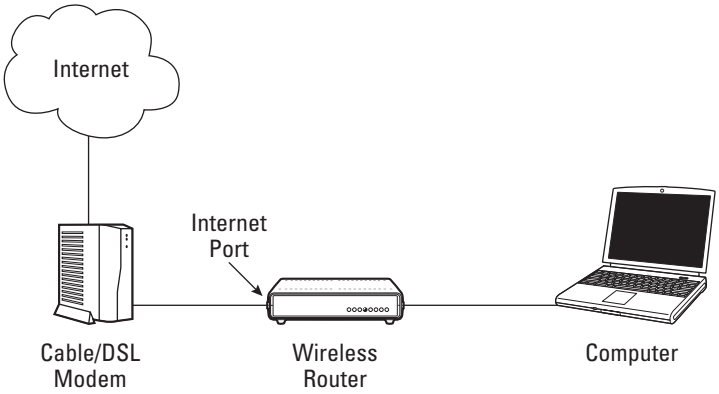


Figure 3-1: The plan for your new network.

Connecting the router to the Internet

Your cable or DSL modem will have one Ethernet cable coming out the back of it. To help you find it, I've taken a picture of my cable modem in Figure 3-2. An Ethernet jack looks a lot like a regular telephone jack, except the Ethernet jack is wider than the phone jack.

Figure 3-2: Finding the Ethernet jack on a cable modem.

Your router has several Ethernet jacks on it. Your router connects your internal network to the Internet. It's expecting the Internet to be on a certain port. This port might be labeled:

- Internet
- Outside
- WAN
- External

Whatever it's called, this port is marked differently than the other ports.

1. **Plug the router's Internet port into your cable or DSL modem's Ethernet port.**
2. **Hook up the power adapter to your router and give it a few minutes to get started.**

   You should see lights on both your cable or DSL modem and the router, indicating that a connection was made. Sometimes the light is right underneath the port itself, sometimes it's on the front of the device.
3. **Unplug the power from your router until you're ready to set it up.**

When plugging in an Ethernet cable, it should click. Give the cable a gentle tug. It should not fall out of the port that it's plugged in.

Plugging your computer into the router

Now that you've found the Internet port on the router, the inside ports should be pretty easy. They are likely numbered and in a group, possibly with a label like Ethernet.

Plug a cable from your computer's Ethernet port into the first Ethernet port on the router. Now you should have something like Figure 3-3.

Congratulations, the hardest part is over! It's time to configure the router.

Figure 3-3: The laptop, router, and cable modem all hooked up.

Configuring the Router

With your router at default settings, you might be able to turn your router on and be on the Internet in a matter of minutes. Even if everything works for you, going through the configuration steps is a good idea. Doing so improves your security, you can upgrade your router's software to the latest version, and you might even find it fun!

Depending on the router you buy, it may come with a CD that takes you through the configuration section. Feel free to use it, because they generally do a good job. You should still read through this section because it describes the settings you want to look at, and you may have to resort to the method we describe below.

I'm also using a Netgear router. If you have something different, the screens will look different but the process will be similar.

If you are having problems with a step here, jump over to Chapter 8 for some troubleshooting information.

Logging into the router

Your router is configured by using your Web browser by entering a URL pointing to the gateway. The URL you enter is either printed on the router or is in the manual that came with your router.

Maybe your dog ate your instruction manual before you got a chance to copy down the URL, and it's not on your router. That's fine — there's a way to find it.

1. **From the Windows Start menu, click on Run.**

   A pop-up box appears above the Start button, asking which program you want to run.

2. **Type in cmd and press the Enter key.**

   A black window opens.

3. **Type ipconfig and press the Enter key.**

   I've pasted what I see.

Your window should look something like Figure 3-4. Look for the line starting with Default Gateway. The gateway is 192.168.1.1, which is the address of my router.

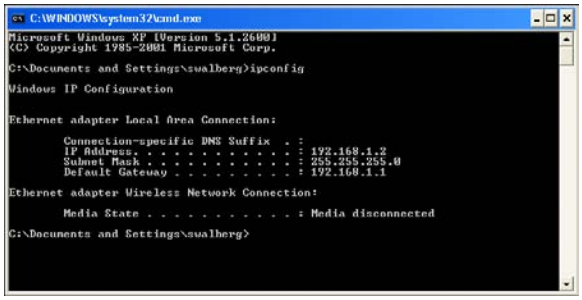


Figure 3-4: Determining your IP address and gateway.

If you don't have an address, or it starts with 169.254, then make sure that your computer is properly connected to the router. You see a status light on both the router and the computer's Ethernet port if you have a connection.

Whichever way you find it, open up your Web browser and enter the address of your router. On my Netgear router it is `http://routerlogin.net`, but it works just as well with `http://192.168`.1.1 that I learned earlier from the ipconfig command.

After connecting, you are challenged to log in, as shown in Figure 3-5.

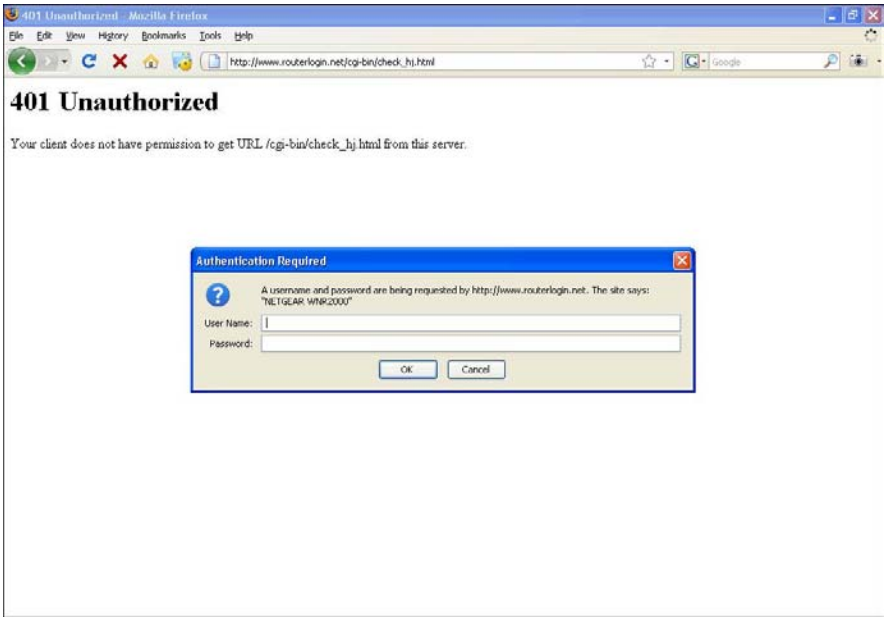


Figure 3-5: The login screen from a router.

The password is printed on the router or in the manual. You can also try a username of *admin* and a password of *password*for many models.

If you lost your manual, the site `www.routerpasswords.com` has the default username and password for many models of routers.

After you've logged in, your router will probably check for software updates. If you are prompted to upgrade your router, you should do so. If you got an error that no Internet connection could be found, don't panic! You might need to make the changes in the next section.

After the router upgrade completes, for better or worse, you are sent to the wizard (no, not the pointy hat kind! I mean the menus that help you set up your Internet connection).

Setting up the Internet connection

The first stage of the configuration wizard is the Internet setup. Figure 3-6 shows the initial question that asks if you want the router to determine the Internet connection type.

Let the detection process proceed, because it can save you some time. After the detection runs, you are given an option to review your settings and to fill in any missing information about your Internet connection. Figure 3-7 shows the configuration screen for the Internet connection.

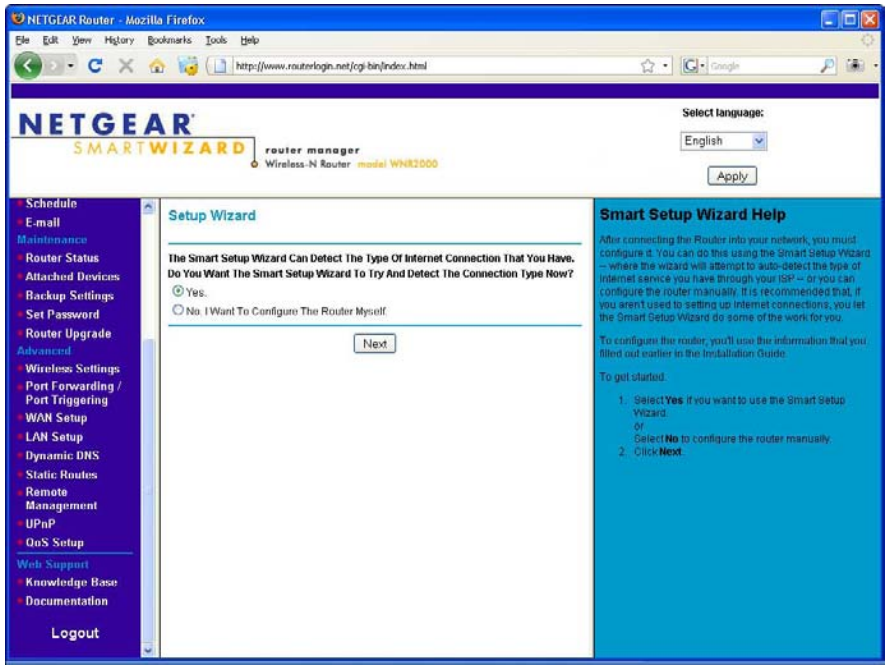


Figure 3-6: To auto-configure, or not?

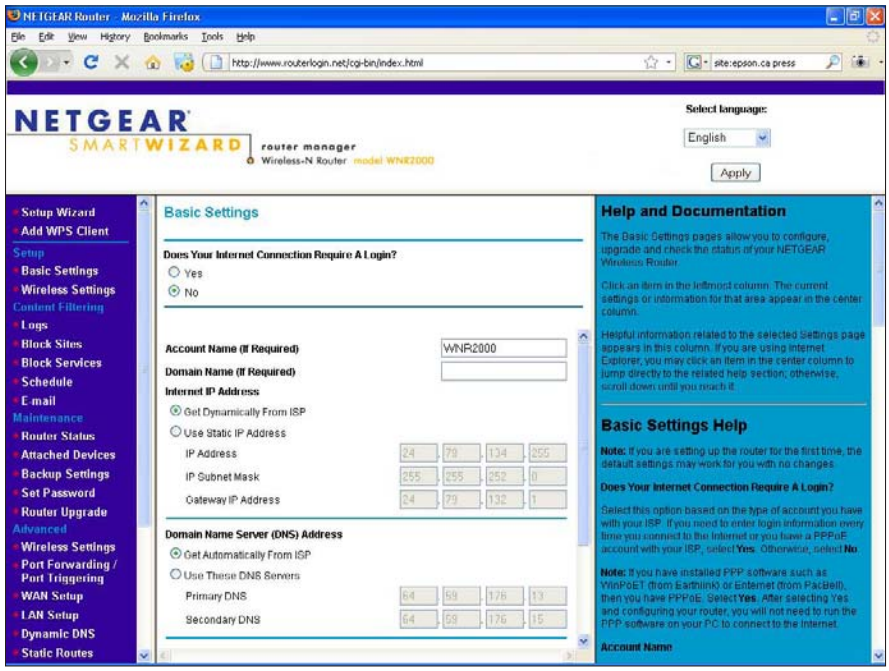


Figure 3-7: Internet configuration screen.

The Does Your Internet Connection Require A Login option is set to No. The Internet IP address is filled in (but grayed out) because the router detected the Internet connection properly.

Do you need to log in?

Cable Internet generally doesn't require a login. If you have ADSL, it depends on your provider. If your ISP gave you a username and password when you signed up, or if the detection failed, then you probably need a login. If you had to run software such as the WinPoET on your computer to get on the Internet, then you need a login.

If you do need a login, follow these steps.

1. **Select Yes at the Does Your Internet Connection Require a Login question.**

   Your screen changes to something such as Figure 3-8.

2. **If your ISP is listed in the ISP section, select it.**

   North American users typically use the PPP over Ethernet (PPPoE) protocol to log in, which means you select Other for your ISP. For those in Europe or Australia, you probably use PPTP (Point to Point Tunneling Protocol). When in doubt, call your ISP and ask.

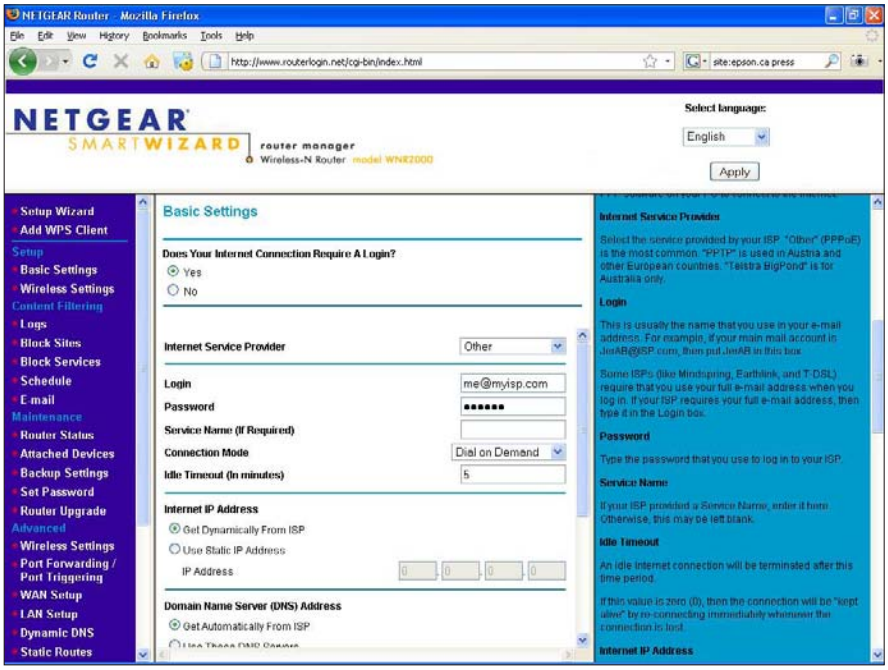


Figure 3-8: Entering your login information.

3. **Enter the login information your Internet service provider gave you, and then scroll to the bottom and select Apply.**

   Doing so resets your router.

4. **Confirm you have an Internet address by selecting Router Status from the main menu.**

   If all went well you see an address on the Internet port. The status light on the router corresponding to the Internet port also changes to green.

If you ran software on your PC to log in to your ISP, then you can uninstall it now. Your router is taking care of logging in for you.

Congratulations, you're on the Internet!

Working with your ISP

Some Internet service providers are picky about who they let on the Internet and will not let you on from a different computer. This situation is most often the case with cable modems, because the ADSL service with a login identifies people by the login. From the ISP's perspective, your router is now the only person using the Internet because all your local devices are hidden behind it.

The first thing to do is to reboot your cable modem. Doing this clears out any computer associations should the restriction be made on the cable modem.

If that doesn't work, try plugging your computer directly into the cable modem (another reason I told you to label your cables!). If your computer works but the modem doesn't, then you need your ISP to intervene.

Give your ISP a call and tell them that you just installed a new router and are having problems connecting. Ask if you're being restricted based on your computer. Also let them know the outcome of plugging in the computer.

If you aren't getting anywhere with your ISP, and your computer works but the router doesn't, you can tell the router to act like your computer. Go back to the Basic Settings menu and scroll all the way to the bottom to the Router MAC Address section shown in Figure 3-9.

Increasing security

Security is a tradeoff between the risk of something bad happening and the frustration you're going to encounter trying to prevent it. We could talk for hours about all the things you could do to keep bad guys out, but in the next couple of sections, I focus on some simple fixes that can make a big difference.

Remember, you're never truly secure; all you can do is make your network hard enough to break into that the bad guys go somewhere else.

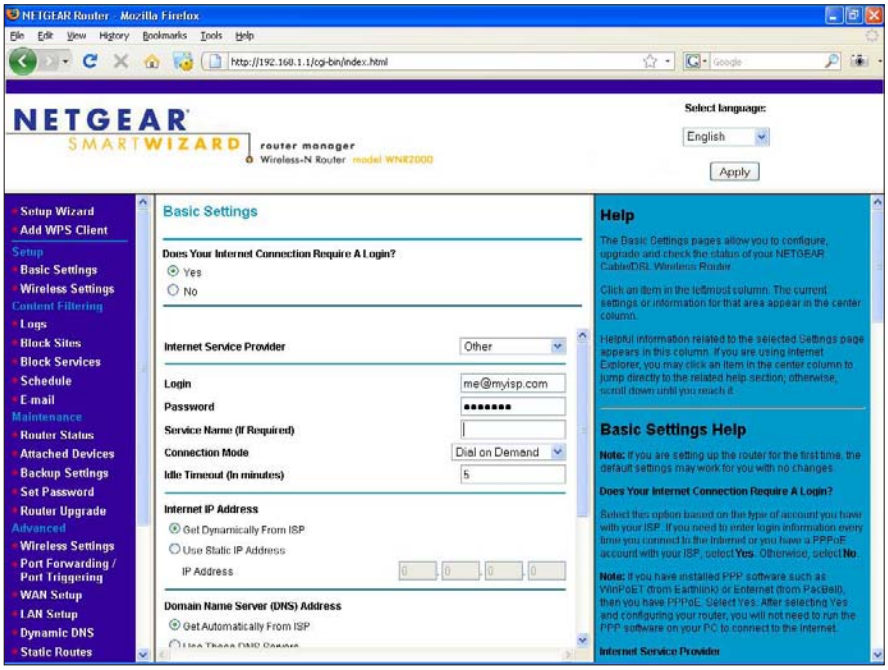


Figure 3-9: Changing your router's MAC address.

Changing the router login information

Most routers come with a default username and password of admin and password, respectively. Want to guess the first thing someone is going to try? That's right . . . "password" is a good way to describe what the word is, but as a password, it makes a bad one.

Change that admin password!

The screen to change your password is found under the Set Password menu item, as shown in Figure 3-10. You are prompted for your old password, which is probably "password" in case you've forgot.

Here's my advice for choosing a good password:

- Make it at least 8 characters.
- Put at least one number and one uppercase character in your password. Passwords are case-sensitive, so *G* and *g* are not the same.
- Make it memorable, but not obvious. If your name is Sarah, you might try something like saraH500. Maybe you like cats, so try 100Meows.
- Avoid too many letters that look the same, such a zero and a capital O, or the number 1 and a lowercase l.

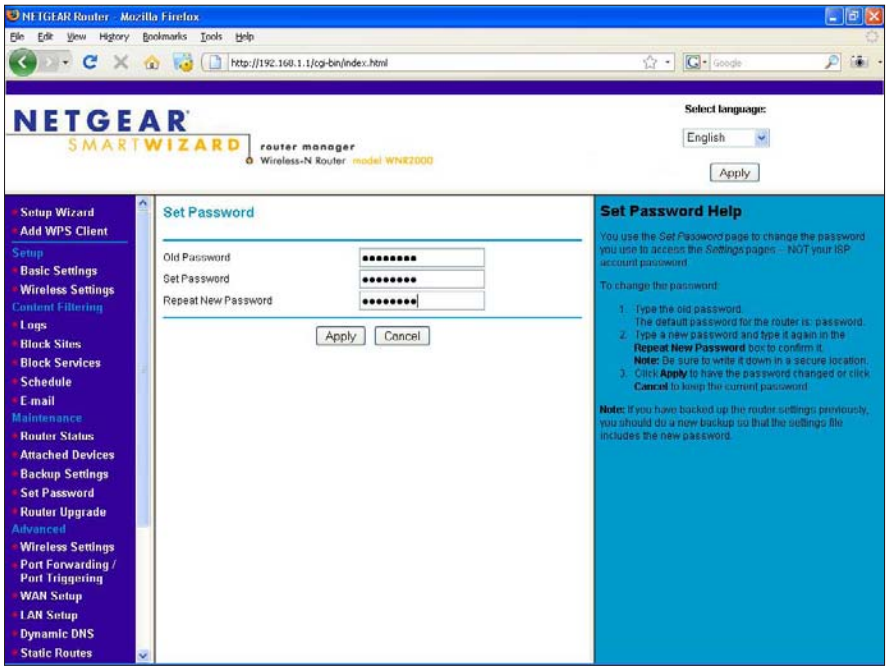


Figure 3-10: Changing your administrator password.

Finally, write the password down and put it somewhere safe (and somewhere that you'll remember). That's right, I told you to write the password down! Doing this is often frowned upon, but think of it this way:

- ✦ You're not protecting Fort Knox, it's your home network. That's not saying your personal stuff isn't important, but with a password that's good enough, you're still making it harder to get in. Remember that security is a tradeoff between safety and convenience.
- ✦ You're going to store the password somewhere safe, like a filing cabinet. You're not going to tape a sign to your front window with the password on it.
- ✦ Someone has to first get on your network before they're going to be able to log in to the router.
- ✦ If you're still paranoid, ignore my advice and make up a complex password. I won't be offended, really.

Keeping others out of your network

If someone could connect to your wireless network, he can surf the Internet from your ISP. That's not such a big deal, but you're now responsible for what they do. If something bad happens, the police will track the perpetrator back to your house. Then you get to explain to the police why it wasn't you.

Secondly, software is available that can intercept your network traffic. At best they see which Web sites you browse to, at worst they pretend to be your bank and rob you blind.

Protect your Network!

Figure 3-11 shows the Wireless Settings screen. At the top is the name of the wireless network called the SSID (Service Set Identifier). This makes your network unique. When you start off, it's usually set to the name of the manufacturer, such as Linksys or Netgear. Not only is a default SSID a magnet for hackers, it could cause conflicts if your neighbor is at the defaults, too. This setting is not a secret, so choose something obvious enough that if you saw it in a list, you'd recognize it.

Leave the channel at Auto — your router will choose the best channel to use.

For the mode, pick one of the higher ones. The options I get are 45 Mbps, 145 Mbps, and 300 Mbps. This is a wireless-N router, so it's capable of the full 300, but I'm in an area with some interference from neighbors so I dialed it back to 145. Try different settings and see which one works the best for you.

The security options dictate what sort of encryption level is used. None is the default and means that anyone can connect without a password. We know that's a bad thing.

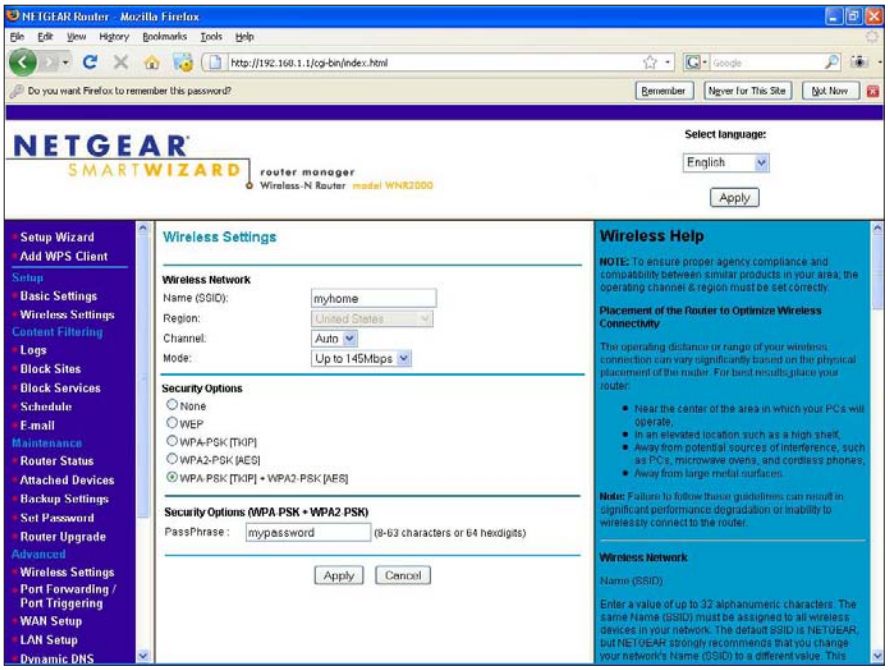


Figure 3-11: Protecting your wireless network.

WEP (Wired Equivalent Privacy) is old and broken. Someone sitting outside your house could break your password in a matter of a few minutes. I'm not even sure why vendors bother offering it; only ancient computers don't support anything better.

WPA and WPA2 (Wi-Fi Protected Access versions 1 and 2, respectively) are the current standards. WPA2 is newer and somewhat better, but some computers only support the original WPA. I recommend enabling both WPA and WPA2 — clients that support WPA2 will use it, and others will use WPA.

You see the box for the passphrase when you select one of the WPA options. A good password is the key to your network's security. You can write it down, but this Netgear router leaves it as plain text so you can look it up easily. (You have changed the admin password for your router, right?)

Dispelling a couple of myths

Wireless has come a long way since it first came out, and people have learned a lot about security over the years. The following list explains what not to do.

- Don't use WEP, use WPA2, or WPA if your computer doesn't support WPA2.
- Don't bother with restricting clients by MAC address. These addresses can easily be spoofed by bad guys.
- Don't hide your SSID; you just make it harder on yourself, and it's still easy for someone parked outside your house to find your SSID. Even the credit card companies have taken this restriction out of their requirements for businesses that take credit cards.

Chapter 4: Deciphering DHCP

In This Chapter

- **Discovering what a DHCP server is**
- **Configuring your DHCP server**
- **Finding out about the other settings that DHCP provides**

In Chapter 3, I explain how to set up your wireless router. And in Chapters 6 and 7, you discover how to set up wireless printers, computers, and even network-attached storage. But, before you can do this, you must first find out about addressing — the topic of this chapter.

The Internet works because everything on it has a unique address, and the devices that run the Internet are very good at getting information between two addresses. Before your computers and printers are ready to talk on your network, you have to make sure they have an address.

There's a protocol called DHCP, the Dynamic Host Configuration Protocol, that not only is the way to automatically address the computers on your network, but knowing the acronym is a great way to impress your geek friends.

Later in the chapter, I go over other related services that might come in handy some day.

Understanding DHCP

To first understand DHCP, you must know a bit about addresses. The most popular analogy is the snail mail system.

Through rain, sleet, or snow

To send a letter, you first put your message in an envelope, then you write your return address on the corner of the envelope and your recipient's address in the middle, and finally drop it in a mailbox. There's a stamp involved in there, too, but the Internet doesn't need stamps; they gum up all the gears.

Someone comes by and empties all the mailboxes into a truck. Trucks are emptied into a collection center. The mail is sorted based on the destination: envelopes are sent on trucks or planes at a facility that's closer to the destination, eventually working their way into a postal carrier's bag and in your friend's mailbox.

Finally, we talk about Internet addresses

As I said earlier, each computer on the Internet has a unique address, which is a number instead of a street name. Each time data (such as an e-mail) is sent over the Internet, the data is wrapped in a *packet* that has the addresses of the sender and the receiver of the packet. The devices that run the Internet look at that destination address and get the packet one hop closer to its destination. The next hop device does the same thing until the final hop — the destination — processes the message.

Incidentally, those devices that run the Internet are called *routers* and are similar to the one you have at home. The major difference is that the routers that run the Internet are more powerful because they have a lot more addresses to deal with, and yours only needs to worry about the one that your ISP gave you.

So, what does an address look like? You already saw one in the last chapter, where you ran the Windows ipconfig command. My address was 192.168.1.2, and I could see that the router's address on the wireless side was 192.168.1.1. My router also had a second (external) address that the ISP gave it, such as 24.79.42.159, which belongs to the cable or DSL side. The router's job is to send packets between these two networks, and it needs an address on each network to do that.

Hiding addresses

Earlier in this chapter, I said that every device on the Internet has a unique address. But you may have noticed that both your router and mine have an address of 192.168.1.1, which makes it not unique. What gives?

Your router also does something special called *address translation*. The networks starting with 192.168.x.x are meant to be private, that is, never seen on the Internet. Your router takes its address on the ISP side (such as 24.79.42.159, in my case) and uses that instead of your computer's address (such as 192.168.1.2) when relaying your packets to the Internet.

When responses come back, the destination is the router. The router remembers who was actually talking and changes the destination back to 192.168.1.2 or whoever was talking.

From your ISP's perspective, there's only one person using their service — your router. Clever, eh?

I still remember my first job out of school, which involved managing a small network. About 40 computers were on the network, and every time I added a new one, I went to a spreadsheet, picked the next available address, made a note in the spreadsheet, and then set up the computer with that address.

Manually specifying addresses is time consuming and error prone. If two devices on the same network try to use the same address, neither of them can talk. Additionally, some of the possible addresses are invalid, and using one will cause problems on your network. Addressing is clearly a job for a computer, not humans.

DHCP solves these problems by letting a computer hand out the addresses. This computer keeps track of who has which address and periodically makes sure the addresses are still in use. DHCP is simple enough that it's built into almost every router on the market, so you can probably start using DHCP right away.

At a high level, when your computer starts up, it sends a message to all the computers on the network that says "I need an address!" If there's a DHCP server on the network, it finds a free address and responds with, "Here, have this address!" Your computer responds with, "Thanks!"

Sounds like a breeze, eh? Of course, it's more complicated than that, but you don't have to worry about the gory details. Understand, though, that DHCP is an ongoing thing. Your computer must periodically remind the router it's still there, otherwise the router will reclaim the address for someone else. This usually happens every 12 to 24 hours and is handled automatically by your computer.

The last thing to remember is that it generally doesn't matter what address your computer has, as long as all the rules are followed. DHCP makes sure you follow the rules, so it doesn't matter if one day you're 192.168.1.2 and when you boot up the next day you're 192.168.1.50.

Your DHCP server

By default, your router almost certainly has DHCP turned on; otherwise, you wouldn't have been able to connect to your router in the first place!

Jump over to the Advanced LAN settings of your router, which I've shown in Figure 4-1.

In Figure 4-1, you see that familiar 192.168.1.1 address, which is the IP address of the internal side of your router. That address stays constant even though the rest of the addresses on your network will be dynamic. The reason is that the computers need to find your router by its address in order to get out on the Internet.

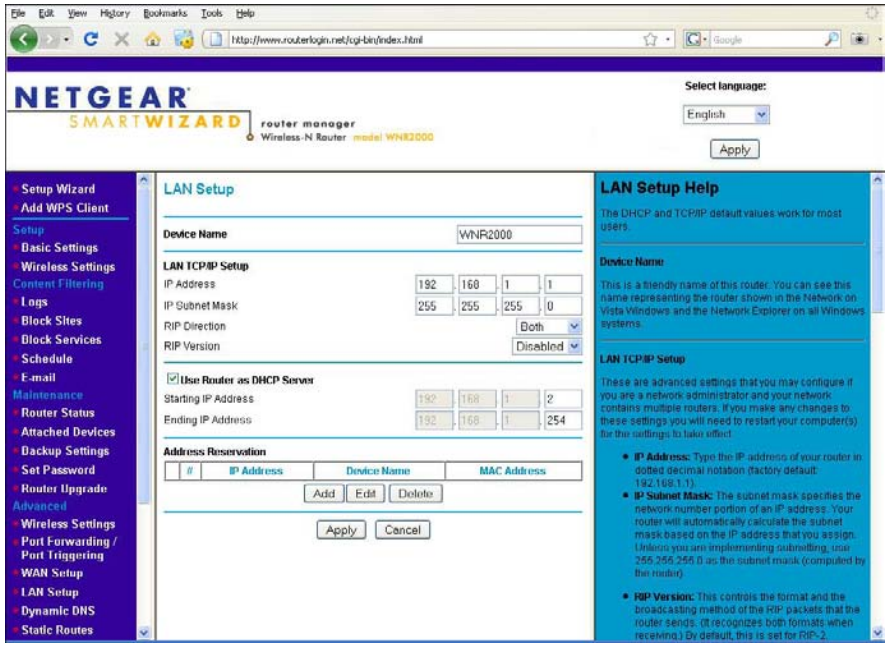


Figure 4-1: Advanced LAN settings.

Don't worry about the subnet mask; it just tells your computer how big the network can get (big enough). And that RIP stuff, pretend it's not there.

What you're really after is the configuration on the second half of LAN setup, starting with Use Router as DHCP Server. This option is selected, and it turns on and off the DHCP functionality. If for some reason you want to turn it off, you deselect this button and click Apply.

Underneath the DHCP on/off switch are two lines that let you set the range of addresses that DHCP uses. You can see that the first three boxes are grayed out, and they happen to have the same values as the IP address of the LAN interface. This is intentional; if you were to change one of those values, you'd be handing out invalid addresses.

You can only change the last value, which can be a number from 1 to 254. Number 1 is already taken by the router itself, so this router is already handing out the maximum number of addresses. These addresses start at 192.168.1.2 and go up to 192.168.1.254, for a total of 253 possible addresses.

Underneath the starting and ending address fields is a place where you can reserve addresses for computers, so the same computer will always get the same address. Just hold on to that thought.

Turning off DHCP

After all that talk about the great things DHCP does, why would you want to turn it off? You probably don't *need* to, but DHCP can get in your way. Int the following sections, I go over some ways to make your new life with DHCP work for the best.

Reserving your spot on the network

Sometimes you've got some software that needs you to do something called *port forwarding*. This means that the router is going to let some connections from the Internet directly into your computer. I'm not going to get into port forwarding in this book, but your software manual has more detailed instructions on what's needed to make it work. Port forwarding needs an address on your network to which to forward the packet.

DHCP gives out addresses that can change. If your router is trying to send a packet to one address, and you've got a different one, what do you do? Turn off DHCP? No!

What if you could still use DHCP but be guaranteed the same known address all the time? No one else would be handed out that address. That's called a reservation. You're simply reserving the address from the DHCP server.

Go back to Advanced LAN Setup and click Add. A screen like the one shown in Figure 4-2 appears.

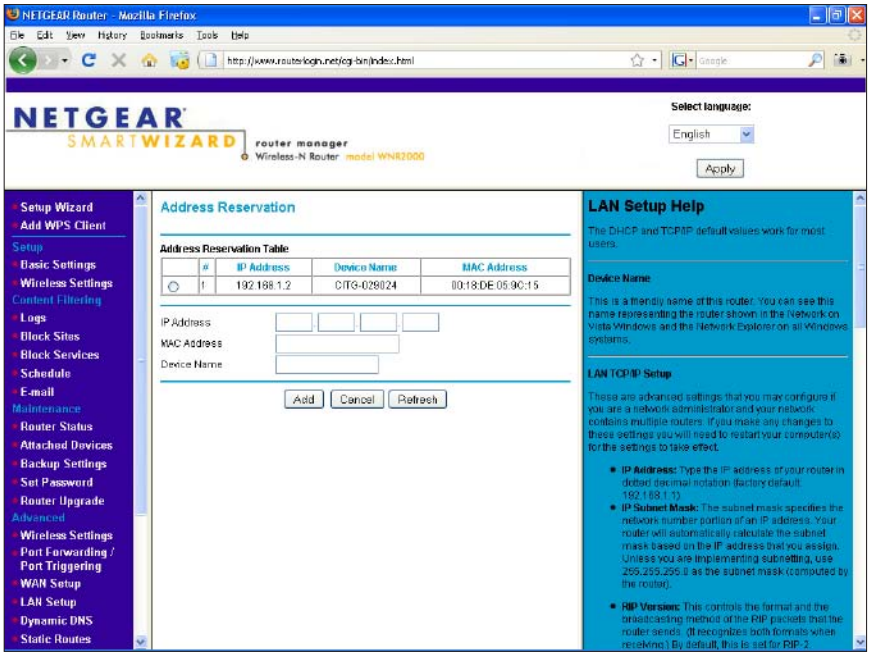


Figure 4-2: Adding a DHCP reservation.

You need the IP address you want to give your machine, your computer's MAC address, and your computer's name to complete this form. *MAC* stands for Media Access Control, and it is part of a protocol that defines how networks work. It's also something you'll be able to forget about except for this one trick: To find out your MAC address, open a command window (Start➪Run➪cmd) and then type `ipconfig /all`. Figure 4-3 shows the result.

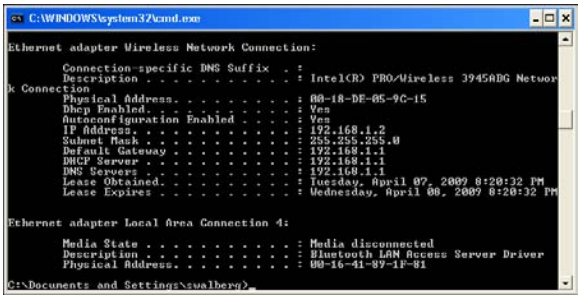


Figure 4-3: Results of *ipconfig /all*.

Look for the line that says Physical Address. Mine is 00-18-DE-05-9C-15 Type that address in the MAC address field, along with your IP address and name, and click Add. Presto! That address is yours forever.

You may be noticing in Figure 4-2 that my MAC is listed right above the field. In fact, if you click the radio button on the left side of that table, it'll even be prefilled in the form, effectively letting you make any dynamic address permanent with two clicks.

It's good to know how to reserve an address the long way, because not all routers support that shortcut.

Just give me static!

In the context of computers, static electricity is usually bad. Static addresses, though, aren't. Sure, they're harder to manage, but if only there were some way we could make them work without having to turn off DHCP.

This one is fairly easy to solve. When looking at the DHCP configuration, you saw that you could change the range of DHCP assigned addresses. Change it to give some space on one side, such as lowering the upper limit to 199. DHCP still offers addresses from 192.168.1.2 to 192.168.1.199, and anyone that wants to put their address in manually can use 192.168.1.200 to 192.168.1.254.

Some network-attached printers don't understand DHCP and need to be addressed statically. The same goes for much older computers, especially computers designed to be servers and not for daily personal use. Fair enough, just give them an address in your static range.

If you do break out a separate area for statically addressed machines, it's a good idea to make a note of it somewhere.

DHCP, get out of my hair!

Sometimes you just want to turn off DHCP. You only want one DHCP server on your home network. If you have another device that's doing the job of DHCP and you plug in your device, then you'll have two devices handing out addresses.

DHCP is so simple that most devices come with it turned on. As you add more pieces to your network, you'll probably come across the situation where you get two DHCP servers. Make sure to turn that second (or third, or fourth) server off.

As a case in point, these combination router–access point–switch devices are roughly the same price as an access point, so you might just come home one day with a second router to expand your new wireless network. Configure wireless, turn off DHCP, and give the new router a different static address, and you can plug it into the rest of your network as if it were an access point. Just remember to leave the Internet port unplugged, because your first router is providing the path out to the Internet, and the new one is bridging your computer between the wireless and wired inside networks.

But wait, there's more!

Looking back at the results of *ipconfig /all* from Figure 4-3, a bunch of other information is there. Most of it isn't that noteworthy, but tI discuss two in the following sections.

Default gateway

The Internet is one big game of Hot Potato. One guy throws his packet to a router, who throws it to the next router down the line, all the way until it lands at its destination. To join in, you have to know where to throw your packet.

Your default gateway is the place that your computer sends all the packets it doesn't know what to do with (for people on your local network, you can talk directly to them). DHCP tells you the address of your gateway when handing out the address. You can see that this address is 192.168.1.1, which is your router.

Without a default gateway, you're not going to get on the Internet.

DNS servers

This chapter has talked a lot about addresses like 192.168.1.1, but you've probably never typed one into your browser. You've always typed URLs like `http://example.com/`, right?

DNS, the Domain Name System, is what translates those names that you understand into the numbers that computers understand. It's like the phone book of the Internet.

Most routers make themselves the DNS server and relay your requests to your ISP's DNS servers. Sometimes they just tell you to talk to your ISP's name servers directly by handing out those addresses. Either way is good.

The funny thing about DNS is that you can be connected to the Internet, but without DNS, you'll get nothing but errors when you try to do anything. That's because your computer has no way to figure out how to convert the names to IP addresses, and you probably don't know the addresses off the top of your head, either. The address is required for your computer to connect to your destination, such as a Web server: a name won't cut it.

Troubleshooting DHCP

If you get an address through DHCP, then DHCP is working great. It's pretty simple that way.

With DHCP, you usually don't end up without an address. If there's a problem, your computer will assign itself an address starting with 169.254, which is called the *autoconfigure address range*. This address isn't helpful, because it's not one of yours and therefore can't be used to talk to the Internet.

If you get this autoconfigure address, then make sure you're within range of your access point. Sometimes you get enough strength from the wireless signal to see the other side, but not enough to have any meaningful conversation, such as the whole, "Hey, I need an address" song and dance that starts things off.

Other times, the problem is related to your wireless drivers, especially if you're trying to get equipment from two different vendors to play nicely together. You need to check to see if you can hookup using a wired connection, and download some updated drivers.

Of course, if you've turned off DHCP on your network, or never had it in the first place, you'll see a lot of those 169.254.x.x addresses until you set up a static address or turn on DHCP.

Chapter 5: Installing Your Wireless Adapter

In This Chapter

- **Installing PCI-based network adapters**
- **Installing laptop expansion cards**
- **Installing USB adapters**
- **Configuring drivers and wireless utilities**

After your wireless router is up and running, you are ready to install the wireless network adapters. Unless you were fortunate enough to have wireless functionality built into your computer, you're going to have to plug something into your computer so that you can get on the wireless network. That something is a wireless adapter, and they come in all shapes and sizes. In this chapter, you find out how to install different kinds of network adapters.

Installing a USB Adapter

USB adapters can be used in both laptops and desktops. Some USB adapters are sleek, little numbers that are designed to be unobtrusive in a laptop, and some are larger but flatter and are designed to be hidden on a desk. They're easy to install in either case, which is why we're looking at them first.

The USB adapter I've been working with is from NETGEAR and is of the laptop variety. However, it includes a USB extension cable and a simple bracket designed to be Velcroed to the wall, so it'll work equally well on a desktop. Have a look at Figure 5-1 to see what I mean.

A spare USB port is, of course, a prerequisite for a USB adapter. If you have USB ports but none are free, consider an inexpensive USB hub that splits one port into four (or more). If your computer doesn't have USB, the only way to get a port would be to add a PCI expansion card.

USB devices are *hot swappable*, meaning you can insert and remove them without powering down your computer. Be careful about the removal part, though; if you're storing anything on the USB device, it might get lost unless shut down properly!

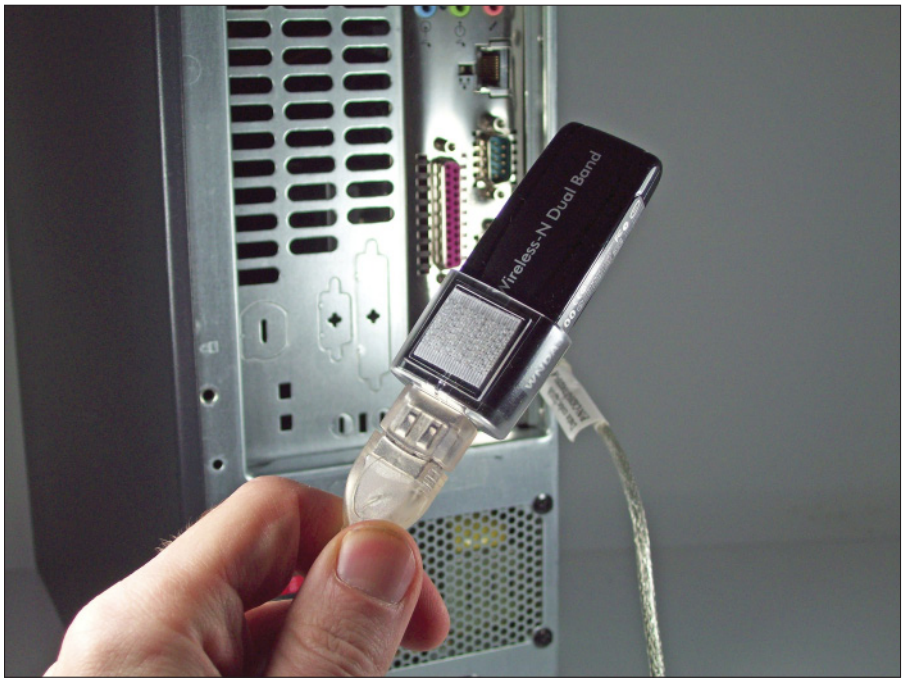


Figure 5-1: A laptop USB dongle that's attached to a desktop.

Installing the drivers first

As magical as it might seem, your computer needs to be told how to do everything through software. You're probably familiar with installing application software such as a word processor, spreadsheet, or games. Another class of software is called *drivers*, which are smaller pieces of code that tell Windows how to work with hardware. Chances are the piece of equipment you just bought came out after Microsoft released your version of the operating system, so Windows probably doesn't know how to deal with your new card without the right drivers.

In some cases the hardware is generic enough that Windows will work fine using its default set of drivers. If the hardware I'm installing includes its own drivers, I always use those. Vendor-supplied drivers are going to have the latest fixes and are usually faster than a generic version. After all, if the vendor made the hardware, I trust its drivers.

When installing the vendor's drivers, you usually get the opportunity to install the vendor's wireless management software, which is much better than the software built into Windows. It's a win-win situation.

1. **Load the CD that came with the adapter into your computer.**

   After you load the CD, the setup wizard starts. (See Figure 5-2.)

Figure 5-2: Starting the USB wireless wizard.

2. **Select the Install from CD option.**

   The wizard is helpfully offering to check for a newer version of the drivers. Because this computer doesn't have any Internet connectivity (yet), the check would fail.

3. **Accept the license agreement and default installation path.**

   The wizard reports that the software is installed, as shown in Figure 5-3.

Figure 5-3: The driver software has completed installation.

4. **Click Next to confirm that the software has been installed, and proceed to the next step.**

   You are asked to plug in your USB wireless adapter. If you got ahead of the game and did this earlier, don't worry, things can still work!

5. **Plug your USB wireless adapter in now. If you need help, see the next section, "Plug in the adapter."**

6. **Click Next.**

   A legal message appears, as shown in Figure 5-4.

Figure 5-4: You're not going to use that in Japan, are you?

7. **After you agree not to engage in any radio warfare, you're asked if you want to use the built-in Windows configuration (Figure 5-5) or to install the vendor's package (NETGEAR Smart Wizard in this case). I always install the vendor's, so select that option and click Next.**

Understanding legal restrictions

Despite the various 802.11 standards being agreed upon internationally, some federal governments have slightly different limits on which frequencies can be used. As a result you get some oddities where some of the higher 2.4 GHz frequencies are legal in Japan, but not the United States, so they get a couple of extra channels than us.

If you're prompted with a legal message like the above, it's best just to fill in the proper country and rely on the software you just installed to know which frequencies can be used.

Figure 5-5: Choose the vendor's management software.

At this point your wireless card is installed and ready to go. If you continue along with the wizard, you'll be able to get online right away. I'm going to stop here and pick it up again in Chapter 6, though.

Plug in the adapter

Identify the USB port on the back of your computer and plug in the USB adapter (or the cable, if you're using the cable.) It should take only slight pressure, so if it's not going in right, try flipping the adapter over. If you think pliers might solve your problem, you're probably wrong.

Figure 5-6 shows me plugging in the cable to a USB port on my desktop.

Your computer will probably emit a satisfying beep indicating the adapter was inserted correctly, and then you're off to the races. The next chapter tells you how to log in to your wireless network.

Using USB

USB is a pretty nice technology. You can pull the adapter from one computer and move it to another if you want, or only have it plugged in when you need to use wireless (like any peripheral, a USB wireless adapter uses power even when you're not using it).

Keep in mind that if you move the adapter from one computer to another, you need to install the drivers on both computers, but only once. The configuration is stored on the computer, not the adapter, so you'll have to set up the wireless networks separately.

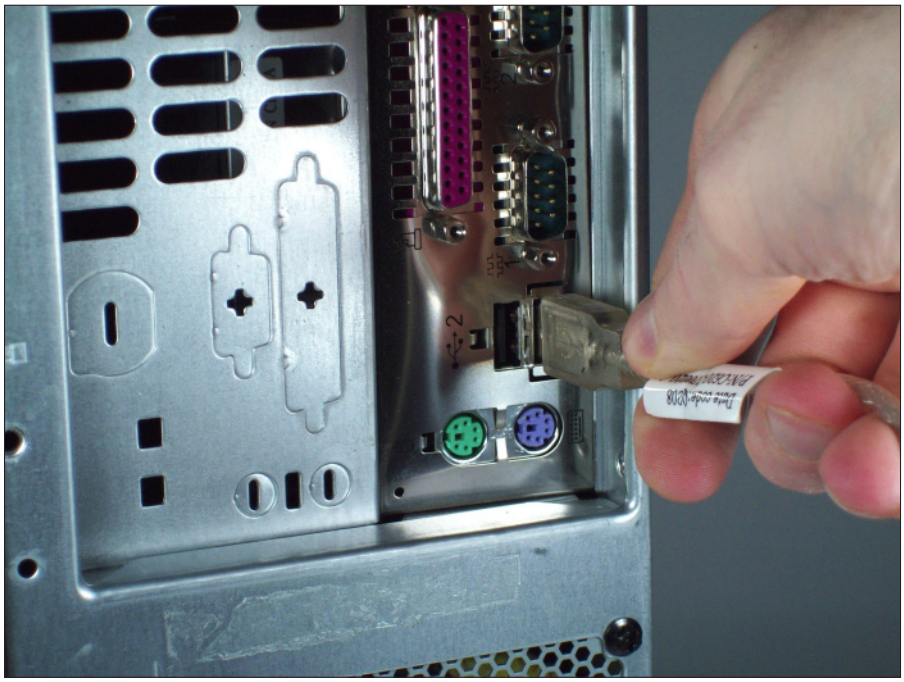


Figure 5-6: Plug in the USB cable.

Finally, be careful! Although the adapter is pretty resilient, after you plug it into the computer it's not too happy being pulled at or bent. If there's a downside to USB, it's that it sticks out of the side of your computer. People who worry about bashing their adapter might be wise to use the desktop adapter and stick it to their monitor; the worst that happens is the cable breaks.

People Can't Memorize Computer Industry Acronyms

Laptop users have another option called PCMCIA cards, PC Cards, or ExpressCards. PCMCIA stands for the Personal Computer Memory Card International Association, though I always remember it as "People can't memorize computer industry acronyms."

ExpressCards are the newer standard, and replace PC Cards. Depending on how old your computer is, you may have one of each or only ExpressCard slots. Either way, these cards slide inside the base of your laptop, leaving only an antenna sticking out.

PC Cards might also be a good choice for older laptops with the slower USB 1.1 ports, which run a lot slower than the PC Card interface.

The D-Link DWL-G630 card I'm using here follows a similar setup process to the other hardware we've looked at.

1. **Make sure your PC Card isn't plugged in. Just like the USB installation procedure, you install the drivers before the card.**
2. **Start the installation program by inserting the CD that came with the card into your CD drive.**
3. **Click Next.**

   A dialog box appears, as shown in Figure 5-7.

Figure 5-7: The D-Link installation starts with a warning.

4. **Insert the PC Card into one of the slots in the side of your computer, like in Figure 5-8.**

   Do this gently because you don't want to bend any pins inside your computer. If the card doesn't fit, check to see if you are trying to plug an older PCMCIA card into an ExpressCard slot (you will see a small piece of plastic inside the slot which is designed to prevent you from plugging the wrong type of card). A hardware detection dialog box opens, as shown in Figure 5-9.
5. **Select Cancel to return back to the manufacturer's installation process.**

   You may see a screen like the one shown in Figure 5-10 that indicates that the driver hasn't passed logo testing.
6. **You are using the manufacturer's driver, so you can safely select Continue Anyway.**
7. **Wait while your computer installs the software.**
8. **After the installation quits, click the Exit button to exit the process.**
9. **Reboot your computer with the wireless card still inside.**

Figure 5-8: A PC Card that's been inserted into a laptop.

Figure 5-9: The Windows hardware detection dialog box.

Figure 5-10: Ignore the warning about unverified software.

Cracking Open That Case!

PCI Cards are a reliable way of getting a desktop onto the wireless network. To add a new card to your machine's motherboard, you must open up your PC. After everything's closed up, the network card becomes a permanent part of your computer. The PCI Card has no risk of getting unhooked accidentally, lost, or having coffee spilled on it. Well, maybe you're not safe from the coffee, but I think you get my drift.

Going over some ground rules

You're going to be opening up your computer and working inside it. I'd suggest it's turned off while you do that. No, actually, I insist that your computer is turned off while you work inside it. Humans and electricity don't mix well.

Like a fuzzy cat, you're a natural collector of electric charge in the form of electrons. Collect enough electrons by shuffling your feet on carpet, rubbing a sweater against other items, or just picking a bad day to work, and you can turn those excess electrons into lightning bolts known as static electric shocks.

Those lightning bolts find their way to ground through the most efficient path possible, and all those electronics in your case provide such a path. The problem is that your computer is made to run on 12 volts, and those shocks that you're throwing around like Zeus run in the tens of thousands. Shock the wrong part and you'll be an unhappy computer owner.

Fortunately, protecting yourself while working inside your computer is quite easy. Follow these suggestions:

- Don't wear a heavy sweater, sweat pants, or dangly jewelry.
- Keep all parts in their protective bags until you need them.

- ✦ Keep a hand on the computer case at all times to ground yourself.
- ✦ Get your tools ready in advance so that you're not building up charge as you run around the house.
- ✦ Hold on to cards by the edges and don't touch the contacts or components.

Also, keep a small dish handy to hold any screws you might have to remove. That's got nothing to do with static electricity — those screws are small!

Installing the drivers

Just like the other devices we installed, you want to install the CD that came with the card before actually installing the card. It's remarkably similar to the USB and PC Card procedure; in fact, it's so similar that I'm just going to point you back to Step 2 in the previous section instead of reproducing it here.

Opening the case

Unplug everything from your computer's case and put it on your desk. The goal here is to separate the lid from the rest of the computer so that you can access the components inside.

Every computer is different, though. Rest the computer on its feet and have the buttons facing you. Look on the sides of the computer for buttons that you can push in to release the top. Push these in while rotating the lid upward, and it should open like a clam.

Failing that, look at the back of your computer for screws that hold the lid to the rest of the chassis. Some computers require that you turn a thumbscrew to release the lid, which slides back to reveal the parts inside.

Figure 5-11 is what my computer looks like. The button visible on the side releases the back of the cover, which swings upward to reveal the inside.

Accessing the PCI slots

Figure 5-12 shows the edge of the wireless card. This is a standard PCI card (Peripheral Component Interconnect) that you can use to expand your computer.

1. **Peer into you open computer case and look for some slots that would fit this card.**

   You should see between two and five in parallel against the back edge of your computer. Some computer designs have a riser board that comes out of the computer's motherboard at a 90 degree angle.

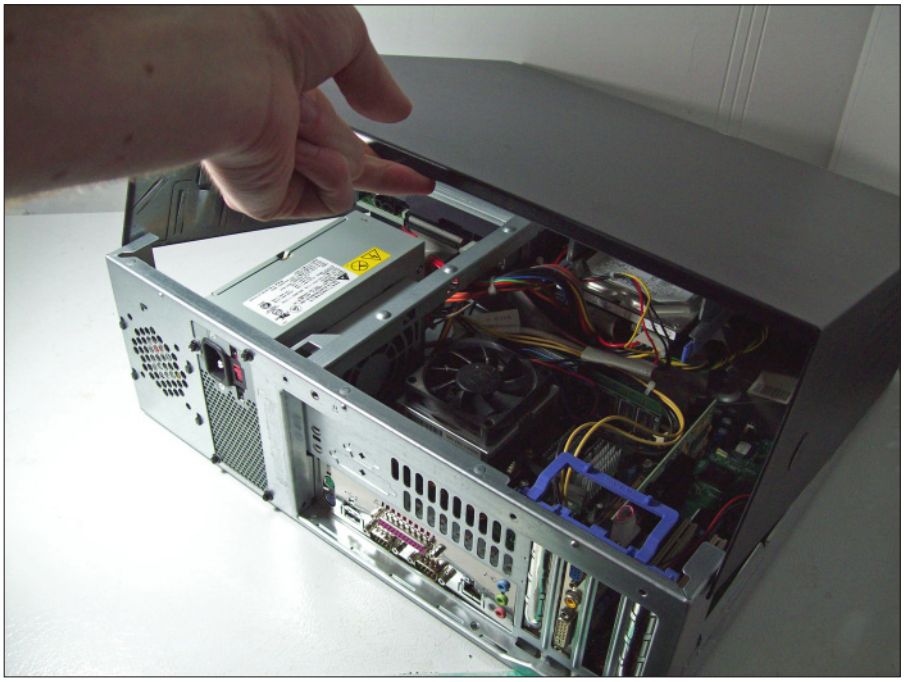


Figure 5-11: Open the case.

Figure 5-12: The edge connectors on a wireless card.

Figure 5-13 shows the PCI slots in my desktop. You may see slots that look similar but are offset somewhat. These are generally not PCI, and you want to avoid them.

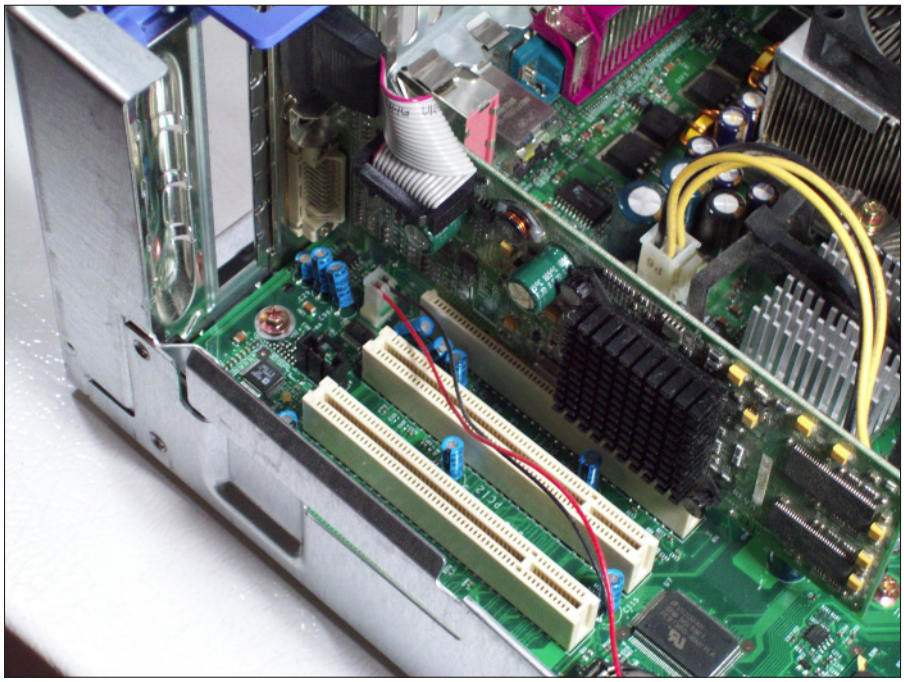


Figure 5-13: PCI slots in a standard desktop.

2. **Notice that the case of the computer has openings to the outside but are probably covered up at this point (you can see such an opening back in Figure 5-13).**

   When properly plugged in, one edge of the PCI card shows to the outside of the computer through one of these openings. Take a moment to figure out which PCI slot you're going to use and which opening on the case corresponds to that slot. The two don't line up perfectly, though, so you can use your card as a guide to figure out which port is to be used.

3. **Depending on your computer, you might have to undo a screw on the case to allow the card to go in.** You replace the screw later to hold the card down. You may also have to punch out part of the case to make room for the card — be careful! Other computers might use a clamp mechanism to hold down all the PCI cards at once.

4. **Gently line up the PCI card with the slot, and then make sure it's straight against the case so that the connectors on the card show through the outside.**

   Figure 5-14 shows the card all ready to go.

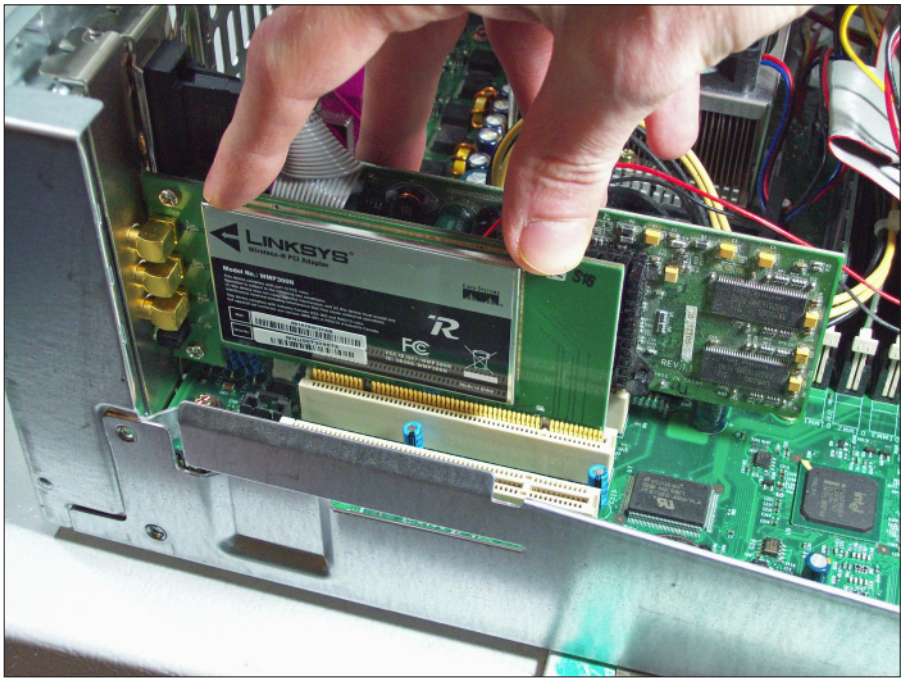


Figure 5-14: A PCI network adapter ready to be seated.

5. **Push down with your fingers on the edge of the card until the card is properly seated.**

   The card should be level in the case, that is, both sides of the connectors should be in the slots to the same depth. The edge of the card that shows outside the computer should also be seated snugly against the case, with the notched edge flush with the case and ready to be fastened.

6. **Screw the card down to the case or replace the clamp as appropriate.**

   Take a last look for forgotten tools and replace the top of the case.

Attaching the antenna

You will see some connectors protruding from your wireless card when looking at the back of your computer, as in Figure 5-15. Screw the connectors from the antenna onto those connectors. Make sure they fit snuggly, but hand-tighten only, please. Your card might indicate which cables go to which ports, so follow those directions. In the Linksys PCI card I'm using, the middle port is marked in blue, but it corresponds to a blue tag on the antenna cable. The other two ports can go in any order.

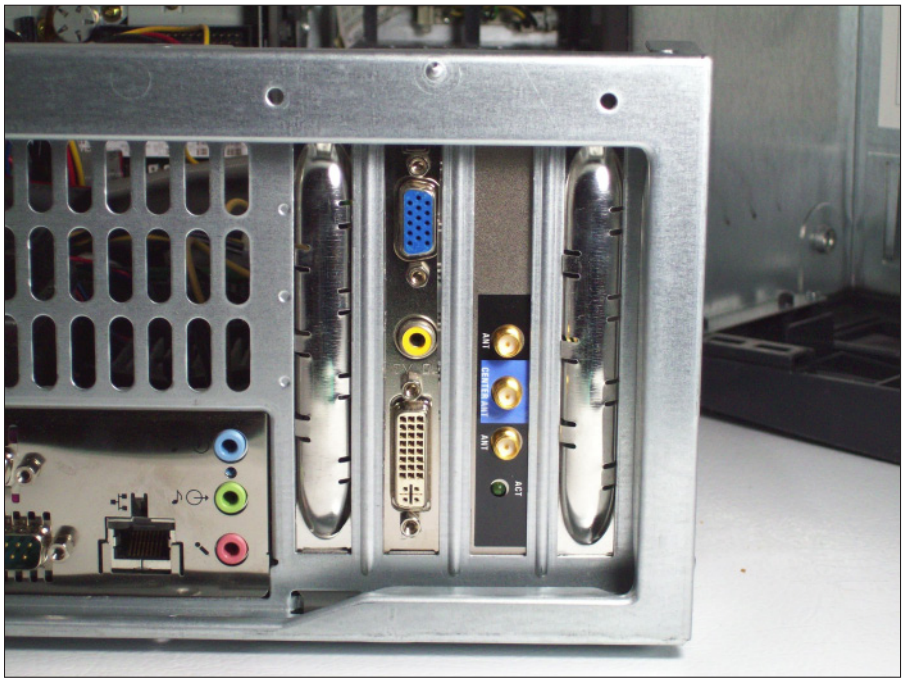


Figure 5-15: Antenna connectors on the wireless card.

Finally, put your computer back in its spot and hook up all the cables. Make sure the antenna cord is free of the other cords, and put the antenna somewhere where it will be unobstructed. That's it!

By now you've got your USB or PCMCIA network adapter plugged into your laptop and the drivers installed. If you're a desktop person, then you've conquered your computer's case and installed a PCI card, or you took the USB route.

Either way, you've got a functioning network card and a wireless network that's just begging to be used. The next chapter looks at getting your computer online.

Chapter 6: Getting Your PC On the Net

In This Chapter

- **Configuring Windows XP and Vista**
- **Using your wireless utilities**
- **Measuring your signal strength**
- **Using your laptop on the road**

This chapter covers how to get your computer on a wireless network. First, you take a look at how to configure a wireless network within Windows XP without the benefit of your wireless utilities. Sometimes those utilities just don't work as well as you'd like, and you have to resort to the old standard.

After looking at using the default wireless configuration, you see how life can be made easier by using the manufacturer's utilities. For those that are still running Windows 2000 or earlier, you need to use the manufacturer's utilities in any case.

Vista is the latest release from Microsoft, so after looking at Windows XP, you find out how wireless is configured in Vista. A lot has changed in Vista, so it's worthwhile looking at it separately.

Finally, you discover what else you can see in the wireless world. If you're ever on the road, this information can come in handy, because you'll have to find a different network to connect to.

Configuring Windows XP

Before you can configure wireless networking in Windows XP, you need to find out some information about the network you're currently connected to. You may think that I'm putting the cart before the horse, but knowing what a properly configured network looks like makes it easier to follow along when configuring your own network.

Microsoft developed the Wireless Zero Configuration system (WZC) short) for configuring wireless inside Windows XP. The name implies that there's no configuration for you to do; unfortunately, that's not necessarily true.

You put a password on your wireless network, so you know that at some point you'll have to type it in. But WZC for short tries to make most of the other choices on your behalf.

Figuring out if you are connected

The system tray, way down in the bottom right of your screen, contains a bunch of icons that give you both a status indicator of some aspect of your system as well a quick way to access options.

Figure 6-1 shows my system tray when I'm connected to the wireless network. The icon of the computer with the radio waves refers to wireless network adapter.

Figure 6-1: Hovering over the network icon shows the network status.

If a red X shows, you know that you aren't connected to your wireless network. But if an X does not appear, you know you must be connected to some network. Hovering the mouse over the icon brings up the network status. From there, you can find out some information, such as

- This computer is connected to the *myhome* network.
- The connection speed is 54 Mbps (Wireless G or A).
- The signal strength is excellent, which is the best you can get.
- The computer is connected to the network (but you already knew that!).

The example in this section shows a signal strength of excellent. Other options are very good, good, low, and very low. As you can imagine, those are fairly subjective. I look at some better ways to measure the strength but in the meantime shoot for excellent through good.

Checking status

That information from the hover was nice, but you can find more help by clicking your mouse a few more times.

Right-click on the wireless adapter icon in the system tray and select Status. Something like Figure 6-2 appears.

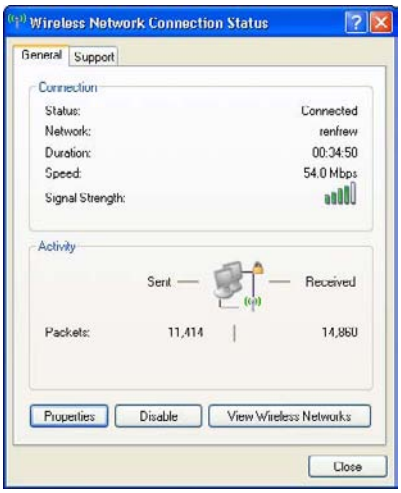


Figure 6-2: The Status page for a wireless network adapter.

At the very top you see two tabs, General and Support. The General tab gives a lot more information than you had before. You can see the status, name, and connection speed of the network. The duration tells you how long you've been connected, and instead of the nondescript signal strength, you get a display from 0 to 5 bars (which really maps to the same scale as before, but looks a lot nicer!).

In the section marked Activity, you can get an idea of how much data you've sent and received. The actual numbers aren't important, other than for curiosity's sake, but sometimes you want to make sure that you're able to transmit and receive. If your computer is supposed to be working, but the received packets counter isn't increasing, you are having a problem receiving data.

The final point of interest on this tab is the three buttons along the bottom (right above the Close button, which closes the window, and is not at all interesting). You've got three options here that you can use later:

- **Properties:** This button takes you to the adapter's property configuration window, which has everything from IP addressing to firewalls.
- **Disable:** Pressing this button disables your adapter and then changes to an Enable button. Pressing the button again re-enables the adapter.

- **View Wireless Networks:** You use this later to show all the wireless networks that your computer can see. You can then pick the one that you want to connect to.

The Support tab, shown in Figure 6-3 has more information about your connection.

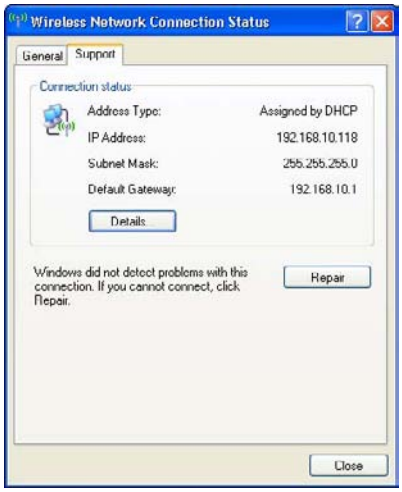


Figure 6-3: The Support tab within the Wireless Network Connection Status page.

The Support tab shows you your IP address, mask, and gateway. Recall from Chapter 4 that if you see an IP address starting with 169.254 that something is wrong with your computer or network, because those addresses are only used when DHCP fails to work.

You can click on the Details button to get even more details, but usually knowing your IP address is enough.

The most important button on this page is the Repair button. If you click this button, Windows disables your adapter, re-enables it, and then goes through the connection sequence again. Often, if everything else looks right but things still aren't working, using the Repair button fixes the problem.

Configuring wireless, the zero configuration way

Ideally, Windows will take care of all the technical details behind wireless configuration. All you need to know is the name of the network and the password.

With that in mind, open up a list of the available wireless networks. You get there either by right-clicking on the adapter icon in the system tray and selecting View Available Wireless Networks or by double-clicking on the same icon and pressing the button marked View Wireless Networks. Either way you go, you see a dialog box as in the one shown in Figure 6-4.

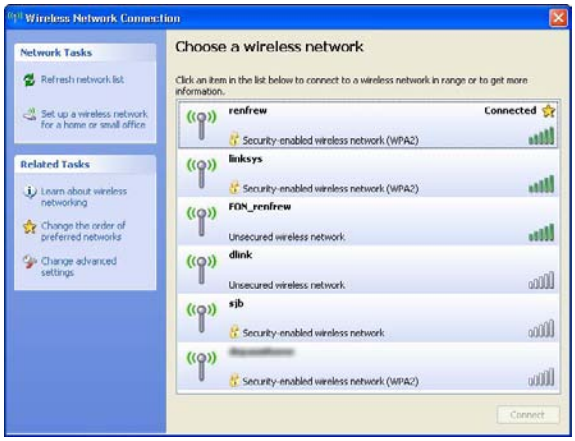


Figure 6-4: The list of available networks.

When you pull up the list of available networks, your computer stops transmitting and receiving on the wireless network and starts listening for any networks that might be in range. This list is then displayed to you.

Several pieces of information in Figure 6-4 help to find the right network to connect to. First, the SSID (Service Set Identifier) is displayed in bold. The SSID is the technical term for the name of the network. Here I can see *renfrew*, which is the name of the network I configured earlier on. Off to the right is the now-familiar signal strength icon. Along the bottom of each row is a description of the type of security the network uses. Anything with a padlock requires a password to join. The text to the right of the padlock describes the exact protection being used, which Windows takes care of on your behalf.

Finally, the gold star on the rightmost side of some rows indicates that this is a so-called preferred network. A *preferred network* is one that Windows will automatically try and connect to. In addition to the star is a behavior, such as Connected for the network you're currently connected to, and Automatic for networks that Windows has been told to automatically connect to.

If you think that a network should be on the list, but it isn't, click the Refresh network list under Network Tasks.

Joining the network

Join the network you want by double-clicking on the row for that network. If the network is secured then you are prompted for a password.

In the dialog box shown in Figure 6-5, you must enter the same password you entered when you configured WPA protection on your router. Type the password twice and click the Connect button. After you've connected to the network, you are returned to the list of available networks.

Figure 6-5: Entering the network key.

You're connected now — congratulations! You can confirm this by noting that the word Connected appears next to your network in the list of wireless networks or by hovering your mouse over the network icon in the system tray.

Configuring wireless, the longer way

Sometimes the network you're connecting to doesn't advertise its existence, even though it's still there. This is often the case at businesses, where at one point in time, hiding your wireless network was considered a security bonus.

Hiding your network doesn't solve any security problems; all it does is make it slightly harder to connect.

If you're playing around as you go, you might find a faster way of getting to certain menus than the way I'm showing you — which is great! I'm showing you the foolproof one.

Follow these steps to connect to a network when you know its configuration but don't see it in your list of available wireless networks:

1. **Right-click on the wireless adapter icon in your system tray and select View Available Wireless Networks.**
2. **Select Change Advanced Settings.**

   The Wireless Network Connection Properties dialog opens.

3. **Select the Wireless Networks tab shown in Figure 6-6.**

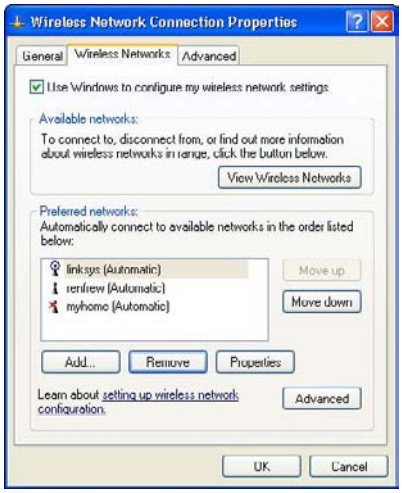


Figure 6-6: The Wireless Network Properties window

This dialog is used to manage all the preferred networks.

4. **Create a new profile by clicking Add, which is found at the bottom of the window.**

   The window shown in Figure 6-7 pops up has three tabs: Association, Authentication, and Connection. Most of the work is in the first tab; in fact, we're just going to glance at the last two.

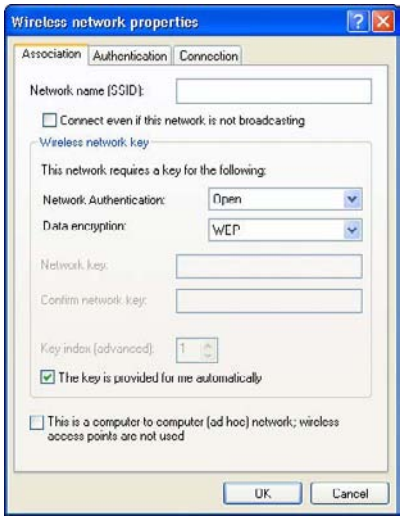


Figure 6-7: The new network's properties window.

5. **In the Association tab, type the SSID of the network you're trying to connect to, which is the same as the name of the network.**

   This value is case sensitive, so "myhome" is different than "MYHOME" and "MyHome."

6. **Make sure the Connect Even If This Network Is Not Broadcasting checkbox is selected.**

   This option is important for networks that are hidden. Checking this option tells Windows to actively look for the network rather than waiting to hear the network announce itself.

   The Wireless network key section is the trickiest part. If you set up your network following the instructions earlier on, you will be using WPA2-PSK authentication and AES data encryption. Make sure to choose WPA2-PSK and not WPA2! The PSK means Pre-Shared Key, which refers to the password you set up on your router. The non PSK version is used in enterprise networks where you are authenticating against a directory server.

7. **Type the network password in the section that asks for the network key. Confirm this value in the next line.**

   If you are unsure of this information, plug back into your router and make sure. It'll save a lot of frustration later.

8. **Make sure that the This Is a Computer-to-Computer Network checkbox is not selected.**

   Figure 6-8 shows a dialog that's been filled out. In the Authentication tab, everything should be grayed out if you are using WPA2-PSK or WPA-PSK.

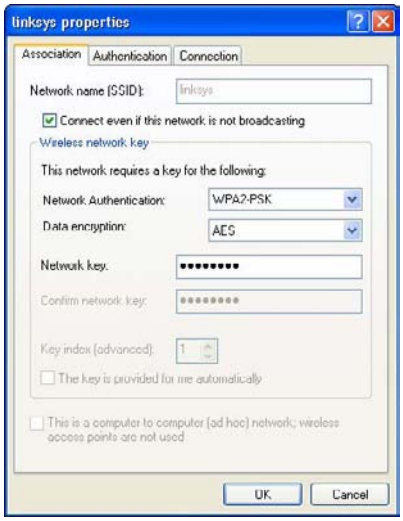


Figure 6-8: A network that's been configured.

9. **In the Connection tab, make sure that the Connect When This Network Is In Range checkbox is selected.**

If you don't have a WPA2-PSK option, then your computer's software might be out of date. Upgrade Windows XP to at least Service Pack 2, which includes WPA2 support. Alternatively, search http://microsoft.com for KB893357, which is the patch that provides WPA2.

10. **Click the OK button to exit the configuration and then click OK again to exit the properties window.**

If you have configured the network correctly, and the network is within range, Windows connects.

Managing your preferred networks

A computer can only be connected to one wireless network at a time. Sometimes, you run into a situation where your computer can see two networks that it knows how to log into, and the computer must decide which network to log into. You control this decision by ordering your preferred networks. Windows chooses the network that's highest on the list.

If you ever connect to a default network like NETGEAR, D-link, or Linksys, make sure that you move it down to the bottom of your list of preferred networks. Your computer doesn't know the difference between the network you connected to at the coffee shop and your neighbor's insecure wireless network, because all it has to go on is the name. With the defaults at the bottom, you avoid the embarrassing situation where you connect to your neighbor's network when you should be connecting to your own.

Go back to the Wireless Network Connection Properties dialog by right-clicking on the wireless adapter in the system tray, selecting View Available Wireless Networks, and then Change Advanced Settings. Figure 6-6 shows this dialog. Look at the Preferred Networks section. You can select any network and move it up or down using the appropriate buttons on the right. If you want to view the connection's settings, highlight the name of the network and click on the Properties button.

You may adjust the priority of any network you have used, no matter if you configured it manually or let Windows set it up for you.

Using Wireless Utilities

The Windows Zero Configuration method isn't too difficult, but you need to do a lot of clicking to find what you want. Wireless support in Windows XP was almost an afterthought, so it's no surprise that there are some annoyances.

Modern network adapters come with a utility for managing the network connections which takes over from Windows Zero Configuration. You must choose to use one or the other — both cannot be active at once. The wireless utility from the manufacturer has its own configuration database, meaning that if you switch back to WZC at some point, you lose all your settings.

Still, I prefer to use the manufacturer's utility because it usually has a nicer interface and often provides more troubleshooting tools than does Windows.

If you are running an earlier version of Windows, such as Windows 2000 or Windows95, then you're pretty much stuck with using the manufacturer's utility.

Finding a network

Just like the WZC procedure, you connect to a network by picking it from the list of available networks.

I'm using a NETGEAR USB adapter and the associated utility called the NETGEAR Smart Wizard. If you're using a different adapter, your screens are going to be different. Most of the utilities are similar, so just click around until you find what I'm talking about.

To find a network, follow these steps:

1. **Open the utility by finding it from your Start menu, or by double-clicking the icon in the system tray.**

   I'm not talking about the Windows network adapter icon, but the new icon that was created when the software was installed.

2. **Select the Networks tab to see the list of available networks.**

   The NETGEAR utility is the only one I've used in which I had to click on a tab to get to the list of networks; all the other ones started off at that screen. The screen is shown in Figure 6-9.

   You get a list of all the available networks, along with an indication of what wireless standard is used, the security mode, and the strength as measured by a percentage. The column marked N indicates 802.11n capable networks.

3. **Double-click on your SSID (*linksys* in this case), which brings up the dialog box you see in Figure 6-10.**

   Wi-Fi Protected Set up (WPS) is a simplified method of connecting to wireless networks. Rather than typing in passwords and any other security settings, a different approach is used. A WPS capable router has a PIN number printed on it, a WPS button, or both. If you supply the PIN

during the connection, then your computer can negotiate the shared secret directly with the router. Alternatively, you can press the WPS button on the router, which puts it in a mode ready to pair up with your computer.

Figure 6-9: The list of available networks as seen by the Smart Wizard.

Figure 6-10: The Wi-Fi Protected Setup dialog box.

4. **Select Yes in response to the dialog box shown in Figure 6-11, which then prompts again to see if the router has a push button.**

5. **The router does indeed have a push button, so click Yes.**

   The next screen, shown in Figure 6-12, asks you to press that button.

Figure 6-11: Do you have a WPS button?

Figure 6-12: Press your WPS button!

6. **Press the WPS button on the router and then come back to the dialog box and click on the icon where indicated.**

   Your computer thinks for a moment and then connects you to the wireless network.

The WPS method is very easy because you don't have to remember any settings. All you need to do is press a button or read a PIN off a sticker.

Configuring Vista

Microsoft's Vista operating system came several years after Windows XP, and Microsoft decided that they should build wireless support in from the ground up. As such, wireless configuration is much smoother in Vista than it is in XP.

Rather than choosing between using Windows for configuration or the manufacturer's utilities, Vista integrates the two. You are free to use either approach because the two integrate with each other. Because of this integration, Microsoft has changed the technology's name from Wireless Zero Configuration to Native Wi-Fi.

Listing available networks

Start off by displaying the list of available networks. To do so, follow these steps:

1. **Click Start and then click Connect To.**

   You get a familiar-looking window showing the list of available networks, as shown in Figure 6-13.

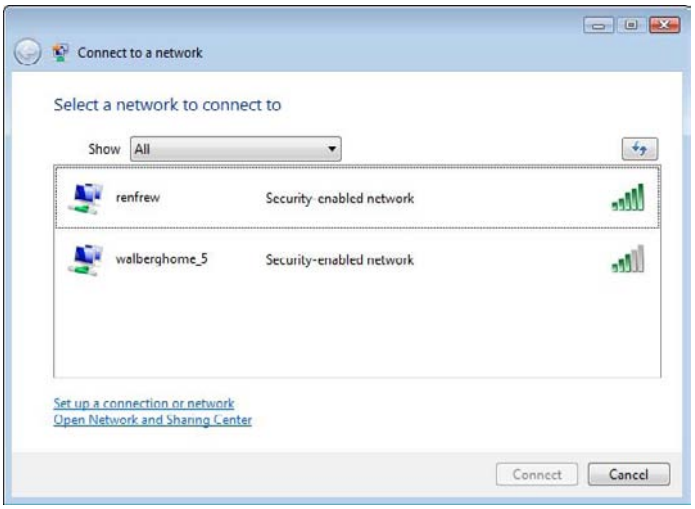


Figure 6-13: Vista's list of wireless networks.

   Just like the Windows XP version, you can see the name of the network, a signal strength, and a list of the security measures used on the network.

2. **Double-click on the network you want, and if it's a secure network, you'll be prompted for the password just as in Figure 6-14.**

   Note that this time around, you only have to type in the password once. If you select the Display characters button, then everything you type will be echoed to the screen instead of just displaying stars.

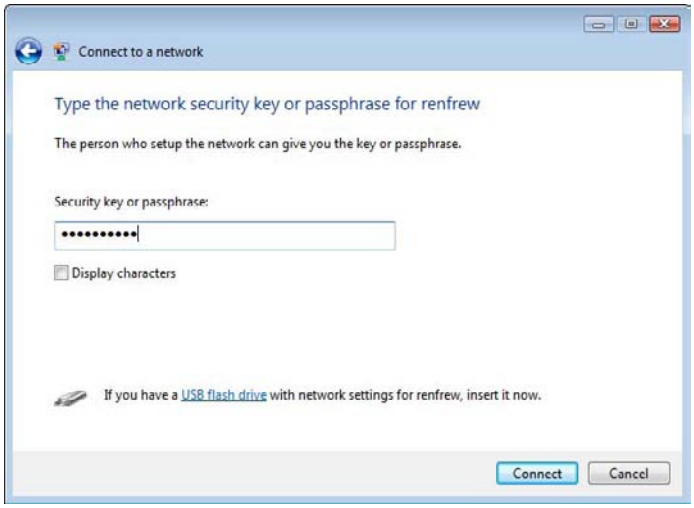


Figure 6-14: Vista's prompt for a network password

3. **Click OK to save the connection and have it start automatically.**

   Vista introduces more security features, one of which requires you to assign a context to a network connection. After you have connected to a network, you are prompted to assign a location, which you can see in Figure 6-15.

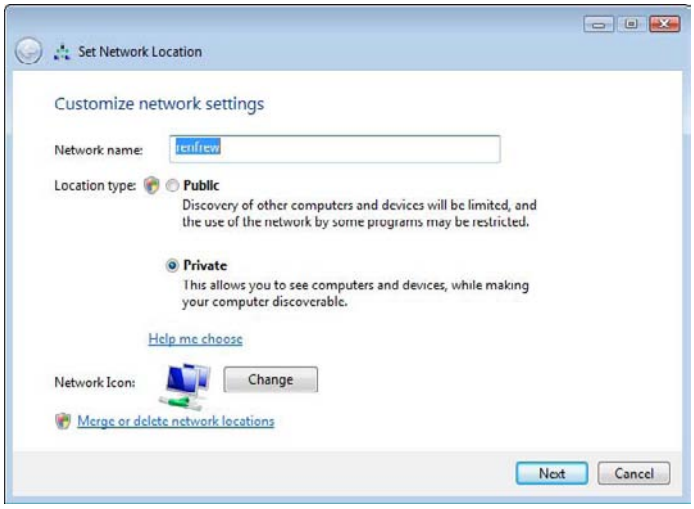


Figure 6-15: Assign a location to a network.

You have three options:

- **Home**: You are using this on a private network, such as at home. Your computer can be discovered on the network, and firewall restrictions are somewhat relaxed.
- **Work**: You are using this connection at work, where your computer is managed by an IT department. This location is virtually identical to the Home location, except that the firewall is further tuned to allow management connections in.
- **Public location:** You are using your computer in an untrusted network that's outside your control. The computer will be hidden, and the firewall is very restrictive. The shields are up, and phasers are set to kill!

4. **Select the Home option.**

Confirming and changing settings

Figure 6-16 shows the Vista system tray. Look at the picture of the two computers with the globe. The icon indicates you are connected to a network (otherwise there would be a red X on top), and the globe indicates that you have a path to the Internet through this connection.

Figure 6-16: The Vista system tray.

Hovering over this icon gives even more details. From the box that appears, you can see that this computer is connected to the *renfrew* network and has access to both the local network and the Internet. The house to the left tells you that the security location is Home. Finally, the signal strength is four bars out of five, otherwise known as Very Good.

To the Control Panel!

Launch the Control Panel by choosing Start➪Control Panel. Then choose Network and Internet➪Network and Sharing Center. (If you haven't noticed by now, everything in Vista seems much cleaner than before, just harder to find!)

The Network and Sharing Center is shown in Figure 6-17. Along the top you can see the same information you learned from the icon in the system tray. The bottom half shows you all the security settings. In Figure 6-17, you can see that this machine is configured for very limited sharing. You may click on each row to change the setting.

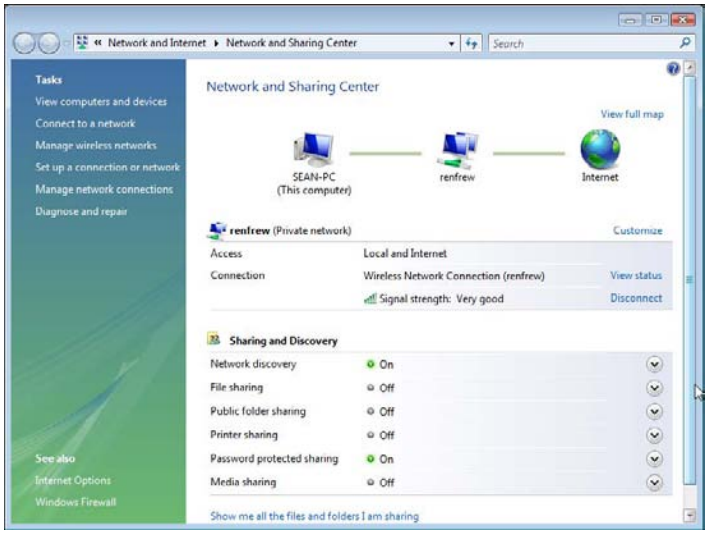


Figure 6-17: The Network and Sharing Center.

To the left are several tasks, the most important of which is the Manage Wireless Networks task. Clicking this takes you to a menu that does much the same as the Wireless Network Properties from Windows XP. Figure 6-18 shows this menu.

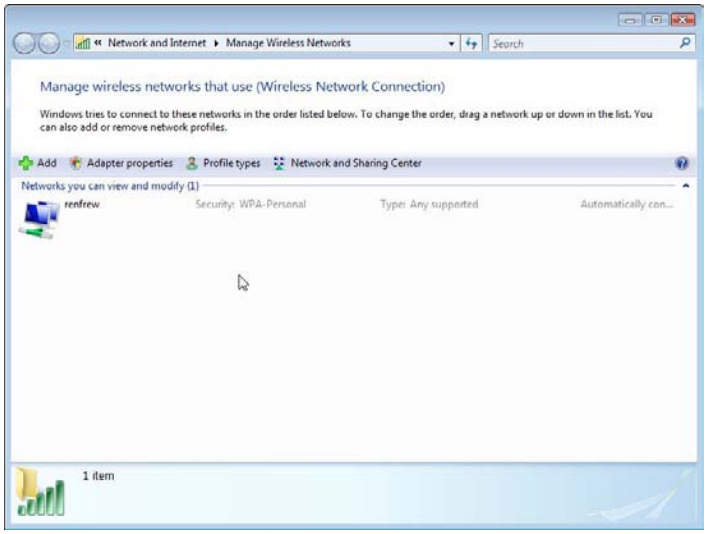


Figure 6-18: Managing Wireless Networks in Vista.

The Manage Wireless Networks menu shows a list of all the currently configured networks; in the example above, there is only one. If you need to reorder the networks, so that one is tried before another, then click and drag

the network to the place in the list you want (Windows XP had Up and Down buttons to achieve the same thing). The Add button adds a network in much the same way that Windows XP does it.

But what's my address?

Our final stop in the Vista configuration is to find your network information, which is helpful to know if you ever call your service provider for help. From the Network Sharing Center, choose the Manage Network Connections option. Double-click the wireless adapter, and you see Figure 6-19.

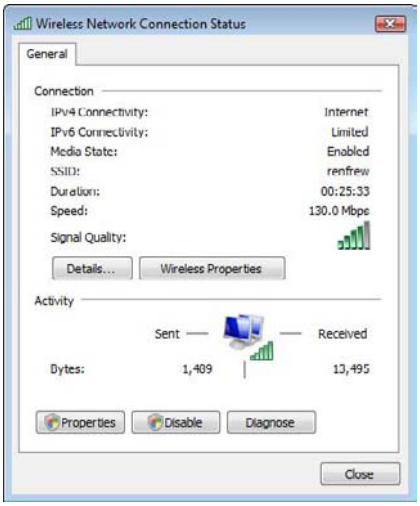


Figure 6-19: Viewing the adapter status.

This dialog box is almost exactly like the Windows XP counterpart. You can see that this adapter has access to the Internet through IPv4 but has limited IPv6 connectivity (this is nothing to worry about, as most of the Internet uses the IPv4 connections, and Vista's trying to get ahead of the curve by setting IP version 6),

Again, just like Windows XP, you can see the connection timer, speed, strength, and packet counters.

The Details button shows the exact IP addresses involved.

Pushing Boundaries

At some point, you're going to venture out of your house and connect to another network, such as one in a hotel, airport, coffee shop, or another building.

Your computer is perfectly capable of keeping track of multiple configurations, so connecting to a new network won't cause any problems when you return home.

Most public networks are wide open and have no security. They employ a *captive portal*, which lets you connect to the network but immediately redirects you to a login screen where you must log in, pay, or otherwise identify yourself before getting on the Internet. Remember that your wireless session is available for anyone else to capture, so be careful about typing in credit card numbers and passwords unless the Web site is protected with *Secure Sockets Layer* or *Transport Layer Security* (you see a lock in your browser window if this is the case, and the address bar might even change, depending on which browser you use). Book IV, Chapter 1 discusses browser security in more depth.

Also, pay attention to which network you are connecting to. If you are at a hotel, you may want to check with the front desk to find the SSID of the network you should connect to. There may be other open networks you can connect to, but you'd be using someone else's network, and you can't be sure what they're doing to your traffic.

Chapter 7: Setting Up Other Hardware

In This Chapter

- **Printing wirelessly**
- **Using wireless file storage**
- **Adding an access point**

One drawback of being wire-free is that carrying your printer everywhere you go is a little tricky! Rather than plugging into the printer every time you need to print, let's get your printer on the network, too! Many printers come with network adapters, so there's no reason you shouldn't be able to print from wherever you happen to be.

Having your computers on the same network also means they can share files. In this chapter, you discover a way to have a permanent file server on your network.

Finally, if your wireless network doesn't reach somewhere, I look at adding another access point to your network to expand that reach.

Printing Wirelessly

Several years ago, the traditional way to get a printer on the network was to shell out big bucks for a printer that supported it, or to buy an adapter that had a parallel cable on one end and a network cable on the other. These devices cost between $50 and $100. I'm not sure about prices in your area, but that's as much as an entry-level printer.

Over the past few years, printers have both dropped in price and become more feature rich. One of the features you can expect to see on some new printers is a wireless network card. This means that the printer can be placed anywhere there's a power outlet. The extra cost to get a model with the wireless card is minimal, and it's only going to get lower.

For example, the device I'm demonstrating here is a color inkjet printer that also copies, scans, and faxes. It's got an 802.11g wireless adapter that can be found online for $150.

Just like the network adapter you installed earlier, you'll need some drivers for your printer. This time, the drivers tell your computer how to communicate with the printer over the network and how to operate the extra features such as scanning and faxing.

As usual, if you've got a different printer than the one I'm using, your screens will be different. However, the steps are similar.

Before you get started, have a look at the documentation that comes with your printer. The printer I'm using comes with a note that says if you intend to use the printer on a network that you should ignore the quick start guide and refer to the network installation guide.

Plug your printer in and install the ink cartridges per the directions in the manual.

To set the wireless configuration on the printer, you first have to get it set up on the wired network. To do so, follow these steps:

1. **Plug the Ethernet cable that came with the printer into the back of the printer and the other end into your wireless router.**

   Figure 7-1 shows the network port on the back of the printer.

Figure 7-1: The wired port on the printer.

Your printer picks up its initial address from DHCP.

If your printer is nowhere near your router, bring your router to the printer rather than the other way around. The only thing you lose is Internet access, which isn't needed for the installation anyway.

2. **Put the CD that came with the printer into your CD drive, and you see the initial screen, shown in Figure 7-2.**

Figure 7-2: The initial printer installation screen.

3. **Click the Install button to begin the installation.**

   After accepting the license and going through the introductory screens, you are prompted to indicate if this is a network installation or not.

   You see a couple more screens of information, after which you are asked how you're connected to the printer (shown in Figure 7-3). Method one is the simplest, as you are already set up that way (despite the picture in Figure 7-4 showing the computer plugged into the network, it works just as well over wireless).

4. **Select Next and the software attempts to discover the printer.**

   If your computer has the Windows firewall enabled, then a dialog box appears so that you can make a firewall exception. Figure 7-5 shows the dialog box, to which you should select Unblock.

5. **After a moment, your printer will be discovered, and you can continue clicking Next until you are asked how you want to print, as shown in Figure 7-6.**

Figure 7-3: Is this a network installation?

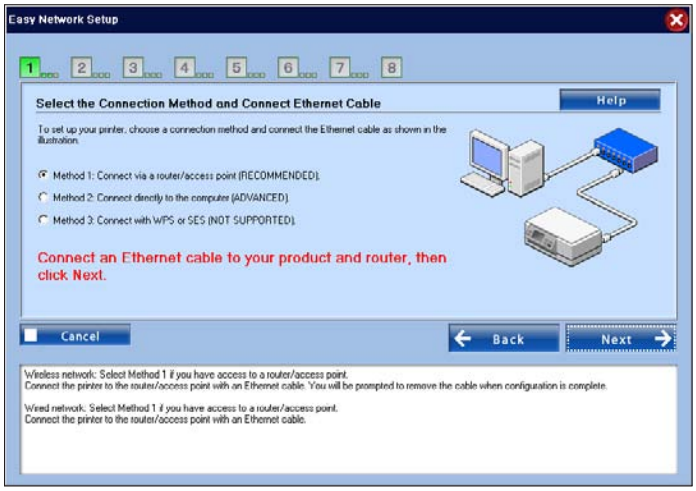


Figure 7-4: How are you connected to the printer?

6. **Even though the printer is plugged in now, you eventually want to get it on the wireless network, so select Wireless.**

   The software will scan for available wireless networks and then present a list of SSIDs that you can connect to, which is shown in Figure 7-7. This is almost identical to how you chose which network to connect your computer to.

7. **Click on your network name to select it and then click the Next button.**

   If your network uses WEP, WPA, or WPA2, you must enter a password.

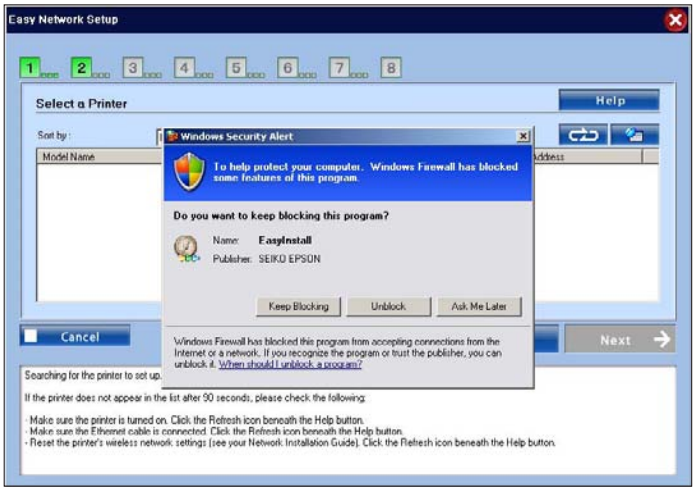


Figure 7-5: Unblocking the application from the firewall.

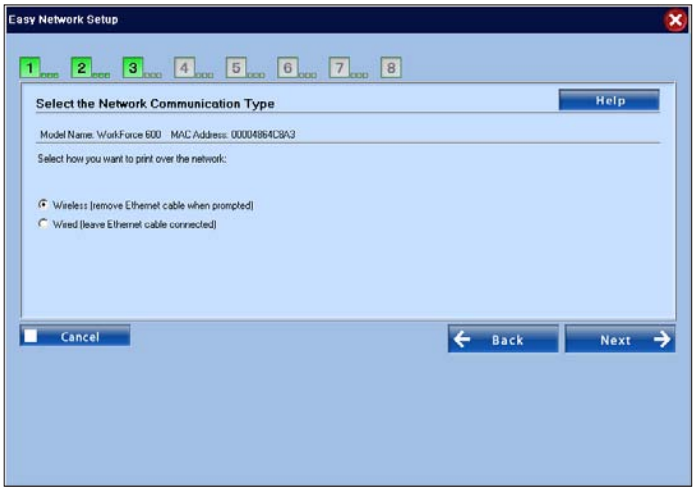


Figure 7-6: How will you be printing?

8. **Type your password, confirm the settings, and then the printer will be configured by the software.**

9. **After the software has confirmed that the printer is configured, you can unplug the wired connection and print a test page when prompted.**

   Your default printer is set to the wireless printer.

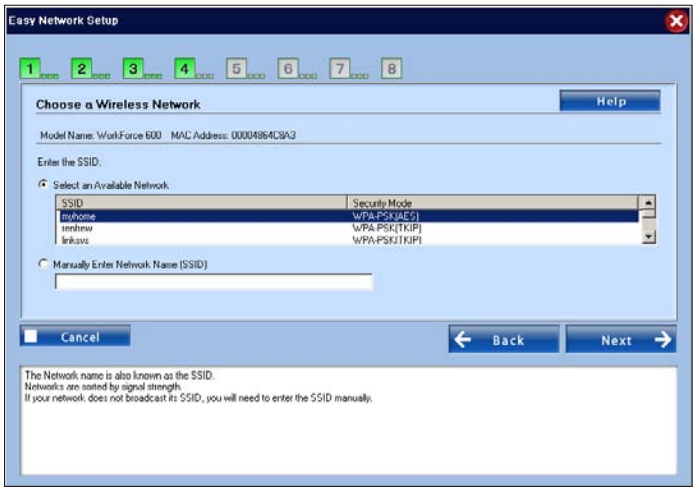


Figure 7-7: The list of wireless networks

If you noticed the WPS option during the setup, then good for you! For some reason, the current documentation specifically tells you not to use WPS, but after you've done the initial installation it works fine. This way would be handy, for instance, should you move the printer to a different network. From the control panel on the front of the printer, select Setup ➪Network Settings➪Wireless LAN setup. From there, you can change the network settings, including performing a WPS setup. You still need the driver on your computer to print, though.

Sharing Files Wirelessly

Sharing files between computers over a network, wired or wireless, is nothing new. However, you do find a few disadvantages:

- **The computer with the files on it has to be turned on.** The current trend is to save energy by turning off computers when they're not in use — which is good.
- **The computer with the files on it has to be connected to the network.** If the file you need is on a laptop that's not at home, you've got a problem.
- **It's more difficult and less secure to share files with the Internet.** If you want to grab some of your home files when you're at work, for example, the usual solution is to expose one of your home computers to the Internet.

Add to this that external USB storage is becoming larger and cheaper. For much less than $200, you can get a 1TB disk that can be used on any computer in your house, without having to take anything apart. Unfortunately, after you plug one of those bad boys into your laptop, you have no more mobility!

With the latest crop of home you simply plug the external hard drive into the router, configure file sharing, and presto! You have a permanent file server that you can store your stuff on. In Figure 7-8, I show a picture of the back of a Linksys WRT610N which has such a feature.

Figure 7-8: A USB port on a router for an external storage device.

A router draws far less power than a computer, is always available, and its position in the network is ideal for performance. The router is also able to share files to both the internal network and the Internet at large because it sits on both of those networks.

Setting up file storage

Start by plugging your USB storage device into the USB port on your router and then log in to your router's administrative interface. On the Linksys WRT610N you access the storage configuration from the Storage menu, which is shown in Figure 7-9.

The menu shows you details about the disk that's currently plugged in. Above, you can see I have a 2GB flash disk drive plugged in. This is a good sign because it means the router has recognized the drive. If you don't see any drives, double-check that the USB cable is plugged in all the way and that the hard drive has power.

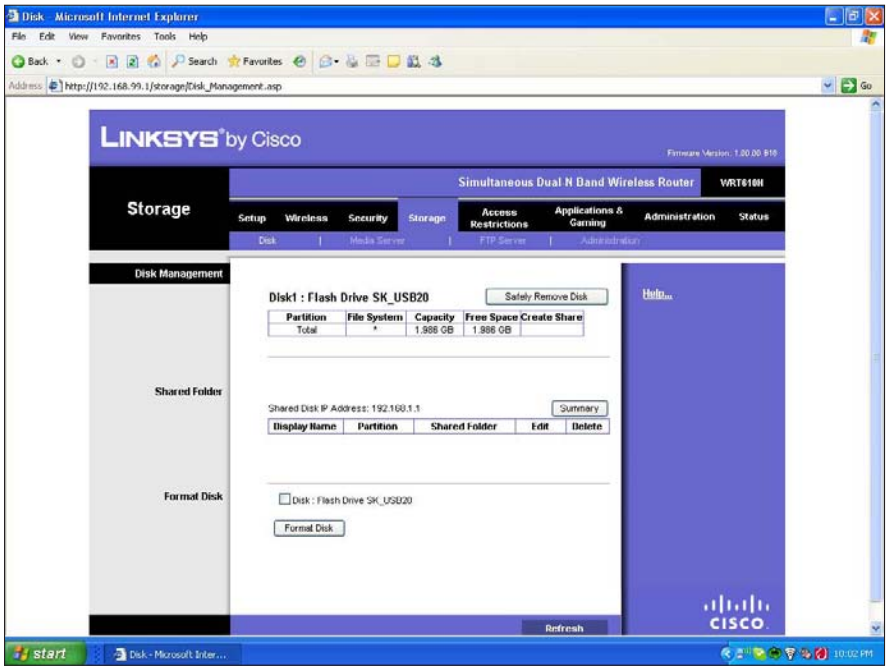


Figure 7-9: The storage menu.

The disk details, shown in Figure 7-9 also include a column called Create Share. Depending on how your disk is set up, you may or may not see a button in that column that also says Create Share. If you do see the button, then you can skip the next section. If your view is like that shown in Figure 7-9, you need to format the disk.

Formatting the disk

Disks must be formatted and partitioned before they can be used. This process lays out certain structures on the disk that the computer uses to remember where files are placed and which parts of the disk are free.

You can format a disk many different ways; however, not all formats are supported by the router. It's easy to determine if you have to format your disk again — if you have the option to create a share, then you don't have to format the disk. Additionally, you can see some partitions listed in the top table.

Formatting a disk deletes everything on that disk. Gone! Kaput! Copy your stuff off the disk to another computer before you format; otherwise, it's gone!

Follow these steps to format a disk:

1. **After you back up your data, look down to the Format Disk section of the Web interface. Check the button next to the name of the disk and push the Format Disk button.**

   You receive a warning indicating that everything on the disk will be deleted, as shown in Figure 7-10.

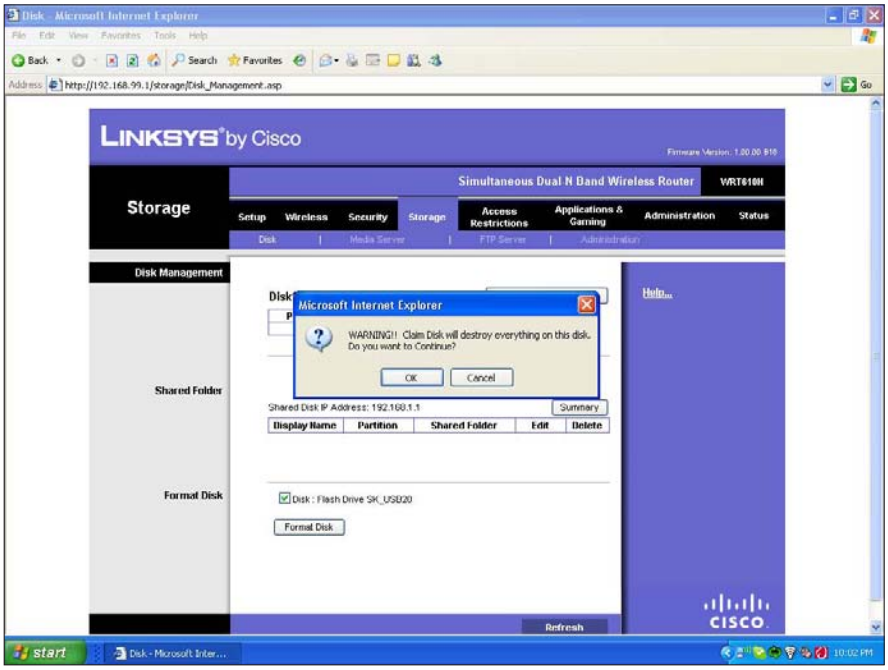


Figure 7-10: A warning before formatting a disk.

2. **If you are sure you're ready to format the disk, click the OK button.**

   After you've done that, you are asked to supply the name of a partition (see Figure 7-11).

   A partition is a way to split out a disk into multiple logical disks. This formatting process assigns one partition to the disk, using all available space, so the name of the partition isn't that important.

3. **Type the name of a partition and click the Format button.**

   You are asked again to confirm that you're okay with any data on the disk being wiped clean, after which the router can chug away while it formats the disk. This may take a few minutes, depending on the size of your disk.

After the formatting is complete, you are returned to the main storage menu (see Figure 7-12) showing the partition that was just created. Note that the Create Share button shows up along with the partition.

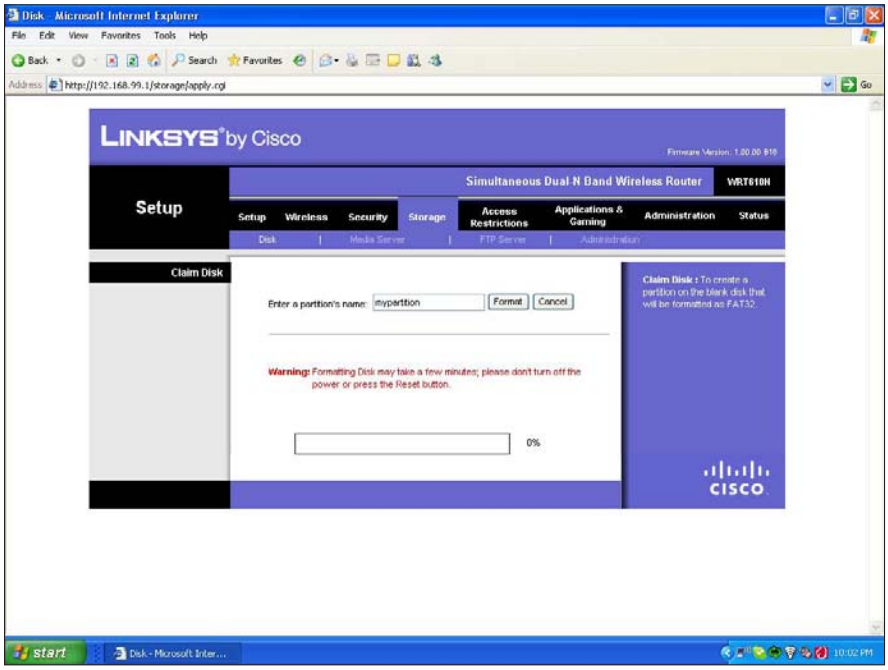


Figure 7-11: Supplying the name of a partition.

Figure 7-12 also shows that a shared folder called *public* has been created. Before you can use this share, though, you must take care of some of the default security settings.

Dealing with security

After you format the disk, the router creates a directory called public and shares it out with the name of Default. When you connect to a network share you must provide a username and password to connect with, which prevents the wrong people from getting at your data.

The router has created two users by default and given them access to the share. One user, *guest*, can only read the data, while the *admin* user can read and write. This is okay, but you want to set the passwords to something you know and control. To do so, follow these steps:

1. **Select the Administration submenu (the one to the right of FTP server, not the one to the left of Status) to see a list of the users and groups as shown in Figure 7-13.**

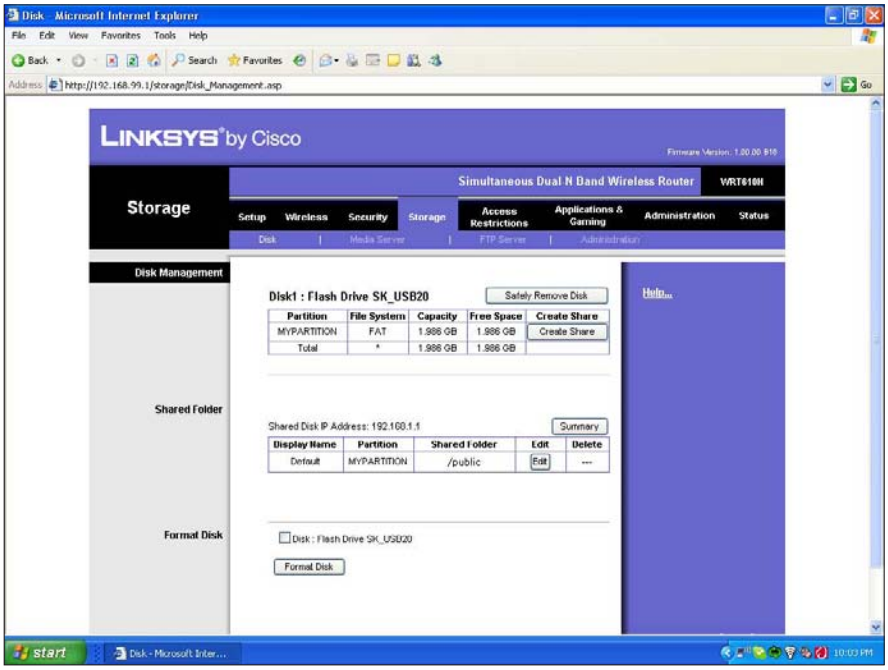


Figure 7-12: The storage menu showing the disk has been properly partitioned.

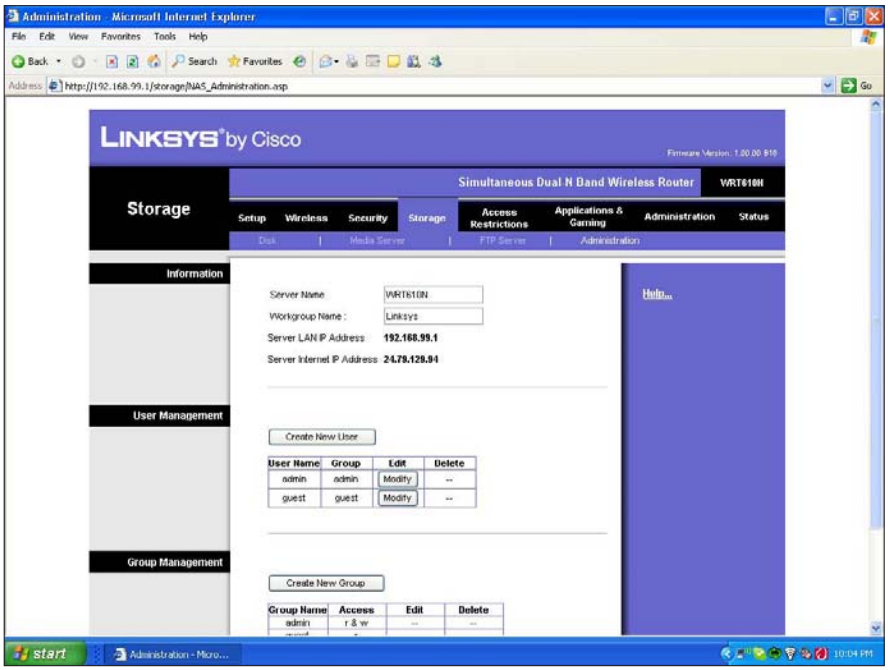


Figure 7-13: Showing the users and groups.

2. **Click on the Modify button next to the Admin user, and a new window, like the one in Figure 7-14, appears.**

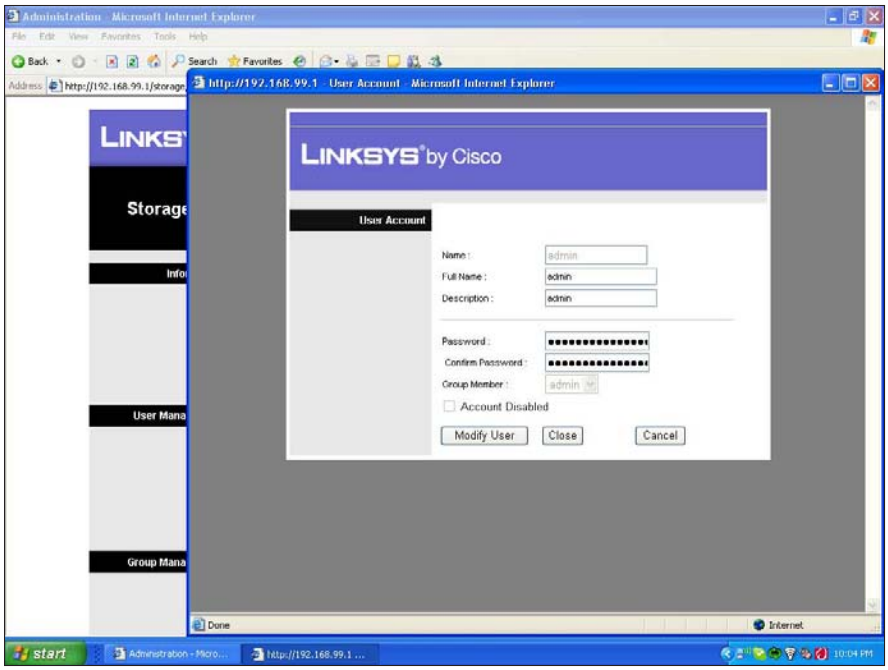


Figure 7-14: Modifying the admin user.

3. **Type a new password in the Password field and then confirm it in the field below.**

4. **Finally, click Modify User to save the change. Repeat this process for the Guest user.**

Connecting to the file share

While you're in the administration menu, make a note of the *Server LAN IP Address*. It's the address of the router, which will now be your file server address.

1. **From the Start menu, select Run, then two backslashes followed by the IP address of the router. I've shown this in Figure 7-15 using the IP address of my router, which is 192.168.99.1.**

2. **After you click OK, you are asked to log in (see Figure 7-16).**

3. **Type the admin user and password where prompted and select OK (you can also select the Remember my password box if you don't want to have to log in all the time).**

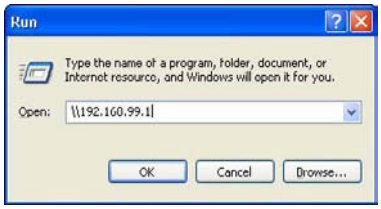


Figure 7-15: Connecting to the file share.

Figure 7-16: Logging in to the file share.

After you've logged in, you see a list of file shares available (see Figure 7-17). The Config file share contains a link to the administrative interface of the router; the Default file share is the one you set up earlier.

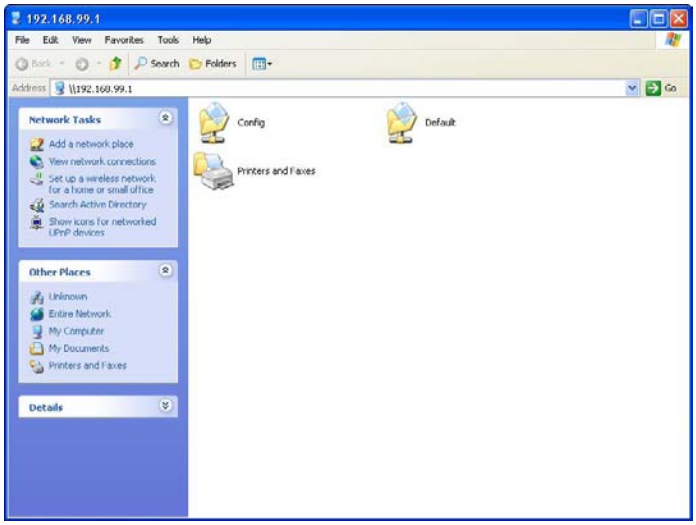


Figure 7-17: The list of file shares

With this all done, you have a centralized place to put your files that never goes away!

Make sure to back up your data, either by periodically burning files to DVD or making copies on other computers. Or, the other way around, this central file share makes a fine backup site for your local files, should something happen to your laptop.

Some of these devices have some features on top of the file sharing. For instance, the Linksys WRT610N can act as a media server which will be auto-detected by Windows Vista and some other universal plug and play capable software. Any media files on the shared hard drive will be instantly accessible to your audio software!

Adding an Access Point

Chapter 1 pointed out that wireless waves don't travel forever, especially if dense objects like walls are in the way. It's possible that you've got some wireless dead spots in your network, or even a whole area such as an outside workshop. Moving your router around might help things out, but at some point you need a second access point.

The general idea behind a second access point is that you plug it into your internal wired network and give it the same wireless settings as the router. If the radios are on two different channels, then your computer will pick which radio to associate with, based on signal strength. If you roam from one radio's space to the other, then your computer moves over to the other access point.

That's the theory, anyway. In practice, I've found that the built-in Windows wireless software doesn't do a great job here, and that you're better off using your manufacturer's software if you plan on roaming between wireless zones. The worst case is that you have to reconnect when you move from one zone to the other.

This is a very effective technique for expanding your network. Your only requirements are an access point and a cable to go from wherever the access point is back to your Internet router.

The trouble I've found with access points is that they're hard to find. I was at an office supply store doing some research, and I found a dozen varieties of wireless routers, but no access points.

Fear not! You'll soon learn how to turn a router into a simple access point. If you're upgrading your router anyway, you can keep your old router to provide lower-speed coverage to a different area of your place.

We're going to be turning off some features that make it easier to connect to your router, but nothing that's irreversible. If you're stuck, do a factory reset on the router and you'll be able to connect again. Usually this involves pushing the reset button while rebooting your router. When in doubt, check the product documentation.

Converting a router into an access point

A wireless router is really a regular wired router with a built-in access point. All you need to do is avoid using the router part, and you've got yourself an access point.

Wireless routers generally have one Ethernet port that goes to the Internet, and about four ports for connecting wired devices into your internal network. These four internal ports are bridged to the wireless side, meaning that they are on the same network.

With that in mind, if you connect the internal ports of two routers together you've got yourself two wireless networks that are connected. See what I mean in Figure 7-18. The goal here is to provide some extra coverage in the basement where the signal is low.

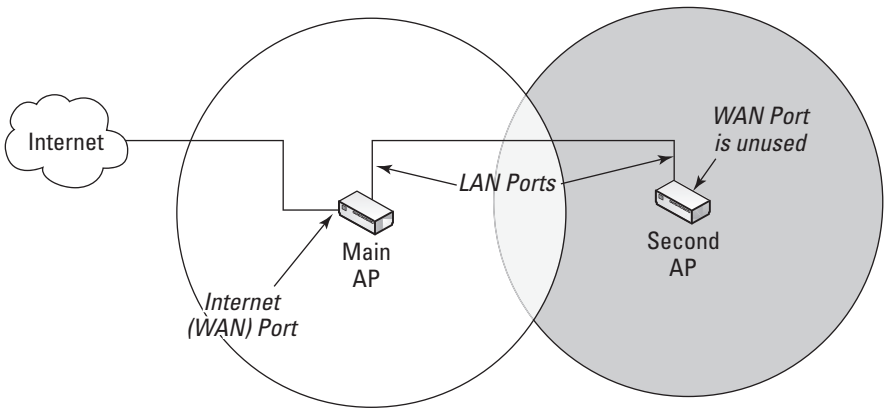


Figure 7-18: Connecting two routers.

As long as those two radios are on different channels, it doesn't matter which one you're connected to because you'll always be in the same network. A few things to keep in mind, though:

- Only one of the routers can be connected to the Internet. The other router's Internet port is not used.
- You need a special cable called a crossover cable to connect two routers together. It looks the same as a regular cable but one of the ends has some of the wires crossed.

- Only one DHCP server is needed for the whole network. If you had two DHCP servers going, there would be a lot of confusion. To make things simple, the DHCP server goes on the router that's connected to the Internet.
- The two routers must have different IP addresses. If they were the same, they'd fight, and your computer would not know how to get out to the Internet. Again, in the interests of simplicity, the router connected to the Internet will keep its address; the other router will pick a new one.

Despite having these four caveats, it's not too hard to do, especially if you do it in the right order.

To keep things straight, the router that connects to the Internet is called the Internet router. The new router is called the expansion router.

Reconfiguring the expansion router

The first order of business is to reconfigure the expansion router. The easiest way to do this is to plug your computer into the router on one of the Internal ports, with the Internet disconnected.

The router I'm using is an older Linksys device that I'm repurposing to expand my wireless footprint. As usual, it may look different than yours, but the concepts are still the same. To reconfigure the expansion router, follow these steps:

1. **Navigate to the Wireless menu and change the network name (SSID), so that it is the same as that on your Internet router.**

   Remember that case matters! See Figure 7-19.

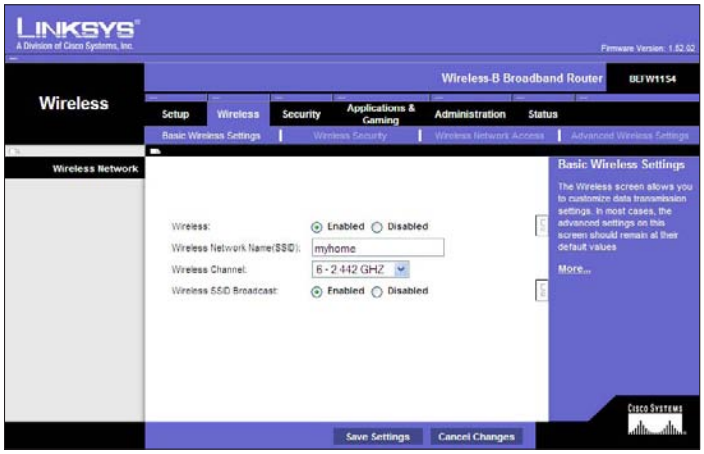


Figure 7-19: Reconfiguring the SSID on the expansion router.

2. **After you've set the SSID, move over to the Wireless Security menu and change the security mode and key to the same thing as what you're using on the Internet router, as shown in Figure 7-20.**

   Disable DHCP on the expansion router and change its address to something that doesn't conflict with the Internet router.

   On this access point, both tasks happen on the same screen. If your router has the features split, then make sure to change the address last! After you change the address, you won't be able to connect to the router until you hook it into the Internet router, at which point you'd have two DHCP servers, which wouldn't be great!

   Figure 7-21 shows the screen to disable DHCP and change the IP address.

3. **Change the Local DHCP Server setting to Disable.**

4. **Change the local IP address to something different than that of the Internet router.** My Internet router's address is 192.168.99.1, so I'm using 192.168.99.2 for the expansion router. Note that the first three numbers are the same, only the last one differs.

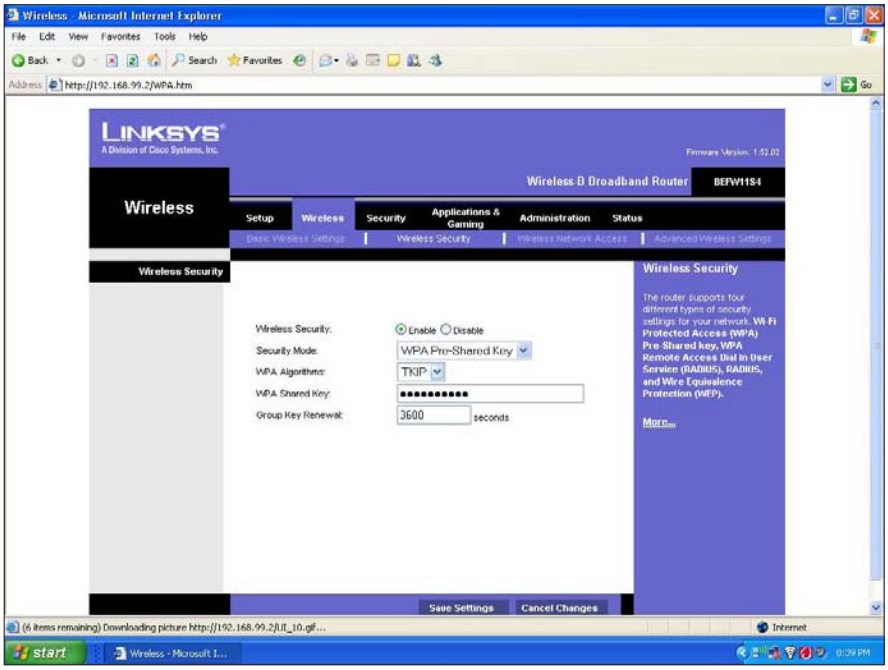


Figure 7-20: Reconfiguring the wireless security on the expansion router.

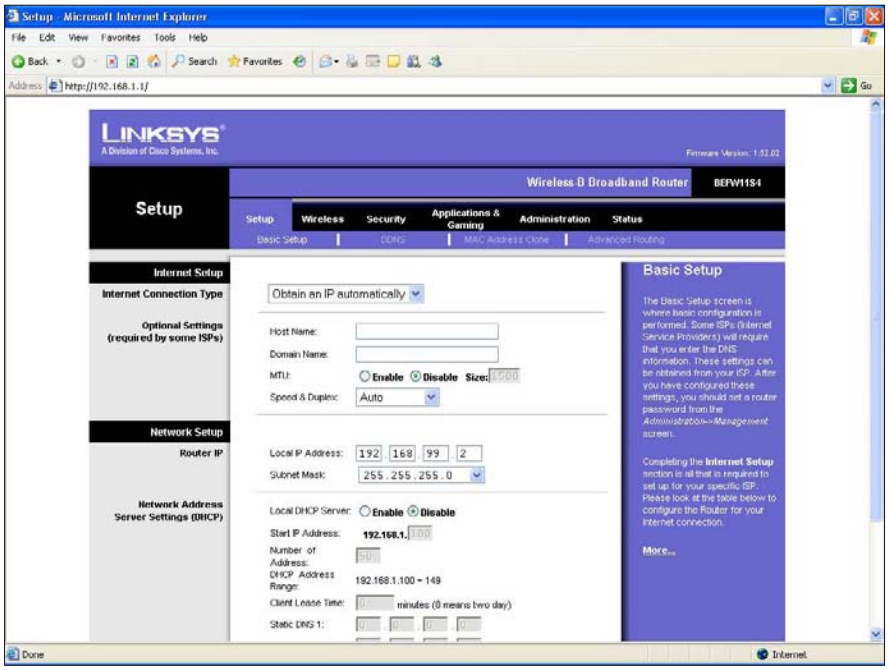


Figure 7-21: Disabling DHCP and changing the IP address on the expansion router.

You might also note that the Internet connection stays on Obtain an IP automatically. This setting doesn't really matter anymore because the expansion router won't be plugged into the Internet.

5. **Click the Save button.**

   After you save the settings, you will lose connection to the router because it's using a new address. (This is expected, and it'll come back in the next step.)

   You should already have a crossover cable run from your Internet router to the expansion router.

6. **Plug this cable into an internal port on each router.**

   The port number doesn't matter, but it has to be the internal port. Don't use the Internet port on the expansion router!

You can now connect to either router using their address in your Web browser. You can access the Internet, and any other computer on your network, while associated to either of the access points. In fact, you shouldn't even know which network you're on!

Chapter 8: Troubleshooting Network Hardware

In This Chapter

- **Isolating network problems**
- **Troubleshooting problems in order**
- **Upgrading drivers and firmware**

Technology always works, right? I don't believe that either. Many pieces have to come together correctly to put a Web page on your computer and get your e-mail delivered so that it's a wonder that it works at all.

Sometimes parts break or just don't work the way you want them to. You've just built a wireless network; it's quite probable that something needs to be fixed.

In this chapter, we look at fixing your network problems, or at least getting far enough that you can point the finger at your service provider.

Before You Begin

Was your wireless network working, then you did something, and then it stopped working? Even if you did something, that shouldn't have made a difference. Maybe you installed some new software, changed a name, or were rearranging some cables.

If so, undo what you did. If it's not undoable (such as moving cables around), make sure everything was exactly the way it was before.

Most computer problems happen because something was changed. It's okay to change things, but when the change makes your computer break, backing out of the change is faster than fiddling around.

Coming Up with a Plan

Successful troubleshooting means following a plan. I'm not talking about a detailed written plan — most often a picture on a scrap of paper can suffice.

Generally, you start at one end of the network and work your way through to the other end until you've found the problem.

Defining the problem

Before you start anything, define your problem. Framing this definition in terms of what you are trying to do that's not working is important. Some good descriptions are

- I'm trying to browse to http://example.com, but my Web browser says "Host not found."
- I'm trying to get my e-mail, but Outlook tells me "Invalid password."
- I'm trying to get the sports scores, but my Web browser just returns a white screen.

Note that in all cases the problem description includes an error message, or at least a description of what you are seeing, along with a description of what you're trying to do. This information helps guide your troubleshooting and will be essential information if you have to call someone for support.

A few bad problem descriptions are

- The Internet is down.
- My e-mail is broken.
- My site doesn't work.

These phrases don't communicate anything to people trying to help, nor do they describe the problem.

If you have multiple computers in your house, then you should check to see if the problem exists on some of those. Doing this helps differentiate a computer problem from a network problem.

Drawing a picture

It may sound corny, but drawing a picture can help your troubleshooting considerably. A picture helps you understand how all the parts go together, which guides your problem solving.

You can see a sketch of my network in Figure 8-1:

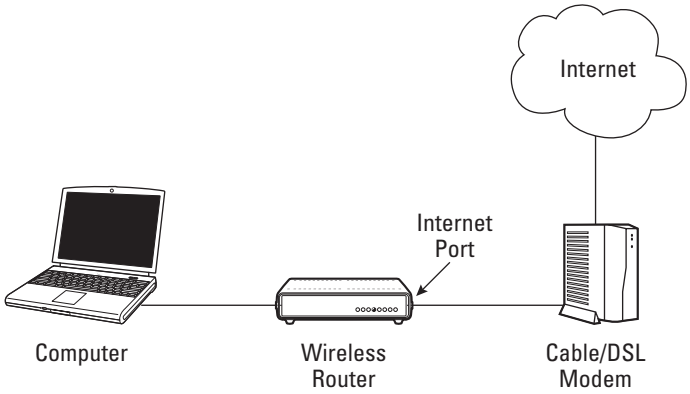


Figure 8-1: A sketch of a network.

See? It can be pretty simple. The computer connects over the wireless network to the router, which connects to the Internet, through the cloud known as the Internet to the Web site.

Is the error message trying to tell me something?

Now that the network layout is fresh in your mind, look at the error message that comes up when you try to perform your task. Is it pointing out something?

For example, if your e-mail client tells you that the username and password are wrong, you should jump straight to verifying those items. Sometimes, though, the error message doesn't make things any clearer for you, which means that you need to continue to troubleshoot.

Is the problem the same for all sites?

If your problem has to do with a Web site, then check another Web site to see if it has the same problem. Sites such as Google.com, yahoo.com, and ebay.com should generally be available, unless the problem is more local.

If you can get to other sites, then chances are your site is having problems, and you'll just have to wait it out. You could call a friend and ask if they're having the same problem, just to make sure.

If other sites seem to be down, too, then the problem is probably on your end, and it's time to fix it.

If Web sites work, but e-mail doesn't, then there's little point in following the guidelines in this chapter. You've shown that the Internet works and that it's a problem with your ISP. Skip straight to calling your ISP.

Looking at Your PC

Starting at the left of the network diagram, you want to make sure your computer's working correctly.

Before you start checking your PC's settings, can you log into the administrative interface of your router while connected to the wireless network? If so, your PC's probably okay, and you can skip to the next section. If not, it's time to troubleshoot the PC.

Repairing your network connection

In Windows XP, right-click on the network adapter icon in your system tray and select Repair. Your computer disables the network adapter and then brings it up.

In Vista, right-click on the network adapter icon in the system tray and select Diagnose and Repair.

Rebooting the computer

If resetting the network connection doesn't work, then reboot your computer. I know it's a pain, but this is Windows after all, and sometimes it needs the computer equivalent of a swift kick in the behind. Rebooting solves a lot of problems.

After a reboot, Windows gets a fresh chance to do things in its own order and from scratch, which is often enough to fix a problem with the computer.

Checking the wireless association

At this point, you've rebooted your computer so you know that it wasn't some sort of transient thing that most computers experience. Looking back at the network diagram, the problem must either be between you and your router, the router itself, or with the rest of the Internet.

If you can, try plugging your computer into the router using an Ethernet cable instead of using wireless. If things work with a wire, then the problem must be with the wireless connection. If not, you can troubleshoot the router.

Go back to your list of wireless networks (see Chapter 6) and make sure you're connected to the right one! If your computer loses connection to your original access point, it will try to find another one and associate with that, even if it doesn't belong to you or work properly. You might not even notice this happening at the time.

If you're not connected to the right wireless network, or you're not connected to any network, review Chapter 6 to configure your computer. Try it with both the built-in Windows configuration and your vendor's configuration tool.

Pay close attention to the signal strength as you configure your network. A low strength is a sign that you need to either move your router to a better spot or add a second access point for more coverage. Put your computer in the same room as the access point while configuring, just to make sure.

Incorrect passwords are often the culprit when dealing with association problems. Review the settings on the wireless router and make sure that they match those on the computer. If Wireless Protected Setup is available to you, then use that method.

If, after all that, you can't associate with your wireless network, skip ahead to the end of this chapter and upgrade your router firmware and your computer's drivers.

Verifying your IP settings

If you're able to associate with an access point and you are still having problems connecting to the Internet, then it's time to make sure you're getting a proper address.

In Windows XP, right-click on the adapter in the system tray and select Status. Then click on the Support tab and click Details.

In Vista, choose Start➪Control Panel➪Network and Sharing Center. Click on the Status link next to your wireless adapter and then click Details.

You are looking for the following information:

- IP address (or IPv4 address in Vista)
- DHCP Server
- Default gateway
- DNS Server

Checking the IP address

The IP address identifies your computer on the network. The IP address probably begins with 192.168, though it could also begin with 172 or 10. These are the reserved private network addresses and are used for people behind routers.

If your IP address begins with 169.254, then you aren't getting an address from your DHCP server. If a computer doesn't hear from a DHCP server, then it picks one of these addresses. This is okay if you have computers that want to talk to each other, but it will not work with your router.

Pay special attention if your computer roams between networks, such as home and work. Sometimes Windows doesn't pick up a new address when it changes networks, and it is vital to have a proper address. This is why the first step in troubleshooting is to initiate a repair operation on the adapter or reboot the computer.

DHCP and your gateway

Your DHCP server should be the address of your router. It should also be the same as your default gateway. If you don't have a DHCP server set, then your computer might be set with a static address. Generally, you want to pick up a dynamic address.

If you have an IP address beginning with 169.254, then it's possible that your router does not have the DHCP service turned on. If so, it's best to do a factory reset of your router and start from scratch.

If your DHCP server is different from your gateway, then you might have two DHCP servers running on your network. Recall from Chapter 7 that you only want one DHCP server, and it should be the device that also plugs in to the Internet (and should therefore be your default gateway).

You should also have a gateway set. The gateway is the device that your computer uses to send information to the Internet.

Changing to DHCP addressing

If you don't have a DHCP server set, then your computer is probably hard coded with an address (also called a *static address*). To work properly on your network, you want to use DHCP addressing.

If your computer was set up with a static address for a reason, such as to work with an office network, then you have to switch your settings every time you change networks. It would be worth your time to find out if you can use DHCP on the other network.

1. **In Windows XP, right-click on the adapter icon in your system tray and select Status.**
2. **From that dialog box, click the Properties button.**

   A dialog box like the one shown in Figure 8-2 appears.

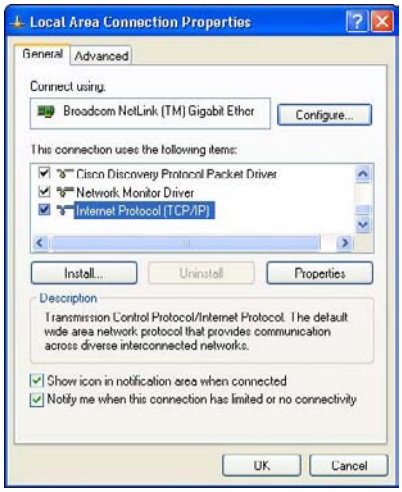


Figure 8-2: Windows XP adapter properties.

3. **In the This Connection Uses the Following Items area, scroll down until you see Internet Protocol (TCP/IP). Select that line and click the Properties button.**

   The dialog box in Figure 8-3 appears.

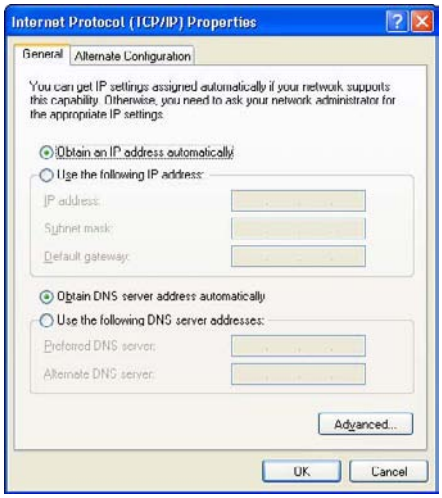


Figure 8-3: Windows XP TCP/IP properties.

4. **The two radio buttons should be on Obtain an IP Address Automatically and Obtain DNS Server Automatically. If the buttons are on a different option, change them.**
5. **If you had to make changes, then continue clicking the OK button to get out of all the menus. You should be able to obtain an address now.**

Vista is slightly different.

1. **Go to Start⇨Control Panel⇨Network and Sharing Center.**
2. **From the Tasks menu, choose Manage Network Connections.**
3. **Select the adapter and choose Change settings of this connection.**
4. **Select Internet Protocol Version 4, as shown in Figure 8-4, and click the Properties button.**

   The dialog box shown in Figure 8-5 appears.

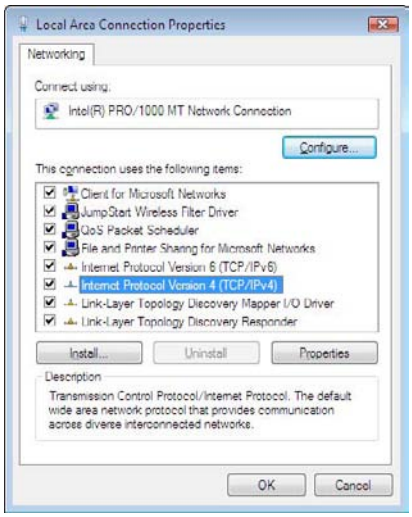


Figure 8-4: Vista adapter properties.

5. **Make sure that the automatic options are selected.**

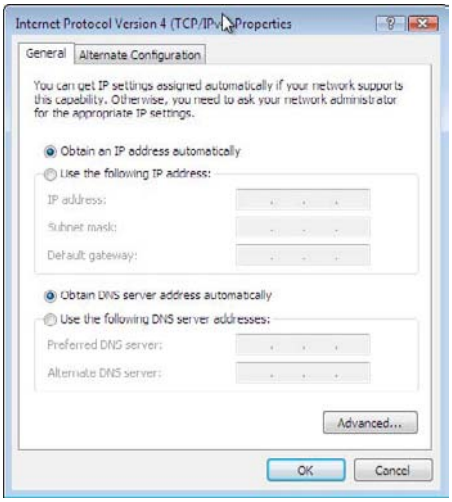


Figure 8-5: Vista IPv4 properties.

Looking at Your Router

You should be able to connect over the wireless network to your router. If not, make sure of the following:

- Do you have DHCP enabled on the router?
- Is the computer able to associate with the wireless network?
- Can you connect to the wireless router's Web interface using its address (such as 192.168.1.1) over the wireless network?

The "Looking at Your PC" section covers these three items in detail.

If you've got through the previous section and still can't connect to the router, then skip ahead to the end and look at updating drivers.

Look back at the network diagram. Because you can connect to the router, you know that your computer is all right and the wireless network works. So, the problem is either the router or the router's connection to the Internet.

Rebooting the router and ISP equipment

Reboots fix a lot of things, and your Internet connection is no exception. Pull the power from your cable or ADSL modem and your wireless router, count to five, and then plug them back in.

While you're at it, make sure that all the cables are plugged in properly. Ethernet cables have a tab on the connector that prevents the cable from falling out, so a gentle tug on the connector verifies that everything is locked in.

Also verify that the devices have power. All devices differ, but they all have some sort of light to indicate that they're on. If, after all this work, you realized that you forgot to plug something in, don't worry; it happens to the best of us!

Give things a few minutes to settle and check again.

Bypassing the router

By now, you've checked all the common problems with the router and you're getting close to the point where you're going to have to call someone for help.

Take your router out of the loop by plugging your computer directly into your Internet connection. For cable modems, this is fairly straightforward, but for ADSL connections you sometimes need some special software.

If you're able to connect to the Internet with your computer directly plugged in to your cable or ADSL modem, then your ISP is off the hook. The problem must be with your router. (I go over this in the next section.)

If you still can't browse the Web with your computer plugged in to the Internet connection, then your provider's probably at fault. You might want to skip down to the "Before Calling for Support" section.

If you've successfully connected to the Internet with the router before, and it just stopped working, then it's probably a problem with your provider. Make sure that you've rebooted everything, and then jump down to the "Before Calling for Support" section.

Setting the connection type

If you remember way back to when you set up the router, you were asked if your Internet Service Provider requires a username and password to log in. This information is required to authenticate to the provider and get your service. If this information is wrong, then you won't be able to log in.

Similarly, if the router is configured to log in, but your provider isn't expecting it, then you have problems.

First, check to see if you're getting an IP address from your provider. On the NETGEAR router, click on the Router Status link, which is in the Maintenance section and is shown in Figure 8-6.

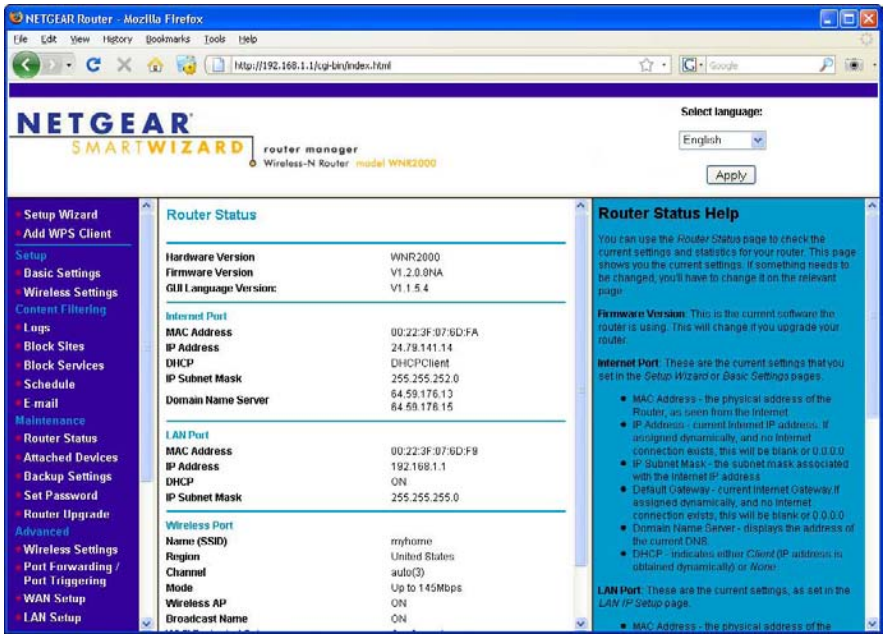


Figure 8-6: The router status screen.

The section of the router status screen headed Internet Port contains the information pertaining to your Internet connection. You can see that an IP address of 24.79.141.14 has been assigned, and that DNS servers have also been given (it is all right that the IP address and the DNS servers look nothing like each other).

If you have an Internet address of 0.0.0.0, then it means that you're not connected to your provider, or your provider is having a problem.

In this event, check the cable between your router and the modem, and between the modem and the provider, to make sure they're attached and in the right port.

Go back to Chapter 3 and make sure your router is set up correctly. If everything seems fine on your end, see the next section to make sure the router's firmware is up to date, and then call your provider.

If at this point all indications are that things should be working but they aren't, you still can't pin the blame on your router or the service provider. In this case, it's best to work through your service provider first to verify that the Internet connection is working, and if that is successful, to call the support line for your router for further troubleshooting.

Upgrading Software

When software is written, the possibility of bugs being introduced exists. One of my favorite quotes about software development is, "If debugging is the process of removing bugs, then programming must be the process of putting them in."

Sometimes software is shipped with bugs (either knowingly or unknowingly), and sometimes changes to other software introduces new bugs.

Thankfully, most devices ship with the ability to upgrade software in the field. For routers, this means that you can upgrade the firmware that runs the hardware. For wireless adapters, this means that you can upgrade the drivers.

The downside is that you need to get on the Internet to get the latest updates. If you are upgrading to regain your Internet connection, then you have to use a working computer to get the appropriate software onto a USB pen drive or a CD-ROM.

To find the latest software upgrades, go to the home page of the device's manufacturer, and look for a link called either "Support" or "Drivers and Downloads." You'll need to know the model number of the device you have.

Upgrading router firmware

Your router is a special purpose computer and needs some special software to make it run, much like your computer needs an operating system like Windows to run. For routers, the manufacturer provides the operating system. The router comes with a version of the software, but periodically updates are released.

Updates are a good thing for you, the consumer. A few years back, when the wireless encryption standards were in a state of flux, manufacturers were able to release updates containing the latest standards. This way, customers could be using the latest security protocols without having to buy a new router. When the 802.11n standard makes it out of draft form, you should be able to download an updated version of your router code that will bring you into compliance.

The software that a router runs is called *firmware*, which is some geek's way of talking about something halfway between hardware and software.

Download the firmware from the vendor's support site and store it on your computer. If you got the file as a .zip file, then unpack it first.

Most manufacturers recommend doing upgrades while connected to a wired port rather than wireless. This is because if the connection is interrupted during the upgrade, the router will only have part of the new image, and it might not run correctly anymore. The technical term for this is called *bricking* your router, because a failed upgrade usually renders the device with the same functionality as a brick.

1. **Look for a menu item within the router's Web GUI that talks about upgrading.**

   Figure 8-7 shows the upgrade menu from the NETGEAR router.

2. **Click the Browse button to locate the image you downloaded and click OK.**

3. **Click the Upload button to send the software image to the router.**

   The next screen prompts you to confirm the version number on the router. In Figure 8-8, you can see that the current revision is 1.2.0.8, and I'm trying to upgrade it with the same version.

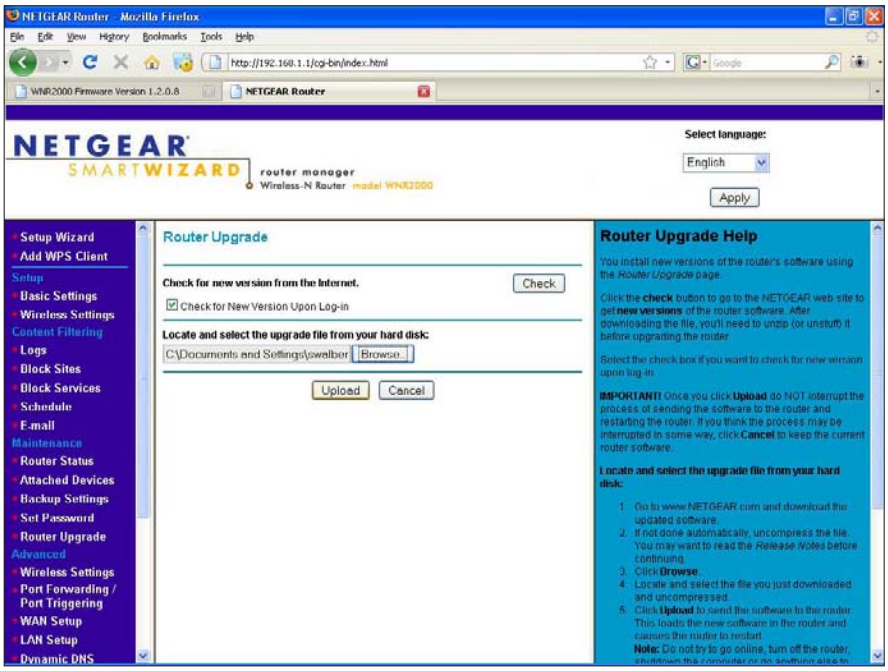


Figure 8-7: The NETGEAR router upgrade.

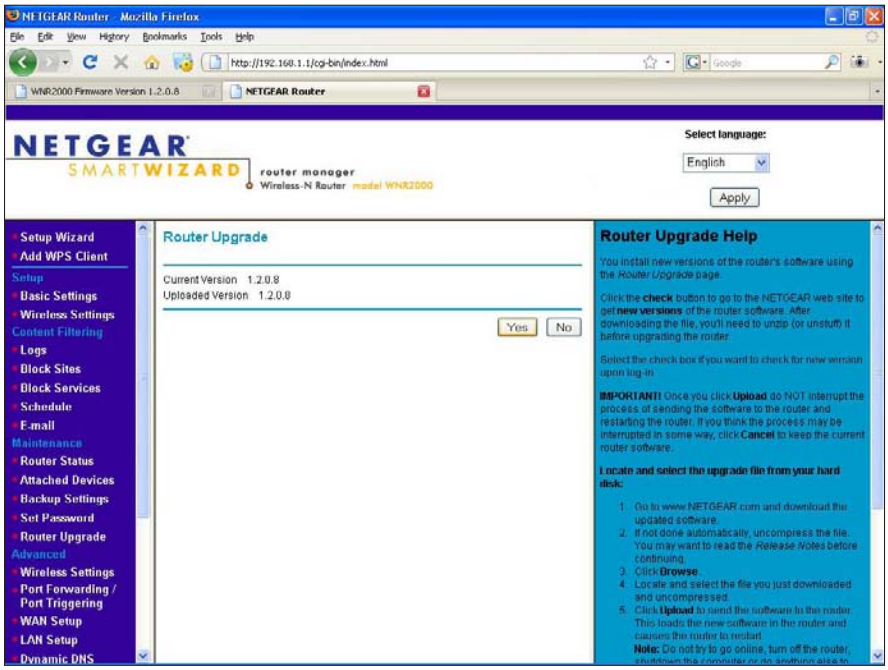


Figure 8-8: Confirming the firmware versions.

4. **Click Yes if you want to continue.**

   The router displays a progress bar and thinks for a while before rebooting and bringing you back to the main menu.

Don't touch your computer while this process is happening. Go grab a coffee or something. It'll finish on its own!

That was easy, wasn't it?

Upgrading your network drivers

The network drivers control how the physical adapter interfaces with the rest of the operating system. Changes to the operating system sometimes mean that you have to update your driver. Sometimes new wireless features are added to the adapter that allow you to be more compatible with other wireless networks.

While you're upgrading your drivers, you may as well upgrade the wireless utilities. In fact, doing both at once is usually easier than going the long way and upgrading your drivers.

Most manufacturers release a self-installing package that automatically updates your wireless drivers and the wireless utilities. It's remarkably simple to use.

For this example, I went to the Intel support site and searched for 3945ABG, which is the wireless card model I have. I know this because it's printed on the bottom of my computer. I was then asked to choose my operating system. Finally, I saw the screen shown in Figure 8-9.

The following options are available:

- The first option is to download only the wireless drivers. Doing this updates the adapter to the latest code, but it won't touch the management tools. The key words here are drivers-only.
- The second option is to download the drivers and management software. This includes both the wireless drivers and the connection utility. This option is the better choice in my humble opinion, even if you don't use the vendor's management utilities.

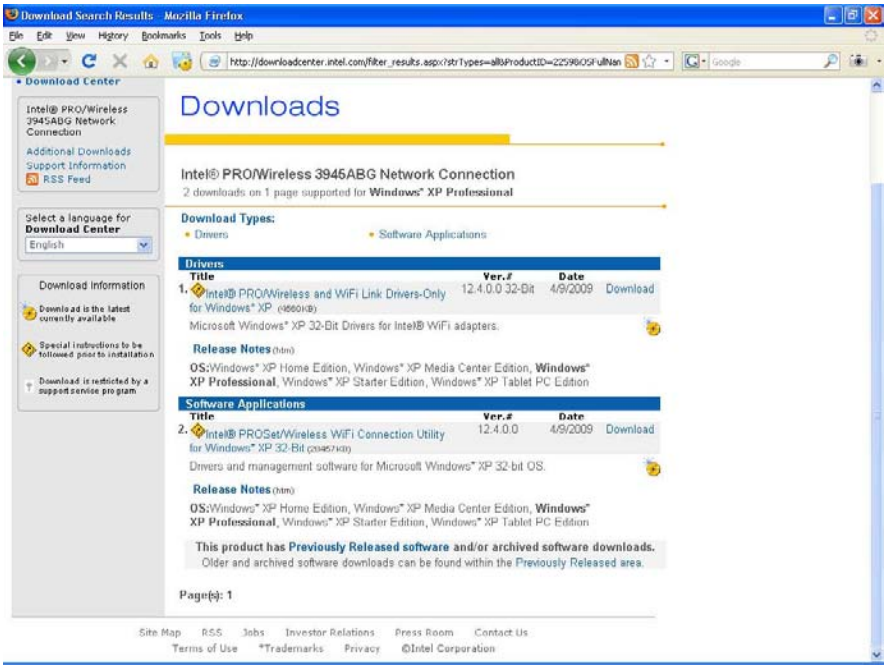


Figure 8-9: Choosing between drivers only, and drivers and utilities.

Click the Download link, accept the agreement, and then save the file to a directory, such as your desktop. Run the program that you downloaded and follow the prompts. It's fairly uneventful.

Before Calling for Support

If you got this far, then you're calling either your ISP or your router manufacturer for support. That's all right, because that's what they're there for. You can do this before you call to make the process go quicker, though.

Whatever you do, don't get mad at the person on the other end of the phone. Doing so just makes the repair take longer. Remember that he didn't cause the problem — they're trying to help you. Introduce yourself and greet them by name.

No matter who you're calling, make sure to have the following things handy:

- A concise description of the problem and what you think should be happening
- An estimate of when the problem started
- A list of what you've done so far
- A description of what your network looks like

If you are calling your service provider, make sure that you know the following:

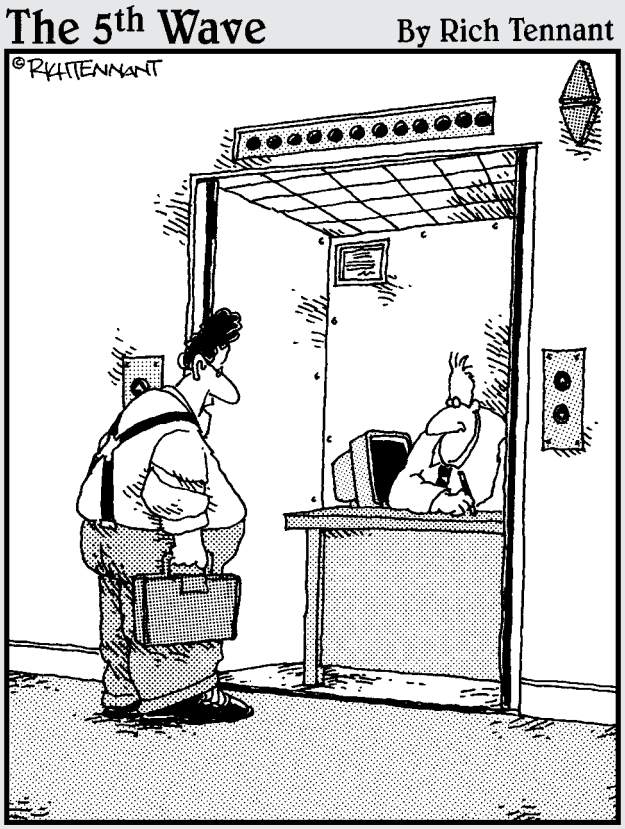
- Your account number or billing address and what kind of service you have
- A description of which lights are on the modem and what color they are
- The last time you rebooted your computer and modem

If you are calling your router manufacturer, have the following handy:

- The model number of the router in question.
- A description of which lights are on and what color they are.
- A summary of what you've tried. Does the router work if you are wired in but not wireless?

The people on the phone will start by asking many of the same questions that have already been asked in this chapter. Just go with the flow — they're just trying to make sure the common problems have been covered.

Book III
Configuring Networks



"You the guy having trouble staying connected to the network?"

Contents at a Glance

Chapter 1: Exploring Windows Networking

In This Chapter

- **Windows XP makes wireless easy**
- **Plug and play . . . hopefully**
- **Choosing the kind of network you want**

Microsoft introduced an easy wireless network setup and configuration with the release of Windows XP in 2001. Prior to that, installing any kind of network using Windows computers was often a hassle and usually unpredictable. Skip ahead to 2009, and subsequent editions of Windows (most notably Vista and the new Windows 7) have made things even easier! In many cases, it's as simple as turning on your computer or flipping a switch on your laptop.

If you have a typical setup, which includes a modern PC and networking equipment released in the past one or two years, creating a wireless network should be a snap. If all goes well, you can install a wireless network adapter in your PC, and you're almost ready to connect with your chosen wireless network. The best part is that once you set up your wireless network, it's completely low maintenance — don't expect to have to toy around with the settings very often. Now, cross your fingers (I'm watching, as is Microsoft) and venture into the relatively painless world of Windows XP and wireless networking.

Installing Is Child's (Plug and) Play

Most of the work of installing a wireless network is done by the computer as part of the operating system's plug and play feature. That means after plugging in your adapter, it should be installed automatically (or close to it). You may have to install a driver or supplemental piece of software to interact with the hardware, but it's a very easy procedure to perform.

With modern wireless technology, installing the necessary hardware into your computer is usually so-called plug and play. In other words, the process is supposed to be mostly automated: You plug in your network adapter

(a card that transmits and receives signals over your wireless network), and the operating system is supposed to recognize, install, and configure it with minimal action on your part.

If you have newer hardware, this should be the case most of the time. If you're trying to use an older or obscure network adapter (stay away from the bargain bins!) or own a computer that you bought more than, say, eight or nine years ago, this might not be the case.

And remember that I'm talking about Windows XP Service Pack 2 or later here. If you're running an older operating system, all bets are off. My advice: Upgrade to Windows Vista before you pursue this course called wireless networking. If you're one of those home computer users that just isn't comfortable using Windows Vista for whatever reason, then you'll want to make sure you're using Windows XP Service Pack 2 at the very minimum or plan on upgrading to Windows 7 upon availability. In order to remain consistent with Microsoft's current offering at the time of publishing, I work with Windows Vista in any relevant procedures.

Just because Windows can configure your network adapter doesn't mean you want it to do so. You may find that the utility software that came with the adapter provides more features and better feedback about signal strength and other basics. For example, the Intel Pro Wireless Network Connection is a more than capable alternative to Windows' Network and Sharing Center.

In that case, let Windows' plug-and-play feature handle the installation, and you can look to the network equipment maker for the software to add any extra features that Windows doesn't add automatically. Just remember, if you decide to use a third-party application to manage your computer's wireless capabilities, it completely shuts Windows out of the picture until you decide to revert.

Working with the Network and Sharing Center

My Network Places is replaced in Windows Vista with the Network and Sharing Center, as shown in Figure 1-1.

The Network and Sharing Center is really a one-stop shop for all of your network needs; it truly is the hub of your broadband experience. When you first access the center, as discussed in the following sections, you will find out a lot about your network. For example, Windows draws a basic schema of your network connection that shows your computer, the name and type of network location, and finally to what you're connected (the Internet!).

Figure 1-1: The new Network and Sharing Center.

From the main panel in the Network and Sharing Center, you can find out more information about your network, such as the name and access you have. While it's a more text-based version of the aforementioned schema, this section lets you rename your network. Remembering Mike's Network is easier than remembering Network 24, which is default Windows fashion. This section is also important because it indicates whether or not you actually have Internet access. When everything is running smoothly, it says Local and Internet. Should you see only Local only, you know you've got problems on your hands and you should consider rebooting either your computer or your wireless router.

The second section of the main pane concerns your file sharing options (Sharing and Discovery). By default, all available menus are collapsed but can be expanded to set your preferences. Each option is represented with a green light (on) or a gray radio button (off), indicating the status. The sharing options also extend to printers, media files, and public folder sharing. I recommend only enabling these options when you are working on a private network, such as at your home. If you are in a public place, you will really want to think twice about making key folders on your computer available to everyone within wireless range.

The left side of the Network and Sharing Center displays a series of tasks and related topics. With respect to wireless networking, these tasks allow you to either set up a new wireless network or connect to an existing, available wireless network within range of your computer.

What is a public folder?

If you grew up using Microsoft Windows as your primary (if not only) operating system over the years, you're undoubtedly familiar with the legendary Windows folders: My Documents, My Pictures, My Music, and so on.

Windows Vista offers a few new changes to that tried and true practice. First, you've likely noticed that Vista has dumped My. More importantly, Vista offers a second set of documents called Public folders. These folders, which include Public Desktop, Public Documents, Public Downloads, and so on, as shown in the figure, let you make specific files and folders available to others on your computer or your network. To use them, simply drag and drop the file or folder into the corresponding Public folder. These folders are accessible from Windows Explorer.

So, when do we actually get to meet the Network and Sharing Center? How about right now? The following sections provide several ways for you to access it in Windows Vista.

Accessing from the Windows taskbar

Here's how you access the Network and Sharing Center from the taskbar:

1. **Right-click the network icon (two screens joined with a planet Earth) in the right-side of the taskbar, as shown in Figure 1-2.**

   The corresponding contextual menu appears.

2. **Click Network and Sharing Center.**

   The Network and Sharing Center appears in a separate window.

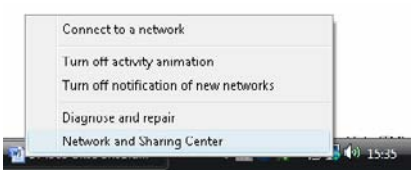


Figure 1-2: Accessing the Network and Sharing Center from the taskbar.

Accessing from the All Programs menu

Perhaps you are more old-school and like to use your keyboard to locate Windows features:

1. **Click the Start menu icon.**

   The Start menu appears.

2. **Type Network in the Start search text box at the bottom of the menu.**

   The entries are filtered to show only applications or elements displaying the word "network," as shown in Figure 1-3.

3. **Click Network and Sharing Center.**

   The Network and Sharing Center appears in a separate window.

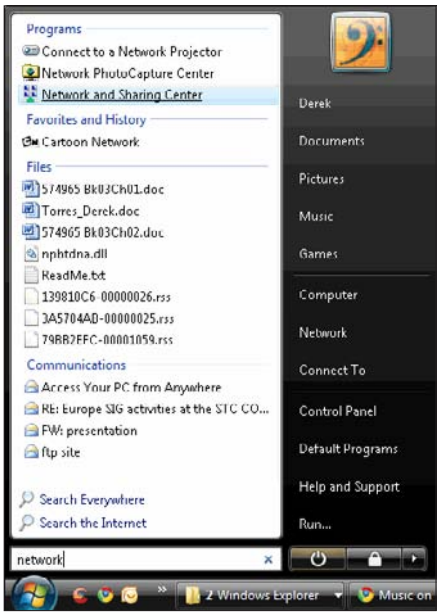


Figure 1-3: The returned list of applications, including Network and Sharing Center.

Mingling with Different Networks

You can create two kinds of networks with Windows:

- **Infrastructure:** Chances are you want to create an infrastructure network, which is the traditional network that uses a DSL or cable modem connecting to your computer directly or through a router.
- **Computer to computer:** You also see this called a peer-to-peer or an ad hoc network. It's a connection made directly between one computer and another.

As always, each has advantages and disadvantages.

Thinking about an Infrastructure Network

Most likely, when you think of a wireless network, you're thinking about an infrastructure network. Book II is essentially about creating an infrastructure network. I avoid repeating that information here.

However, anytime you communicate between a wireless access point (such as a wireless router) and a wireless network adapter, you're moving information over an infrastructure network. When you're on the road and using a coffee shop's wireless access, you're connecting to an infrastructure network. Your computer is connecting through a wireless access point, which in turn connects to the Internet.

In most cases, it just makes more sense at home to set up and run this kind of network instead of a computer-to-computer network.

Creating a Computer-to-Computer Network

A computer-to-computer network means exactly that: Your computer is wirelessly connecting directly to another computer. This is known as an ad hoc network. Both PCs need wireless adapters, of course. Windows XP also will need to be set up to handle a computer-to-computer network connection.

At one time, a computer-to-computer network may have been cheaper to create because you didn't need a router. Instead, one computer can connect to the Internet and the other PC can wirelessly share that connection. Declining hardware costs provide no reason to use a computer-to-computer network when what you really need is an infrastructure network, which requires a router and possibly other hardware.

You can use a computer-to-computer network in your home or on the road, but a wireless network usually has specific applications, including the following:

- On a business trip, you and a colleague can connect your laptops wirelessly, allowing you to share files without the use of a router or other wireless access point.
- Anytime you're mobile, the network moves with you because you don't have to lug routers or other hardware (aside from your laptop).
- Anywhere an infrastructure network's wireless access point is unreachable; a computer-to-computer network provides an Internet connection, provided one of the computers is connected to the Internet.
- If you don't want to rely on the hardware in an infrastructure network, a computer-to-computer network provides redundancy. If a router goes down on an infrastructure network, the whole network stops working.

With a computer-to-computer network, another computer can always share the load. (This assumes more than two computers are in the computer-to-computer network.)

Creating a network for work

Depending on your network configuration at work, it may be possible for you to connect to your servers or computer at the office from home or on the road. To do this, you must first connect to your office's network and then use the Remote Desktop Connection application, which allows you to connect directly to a specific machine or server.

Before trying to create a connection to your office's network, verify with your IT or helpdesk team that you are authorized to create such connection. You also want to make sure that you have the parameters and login settings necessary to log on successfully. Of course, for security reasons, be sure to log off from the network or your remote computer when you are done with your session.

To connect to a work network, you need to first connect to a Virtual Private Network (VPN), which lets you act as if you were plugged in at the office. This type of network is covered in Book V, Chapter 6.

After you are connected to your VPN, go to Start➪All Programs➪Accessories➪Remote Desktop Connection. Once you add your credentials (available from your company's network administrator, if you don't already know these details), you can access your computer exactly as if you were at work.

Enabling Internet sharing

After you have a computer-to-computer network set up, you can configure one computer to share an Internet connection with the other computers. I don't recommend using this fast and dirty way to share broadband access unless you have no other choice. It's slow compared to using an infrastructure network with a router.

If you can, try to build an infrastructure network where a router does the work of divvying out IP addresses to each computer and, most importantly, hides the network behind a firewall.

This method is really a last-ditch effort when you need to share an Internet connection. With the advance of networking and wireless technologies in recent years, it's hard to believe that this option is still available!

Chapter 2: Managing Available Networks

In This Chapter

- **Finding out about wireless networks**
- **Adding a preferred network**
- **Watching your network**
- **Setting some advanced preferences**

A good thing about wireless networks is that you don't have those pesky Ethernet cables to tie you up in knots. I can still remember back in the old days when I'd have those drab, gray cables running from room to room. I also remember constantly tripping over said cables; fortunately, those days are gone! That doesn't mean that wireless networks are always easy to set up and use. Hopefully, you've made it past the rough spots and are ready to actually transfer data around your home.

Maybe your wireless network is ready to send data between your living room and second-floor bathroom. If so, make sure your PC can see the router and any other access points. That's where Windows Vista's Connect to a network feature in the Network and Sharing Center, formerly known as Available Networks for Windows XP, enters the picture.

I also discuss some ways to monitor your network's signal strength and capacity. Other chapters discuss similar network troubleshooting and maintenance topics:

- Book II, Chapter 8 gives you some help troubleshooting network adapters.
- Book III, Chapter 5 discusses how you confirm your wireless network is working.
- Book IV, Chapter 3 gives you some tips for solving wireless networking problems.

Discovering What's Out There

Notice that the title doesn't say who is out there. After all, this chapter's about wireless networks, not dating. If you're still interested in finding what's out there, read on, because you're in the right place.

The Connect to a network feature lets you see what networks are available — for dial-up, VPN, and wireless. Available means that they're out there, probably close by. The list should include one or more of your own networks, if all goes well. If you don't see your networks, be concerned.

If you sort the list to only display available wireless connections, the list is displayed by signal strength, which is indicated by a series of bars (much like the ones used by mobile phones to display signal strength).Your network(s) should be at the top of this list; if it's not, it should be quite closer; otherwise, we should discuss where your wireless router is stored, not to mention where it is that you tend to do most of your work.

In some cases, you see neighbors' wireless networks. That doesn't mean that you can connect to those networks, though. (I tackle that issue in more detail, along with other security topics, in Book IV.)

You likely won't see wireless networks where the owners have intentionally made them invisible to public viewing. The geeks can still discover your network name, but it's one tool in your security toolbox. After I tell you about monkey wrenches and screwdrivers (I'm trying to milk this toolbox metaphor), I talk about how you can make your network mostly invisible in Book IV.

1. **Right-click the network icon in your Windows notification area.**

   A menu appears.

2. **Select Connect to a network.**

   You see something like Figure 2-1. The dialog box lists Available Networks. In this case, Dog is the network and Livebox-bbcc is the neighbor (possibly the one with the barking dog and who insists on partying every weekend).

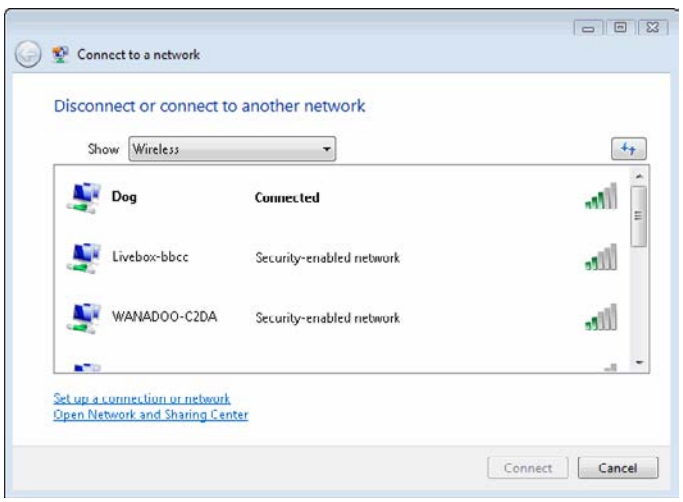


Figure 2-1: The Connect To a Network dialog box displays all available wireless networks, or rather all those in range of your computer.

3. **Click the name of the desired network and click Connect.**

   If the selected network requires a network key, now's the time to type it in this screen of the dialog box, as shown in Figure 2-2.

Figure 2-2: You need to know the security key for a secured network before you can use it.

Some networks require a network key, which is basically a password with so many unrelated letters and numbers that only a Jeopardy contestant can remember it. You can tell if the network requires a network key because it is labeled as a security-enabled network.

What if an available network requires a network key, but you don't have one? If you're sure it's your network or one you've been invited to use, you should ask its administrator for The Magic Key. Unfortunately, "abracadabra" doesn't work here.

4. **If a network doesn't require a network key (labeled as an Unsecured network), click the Connect Anyway link as shown in Figure 2-3.**

   If you do use an unsecured network, be aware that your data may be visible to other parties. Though there is some security risk in using unsecured networks, you can take precautions (and others that Windows automatically takes for you in this case, which I will discuss later).

   It's a scary option, I know, but select it for now. I tackle security issues in another chapter. That's it! You're done.

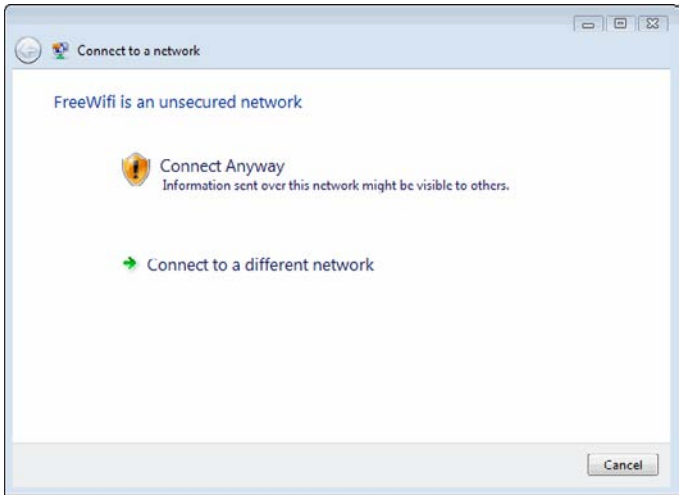


Figure 2-3: If you are going to use an unsecured network as a wireless connection, Windows makes sure that you realize what you're getting yourself into.

You can do something that ensures almost always having a working Internet connection. In one word, it's called redundancy. Say a DSL line now comes into your house. Well, call up the cable company and order its cable modem service, too. Now use one connection for your wired network and the other connection for your wireless network. If one goes down, you can easily switch to the other Internet connection. Too bad you can't do that with electrical service!

What the heck is a, b, g, n?

When you went to your local electronics store to buy a laptop, or a wireless router/card, you likely noticed that 802.11 (followed by a/b/g/n) appeared on the box. These are wireless protocols that are used to designate a set of standard for wireless communications. For example, if you are using 802.11a (which is very unlikely these days), you know that your wireless connection is operating on a certain frequency and has a set data transfer rate.

There are currently four protocols used for wireless communications. The oldest are "a" and "b" — which are also the least powerful. I'd say that "g" is the most commonly used protocol, but it will quickly be replaced by the "n" protocol, which has only been available for a relatively short amount of time. When you buy a wireless router, you must make sure that your laptop computer or wireless card is compatible with the router. If you buy an 802.11n wireless router, but only have a "g" compatible card, you won't be able to take advantage of the high performance of the "n" protocol.

To get a good idea of the difference between the various protocols, here are some facts and figures:

✓ (A) 802.11a	✓ (G) 802.11g
Frequency 5 GHz	Frequency 2.4 GHz
Typical Data Rate 23 Mbit/s	Typical Data Rate 19 Mbit/s
Max Data rate 54 Mbit/s	Max Data rate 54 Mbit/s
Range 115 feet	Range 125 feet
✓ (B) 802.11b	✓ (N) 802.11n
Frequency 2.4 GHz	Frequency 5 GHz and/or 2.4 GHz
Typical Data Rate 4.5 Mbit/s	Typical Data Rate 74 Mbit/s
Max Data rate 11 Mbit/s	Max Data rate 300 Mbit/s (2 streams)
Range 115 feet	Range 230 feet

Viewing Available Networks

If you followed the previous set of instructions, you've made it past the initial gatekeeper. You can view all available networks now. After following the steps in the preceding section, you find yourself in the Wireless Properties dialog box.

As I mention earlier, you may see your neighbors' wireless networks on the list. Ignore them, as it's the right thing to do. Hopefully, they'll do the same for you. Besides, you were wise enough to enable security on your wireless network, so there's no chance of them getting on, right?

If the stars are aligned, you see your wireless network along with other kinds of networks on the list, as shown in Figure 2-4. Again, in the example the network is dubbed Dog, which does not reflect on myself, my cat, or my network hardware.

You can refresh the list of available networks by clicking the — yes! — Refresh button, which is above the list of networks, to the right (across from the Show scroll-down list). If you're in a neighborhood with lots of wireless networks, you'll probably see this list constantly change as some networks go live and others shut down.

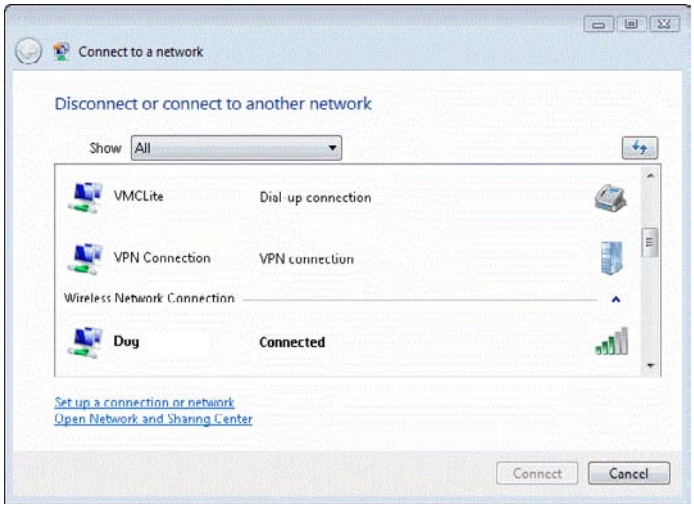


Figure 2-4: Besides your wireless networks, you might also find dial-up and VPN connections.

You can configure an available network from the Manage Wireless Networks page, which is available from the Tasks list in the Network and Sharing Center. Configuration options include changing the network name (which is also called the SSID) and the wireless network key. Here's how you configure an available network:

1. **In the Network and Sharing Center, click Manage wireless networks under the Tasks list.**
2. **Click the name of the network you wish to configure.**
3. **Right-click and select Rename. (The network name becomes an enterable text box, as shown in Figure 2-5.) Rename the network and click outside the box.**

   A dialog box appears warning you of the consequences of such actions. Validate this dialog box. The network appears in the Manage Wireless Networks page with its new name.
4. **Right-click the name of the network and click Properties; click the Security tab.**

   The following dialog box appears, as shown in Figure 2-6.
5. **You can make one or more changes to Association settings:**
   - Toggle Network Authentication between Open and Shared.
   - Change the Data Encryption setting to Disabled or WEP. If you select WEP, you can enter a network key and make other related changes. WEP is discussed in Book IV, Chapter 3, which covers the implementation of wireless network security.

6. **Click OK.**

   Whew! That's it for configuring available networks. Now, onward to preferred networks.

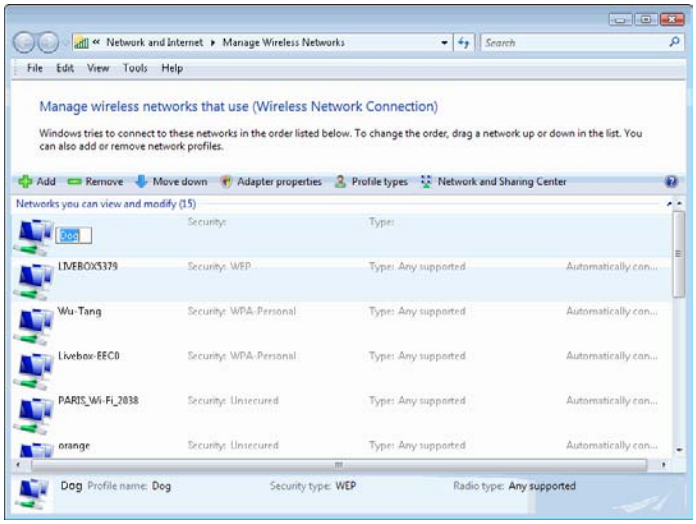


Figure 2-5: You can rename your SSID, or wireless network, to make it more recognizable.

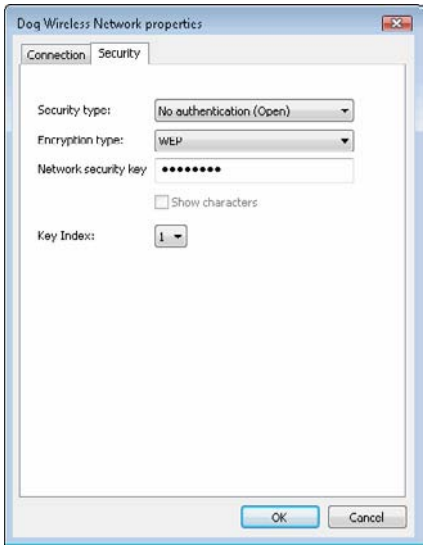


Figure 2-6: The Properties dialog box lets you make some pretty important security decisions.

Managing Preferred Networks

You also can make an available network a preferred network. This gives some networks priority over other networks in case Windows has several from which to choose. It also lets you save custom configuration settings so you don't need to make them twice for the same network. When you find yourself in an area covered by a particular wireless network you used in the past, you'll be all set to connect.

In Windows XP, there was actually a dialog box called Preferred Networks. Now it's handled from the Manage Wireless Networks page. Here's what you can do from this page:

- Add a network
- Remove a network
- View a network's properties
- Reorder a preferred network's position

Each time you connect to an available network, the network is added to the list of preferred networks. But just because a network appears under Available Networks does not mean it's automatically added to the Preferred Networks list.

Connecting with your peers

Most wireless networks are called access point, or infrastructure, networks. That means your computer connects to the Internet through a wireless router or other access point. Chances are, this is how you'll set up your wireless network.

But there's another way (isn't there always?) you can create a wireless network by connecting two or more computers together. A computer-to-computer network lets you skip wireless network routers and other access points. Instead, PCs talk directly with one another, transmitting and receiving data through their network adapters.

A computer-to-computer network is also known as a peer-to-peer or ad hoc network. One name wasn't enough, so the Lords of Geekdom bestowed it with three names.

The obvious advantage is cost: You don't pay for as much networking hardware. One computer usually serves as the gateway to your Internet connection, assuming some of the duties of a dedicated hardware router. Peer-to-peer networking also is handy for connecting a PC to a wireless print server, or networking two TiVo units.

If all you want is to wirelessly connect to PCs in your home, it may be the answer. I discuss the actual set up of these networks in Book III, Chapter 1.

Of course, the Add a network feature lets you do more than just add your own network. For example, let's say that you've been using a new wireless connection that is available to you, but your computer insists on always looking for, and connecting to, an older wireless connection. You can add this network while it's in range, and it adds it to the list of preferred wireless connections. From there, you can use the Move up and Move down buttons to rank its priority. You can also create an ad hoc connection (computer-to-computer) from the Add a network feature in this page.

Adding a preferred network

Follow these steps to add a preferred network:

1. **Click the Add button.**

   A Wireless Network Properties dialog box opens, as shown in Figure 2-7.

2. **Enter the network's name and other details.**

3. **Click OK.**

   You're done. That's all there is to adding a preferred network.

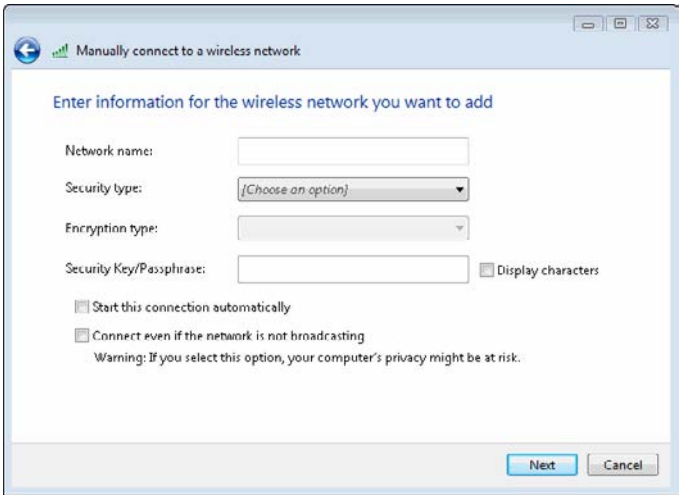


Figure 2-7: You can manually add your own preferred network from scratch.

Removing a preferred network

This is how you remove a preferred network:

1. **Select the network you want to remove.**

2. **Click the Remove button.**

Viewing a network's properties

You can view a preferred network's properties by following these steps:

1. **Select a preferred network.**
2. **Click Properties.**

   That now-familiar Wireless Network Properties dialog box appears. Make whatever changes, additions, or deletions you like to properties.
3. **Click OK to finish.**

Reordering preferred networks

Windows (XP, Vista, and 7) starts with the first network and moves down, so you'll want your most-used networks toward the top of the list. Here's how to move preferred networks on the list:

1. **Select a preferred network.**
2. **Click either Move Up or Move Down. You can also drag-and-drop a network from the list to its preferred location in Vista.**

   The preferred network is reordered in the Preferred Networks list.
3. **Repeat as many times as necessary to rearrange the order of preferred networks.**

Now you've reordered your life — or at least your list of preferred networks. It's a good start, though!

Viewing an Available Network's Signal Strength

You'll be happy to know there's a simple way to view the strength of your wireless network's signal. It doesn't provide a great deal of information, but it's enough to know whether you ought to, say, move your wireless router closer to your computers.

A good time to check your network's signal strength is when you first set it up and anytime you move your PCs or other network hardware. By moving components just a few feet from their original positions, you might find that the signal strength drops. In that case, you can scurry about, putting everything back in place.

Then, with thinking cap firmly applied, you can reconsider where you'll move your equipment.

There are other software and hardware tools for viewing your network's signal strength. I'll discuss them in a later chapter.

To view a simple but helpful visual graphic showing your network's signal strength, just follow these steps:

1. **Mouse-over the network icon in the Window notification area.**

   A pop-up menu appears.

2. **Look at your computer's connections; the strength is displayed next to your network's name.**

   A small bar graph provides a quick look at the strength of your wireless network's signal, as shown in Figure 2-8. If four or five bars are highlighted, you're enjoying strong, robust signal reception.

Figure 2-8: With four bars highlighted, this network is cranking.

If three or fewer bars are highlighted, you have a pretty weak wireless connection. Read Book IV, Chapter 3, which helps you solve wireless network problems like this one.

On the road again

Many of the topics tackled in this chapter also apply to mobile computing. When you're in an airport, for example, you hopefully see one or more wireless networks available for your use — although some or all may require payment.

When you're in an airport or other public area (or even in one of your company's offices) where you expect to return on a future trip, you can add the network to the list of preferred networks. If you need to make any special configurations for accessing a particular network, you can save them for the next time you connect to the same network.

Monitoring signal strength becomes even more important on the road. Here are some examples:

- By moving just 50 feet to a new location, your airport connection may grow stronger.
- If you're in a strange office, you may not know that the steel walls are blocking a nearby network. By moving around and checking signal strength on your laptop, you find the best spot for (wireless) networking.

Chapter 3: Creating Bridges

In This Chapter

- **Bridging two or more networks**
- **Building the bridge with hardware**
- **Doing what you wish with a bridge**

No, this isn't a chapter on civil engineering. And I'm not going to tell you how to build a bridge on the River Kwai, although I may in an upcoming sequel. (Naturally, I'll be playing William Holden's part after I shed a few pounds.) Instead, this chapter is about bridging two or more networks.

Huh? A bridge is software or hardware that connects two or more different networks together.

Huh is exactly what I said when I first learned about creating a bridge between, say, a wired Ethernet network and a wireless network. What is it? Why do I need it? Is the Big Bang overrated?

If all goes well, instead of "Huh?" your response by the end of this chapter will be "Duh!" These are times when I would want to bridge two or more networks:

- You're adding a wireless network and want it to piggyback on an existing wired Ethernet network. The wireless network has access to the same things — hardware and data — as the wired network does.
- You want to bridge two wired Ethernet networks. This occurs mostly in business environments, but it could occur in a home, too. The wired networks are physically separated and the most convenient way to connect them is by creating a bridge.
- You want to extend the range of a wireless network. By bridging two wireless access points, you can expand the signal range without laying any wires.

You can use a wireless access point as a bridge, if the access point's hardware is equipped to handle the task. Not all wireless access points can be used as a bridge; it must specifically say it can be used as one.

Bridging with Windows Vista

Windows Vista makes it easy to create a bridge between two or more networks connected to the same computer.

You need a network adapter, which serves as a communications point between your computer and the network, for each network you want to bridge. If you're bridging a wired network with a wireless network, your computer needs two adapter cards: one for the wired network and one for the wireless network.

Creating a bridge

Use the following steps to bridge two networks in Windows Vista:

1. **Click Start.**

   The Start menu appears.

2. **Click Network and Sharing Center; click Manage network connections from the Tasks list.**

   The Network Connections dialog box appears, as shown in Figure 3-1. Be sure not to click Network from the Start menu; it opens the Network page. (I know, it gets confusing!)

3. **Select the networks you want to bridge.**

   The networks you select are highlighted. You can select multiple connections by holding down the Ctrl key as you click each network.

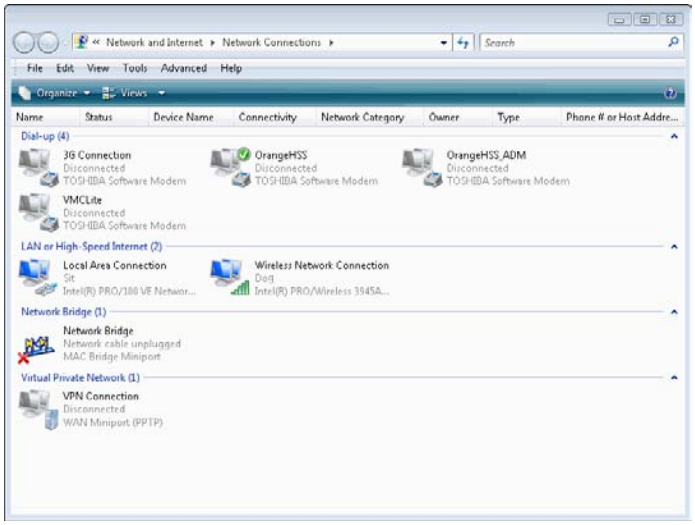


Figure 3-1: Network Connections dialog box.

4. **Right-click one of the highlighted networks and select Bridge Connections, as shown in Figure 3-2.**

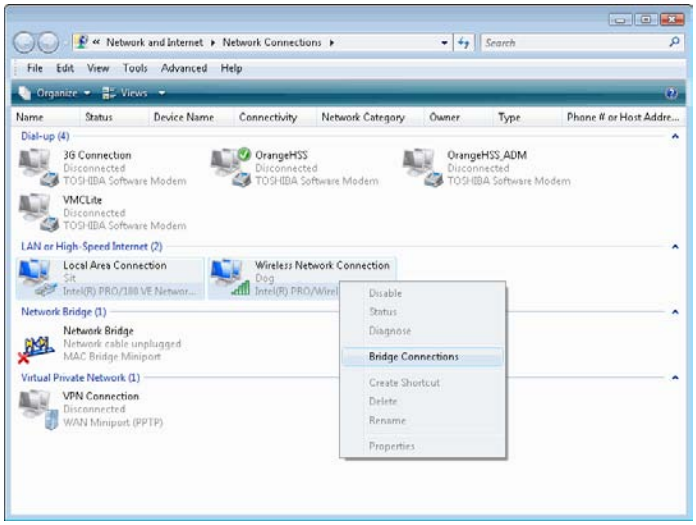


Figure 3-2: Bridging the networks you selected.

Windows Vista bridges the connections, as it indicates with the dialog box shown in Figure 3-3.

Figure 3-3: Windows bridging the connections.

The network connections are bridged, as shown in Figure 3-4.

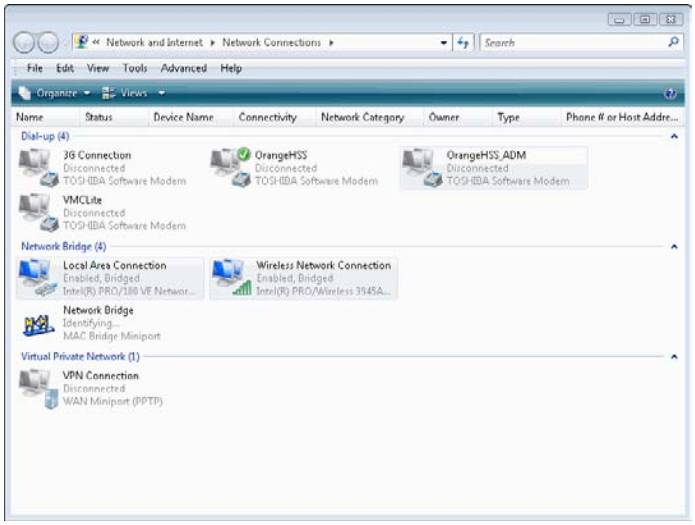


Figure 3-4: These bridges aren't burning.

Adding a network to a bridge

You can easily add a network to an existing network bridge. Just follow these steps:

1. **Click Start.**

   The Start menu appears.

2. **Click Network and Sharing Center; click Manage network connections from the Tasks list.**

   The Network Connections dialog box appears.

3. **Right-click the network you want to add to the bridge and select Add to Bridge.**

   Windows Vista adds the network to the bridge. The Status column in the Network Connections column shows Bridged once the network has been added to the bridge, and it also appears in the Network Bridge section of the page.

Removing a network from a bridge

Maybe you've added a bridge by mistake, or maybe you're ready to burn a bridge or two. Follow these steps to get rid of a network from a bridge:

1. **Click Start.**

   The Start menu appears.

2. **Click Network and Sharing Center; click Manage network connections from the Tasks list.**

   The Network Connections dialog box appears.

3. **Right-click the network you want to remove from the network and select Remove from Bridge, as shown in Figure 3-5.**

   Windows Vista removes the network from the bridge.

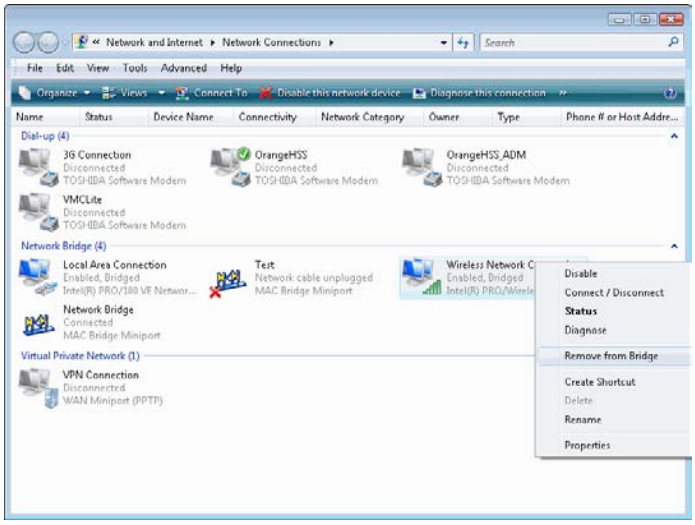


Figure 3-5: Removing a network from a bridge.

Deleting a bridge

If you need to delete a bridge, here are the steps for doing so:

1. **Click Start.**

   The Start menu appears.

2. **Click Network and Sharing Center; click Manage network connections from the Tasks list.**

   The Network Connections dialog box appears,

3. **Right-click the network bridge and select Delete, as shown in Figure 3-6.**

   Windows Vista deletes the network bridge.

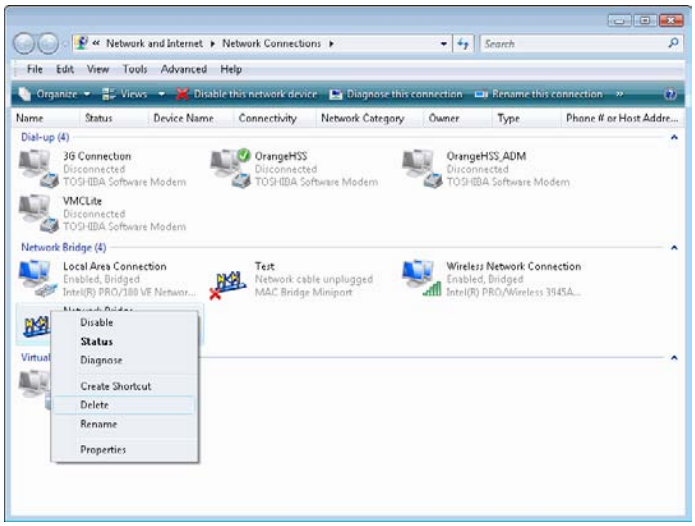


Figure 3-6: Deleting a network bridge.

Chapter 4: Configuring Printers

In This Chapter

- **Sharing a printer on your network**
- **Adding a network printer**
- **Switching the default printer**

A wireless network is about more than just sharing Internet access and your multimedia files. You also can do things like share a printer among all the computers on your wireless network. I don't need to tell you how helpful that can be these days, especially when more and more households are using multiple computers.

In this chapter, I explain how to set up printer sharing across a network, as well as how to add a new printer and change the default printer.

Learning to Share

You can add and select printers that you will use over your wireless network. For instance, you might be sharing a laser printer on your network and want to add a color inkjet printer that's connected to another computer to your network. Here's how to share a local printer on your entire network:

1. **Click Start.**

   The Start menu appears.

2. **Click Control Panel.**

   The Control Panel appears.

3. **Click Printer in the Hardware and Sound section.**

4. **Do one of the following:**

   - Right-click the printer you want to share and select Sharing.
   - Click Change sharing options and confirm the operation.

5. **Select the Share This Printer button.**

6. **Type a name for the shared printer, in the text box as shown in Figure 4-1.**

   Try to choose a name that's meaningful to you and to others who use the network. Printer is simple, but not very meaningful, especially if you have more than one printer on the network. Better examples include Upstairs Laser and Basement Color.

Figure 4-1: A meaningful name is better than a short name.

There is no longer a character limitation when naming your shared printer; however, be mindful that there are some characters that cannot be used. For example, the uses of slashes or other special characters are not allowed. If you use an *illegal* character, don't worry about it, Windows shows you the error of your ways. It is then up to you to correct it. It's important to learn from one's mistakes.

7. **Click OK.**

   An image of two people appears, which fortunately replaces the open-palm hand that appears superimposed on the printer's icon, as shown in Figure 4-2. (I think the shared icon looks like a guy in a rather boring family portrait, but that's me. I may die young from cynicism, but at least there won't be any nasty surprises ahead.)

   You're all done here. Move along, move along.

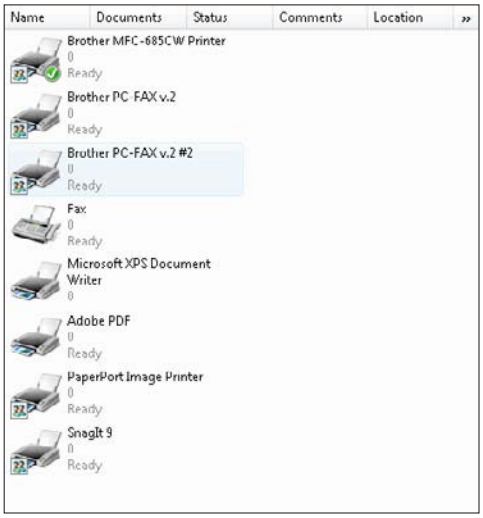


Figure 4-2: Share and share alike: The printer is ready.

Feeling Selfish and Turning Off Sharing

Just as you giveth, you can taketh. It may occasionally be a good idea to turn off your printer sharing. For example, if you know that you're running a bit low on ink or paper (and hey, those cost a lot of money these days!), you may want to limit access to your printer. If you know that you're going to be tying up the printer for a few hours and can't bear the thought of anyone encroaching on your territory (or simply sliding in a quick print job), then you may want to pick up your marbles and go home, or simply un-share your printer.

If, after setting up printer sharing on your network, you decide that you no longer want to share the printer, you can easily switch it off. Just follow these steps:

1. **Click Start**.

   The Start menu appears.

2. **Click Control Panel.**

   The Control Panel appears.

3. **Click Printer in the Hardware and Sound section.**

4. **Do one of the following:**

   - Right-click the printer you want to share and select Sharing.
   - Click Change sharing options and confirm the operation.

5. **Deselect the Share This Printer button.**
6. **Click OK.**

   The sharing symbol disappears from the printer's icon. That's it for switching off printer sharing. If you want to add a network printer, mosey on over to the next section, please.

Adding a Network Printer

Windows Vista usually installs printers for you automatically if you're connecting the printer directly to your PC; if you've been around computers since the Windows XP (or even Windows 95) days, then you likely know this. Of course, this might not be enough. There are other computers out there just waiting for you to print your prose. If you want to add the ability to use a printer that's connected to another computer on your network, rather than one connected directly to your computer, you need to follow these instructions for each printer you want to add.

Sharing must be enabled before you can add a network printer. You must enable sharing from the computer that connects to the printer you want to share.

To add a new network printer, follow these steps:

1. **Click Start.**

   The Start menu appears.
2. **Click Control Panel.**

   The Control Panel appears.
3. **Click Printer in the Hardware and Sound section.**
4. **Click Add a Printer from the menu just under the file menu.**

   The Add Printer wizard appears.
5. **Click Add a network, wireless or Bluetooth printer.**

   The list of available printers appears, as shown in Figure 4-3.
6. **Select a printer and go to Step 7; otherwise, if you cannot find the printer you want, click The Printer I Want Isn't Listed option and carry on.**
7. **Do one of the following:**
   - Select Browse for a Printer if you don't know the printer's name and network address.

- Use Select a shared printer by name, if you know the printer's name, and Add a printer using a TCP/IP address if you know the network address. Skip to Step 10.

The Browse for Printer dialog box appears.

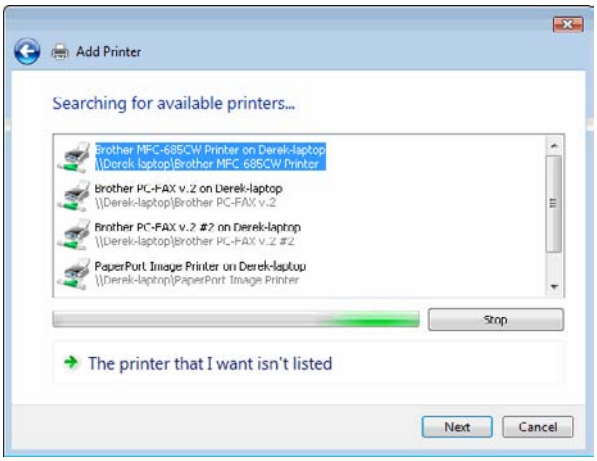


Figure 4-3: Selecting a network printer.

8. **Wait for the newly selected printer to go ahead and configure, and think of a new name for your printer.**

9. **Type the name in the dialog box shown in Figure 4-4 (or leave the default name, it's really up to you!) and then click Next.**

   The congratulatory message appears, letting you know that your network printer is now installed.

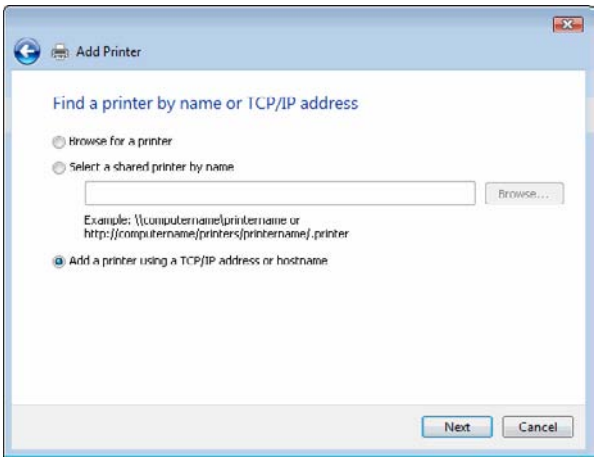


Figure 4-4: Finding the desired printer by TCP/IP address or hostname.

10. **Do one of the following:**
    - Select Finish if you want to finish any remaining work with the wizard.
    - Select Print a test page if you want to make sure your new printer really works!

You just added a network printer to your personal computing arsenal!

Changing the Default Printer

You can change the printer that Windows Vista uses as its default printer. The default printer is the one where your print jobs automatically go. Although you can always choose another printer on the network (if there is one), doing nothing means your default printer handles the job.

Usually, your default printer is your local printer (the one hooked up to your computer), but you can choose to make a network printer the default printer. Of course, you may want to look twice and make sure that you're online; otherwise it's likely that your network printers won't appear. Here's how you do it:

1. **Click Start.**

   The Start menu appears.

2. **Click Control Panel.**

   The Control Panel appears.

3. **Click Printer in the Hardware and Sound section.**

4. **Right-click the printer you want to have as your default printer.**

5. **Select Set as Default Printer.**

   A white check mark on a green circle appears on the printer icon. It indicates that the printer is now the default printer, as shown in Figure 4-5. You're done.

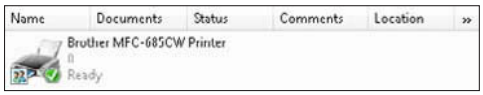


Figure 4-5: This printer's your default.

Chapter 5: Confirming Your Network Works

In This Chapter

- **Checking your signal strength**
- **Monitoring your network's activity**
- **Avoiding possible signal obstacles**
- **Handling interference**

"Eureka!" That's what you hope comes out of your mouth after setting up a wireless network. You may want to yell from the rooftops, or wherever you can find the tallest antennae that your new wireless network is running without any problems. Hold that thought: First check on your network's health. That includes viewing the signal strength as well as monitoring its activity (that is, the network traffic). After all, what's the point of having a wireless network if it is an underachiever?

Flexing Your Signal Strength

You'll be happy to know of a simple way to view the strength of your wireless network's signal. This method doesn't provide a great deal of information, but it's enough to know whether you ought to move your wireless router closer to your computers. Sometimes that's all you really need to know. Don't forget — a wireless connection is always weaker than a traditional, wired connection. In other words, you'll experience slower download speeds than a wired connection. That's why it's important to make sure your signal strength is as strong as possible, to guarantee the best possible results from your wireless network.

You should check your signal strength at two different times:

- When you first set up your network
- Anytime you move your PCs or other network hardware

Moving components just a few feet from their original positions may cause signal strength to drop. In that case you can scurry about, putting everything back in place. Then, with thinking cap firmly applied, you can reconsider

where you'll move your equipment. You also have to take in to account the realities of where you installed your network; for example, the layout of your house if this is a home network. For example, I live in a building from the early 1800s; the walls are quite thick, so if I put my laptop on my desk, next to the wall, I don't get a very good signal. If I move my laptop just a few feet behind me, the signal jumps to full strength.

Windows Vista has several built-in tools for testing your network. I discuss these in Book IV, Chapter 3.

To view a simple but helpful visual, just follow these steps:

1. **Right-click the network icon in the Windows Vista notification area.**

   A pop-up menu appears.

2. **Identify the desired network.**

   Next to the network connection is a small bar graph that provides a quick look at the strength of your wireless network's signal, as shown in Figure 5-1. If four or five bars are highlighted, you're enjoying robust signal reception. This is much easier than in past versions of Windows, where you actually had a procedure to work your way through simply to see if you had a decent connection or not.

Figure 5-1: With four bars highlighted, this network is cranking.

   If only three or fewer bars are highlighted, you have a pretty weak wireless connection. You'll want to read Book IV, Chapter 3, which helps you solve wireless network problems like this one.

3. **When you're done viewing your signal strength, move your mouse away from the pop-up menu.**

You can also find out the strength of your network using a more procedure-intensive way. The Network and Sharing Center, shown in Figure 5-2, opens and tells the strength with text. Here's how that text breaks down compared to the bar graph:

- **Excellent:** Your network is just full of energy. This is equivalent to four or five bars.

- **Good:** Your network is doing a fine job. This is equivalent to three bars.
- **Fair:** Your network is doing an OK job, but it's not living up to its potential. This is equivalent to two bars.
- **Poor:** Your network is an underachiever. You may want to start shifting things, because you likely only have one bar.

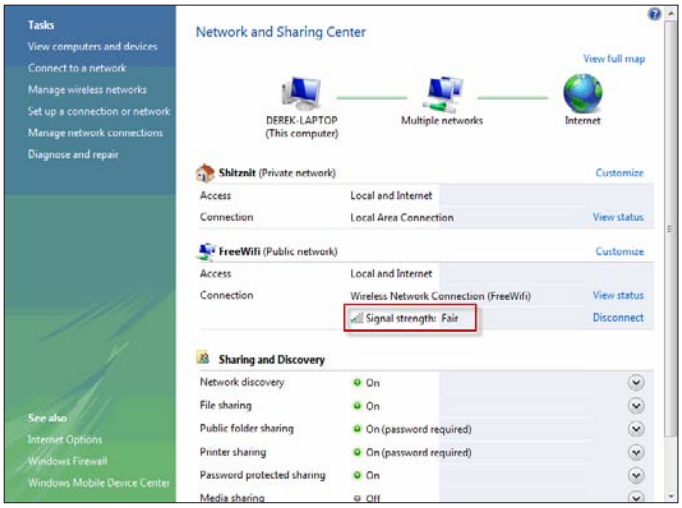


Figure 5-2: The Network and Sharing Center also shows signal strength.

A more sophisticated way of measuring signal strength is discussed a little later in this chapter. Using a third-party software program, you can get a pretty accurate read on the strength of nearby Wi-Fi access points.

Monitoring Your Network

After you've decided which wireless networks you want to connect to, some Windows Vista tools can monitor those networks. One of these tools is in the same dialog box that shows your signal strength. Another is a real-time graphical network monitor that's part of Windows Task Manager. In the following sections you learn how to use these tools. Most people use these tools simply to establish that their network is up and running properly. For example, if your network seems a bit sluggish, these tools will show you whether or not data is getting in or out.

Viewing your network's activity

In the Wireless Network Connection Status dialog box, you can see how much data is moving in and out of a PC over your wireless network.

Here's how you view it:

1. **Confirm that your wireless network is enabled.**

   If it's not, enable it. If you're also running a wired network, disable it. If you're using a laptop computer, it may be as simple as flipping a switch.

2. **Right-click the network icon in Windows Vista notification area.**

   A pop-up menu appears.

3. **Select Network and Sharing Center.**

   The Network and Sharing Center appears.

4. **Click View status on the Connection row of your wireless connection.**

   Select the General tab if it's not already selected.

5. **The Wireless Connection Status window appears.**

   In the Activity area you can monitor bytes sent and received, as shown in Figure 5-3. If there's a number below Sent but a zero is beneath Received, your wireless network may not be working properly. If there are at least three-digit numbers under both Sent and Received, your network should work.

6. **Click Close.**

   That's it for one view of network activity!

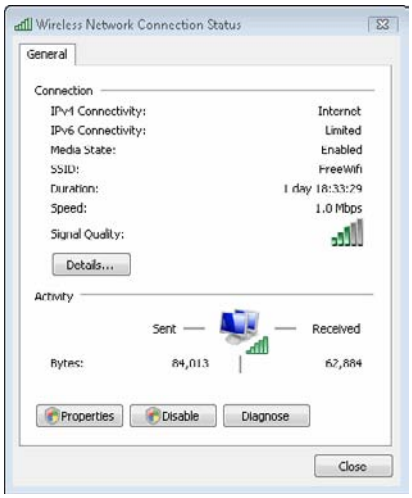


Figure 5-3: A network showing signs of activity is a healthy network.

Viewing a real-time networking graph

To monitor your wireless network, just follow these steps:

1. **Press Ctrl+Alt+Delete.**

   This is affectionately known by many as the Vulcan death grip. But in Windows Vista, instead of immediately rebooting your PC, it displays the Windows Task Manager dialog box. If that still freaks you out, you can always use Ctrl+Shift+Esc or right-click an open space on the Windows taskbar and go on to Step 2.

2. **Select Task Manager.**

   You see several tabs at the top of the dialog box. By default, you are in the Applications tab.

3. **Select the Networking tab.**

   A graph like that in Figure 5-4 shows your wireless network's activity in real time. In this example my wireless network is using about 1 percent of its capacity. The bandwidth I'm using appears consistent because I'm streaming music over the Internet.

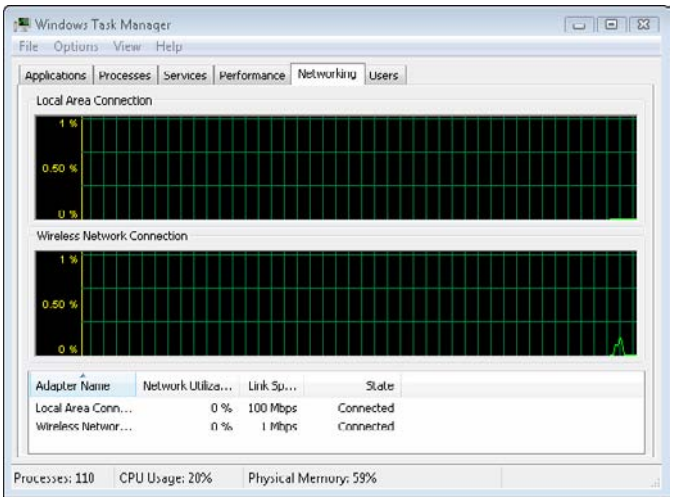


Figure 5-4: A graphics display shows your network's heartbeat, while a text area supplies other useful information.

If you also have a wired Ethernet network active, you see two graphic windows. One window shows the wired network while the other window shows the wireless network.

The bottom window shows a bunch of information about your wireless network. For starters, you see the Adapter Name, Network Utilization, Link Speed, and several columns displaying your network's throughput (how much of the network's capacity is actually being used).

4. **When you're done viewing your wireless network's activity, close the Task Manager.**

   That's it! See how easy it is to monitor your wireless network's activity?

Changing the networking information you see

When viewing the Networking screen in Windows Task Manager, you see some detailed text information below the glitzy graphical display. It's easy to change the columns displayed there:

1. **In the Windows Task Manager, choose View➪Select Columns.**

   The Select Networking Page Columns dialog box appears, as shown in Figure 5-5.

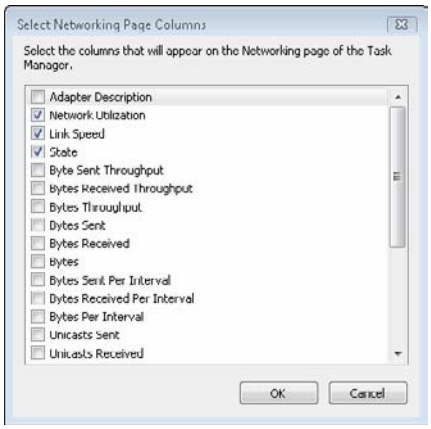


Figure 5-5: Choosing the information you'll see in the networking graph

2. **Select or deselect the boxes next to columns you want to display.**

   The default selections are usually sufficient. However, you may want to see something specific, or your network administrator may ask you to add columns while diagnosing a problem with your network. For example, you might want to see the number of bytes that were sent or received in order to see exactly how much data has been flowing across your network.

3. **Click OK.**

   Any column changes appear in the text area.

4. **If you added columns, you may need to resize the Windows Task Manager dialog box to see them. Point the mouse over the Task Manager's outline until you see a double-headed arrow and click and drag to resize.**

5. **Close the dialog box when you're done viewing the Networking screen.**

   You're done — and you're one step closer to becoming an experienced wireless network administrator.

Stumbling Upon NetStumbler

Although you can get a rough reading on your signal strength from Windows and monitor your network, another tool gives you a more detailed view: NetStumbler. It's free for home users (commercial and government users are encouraged to donate $50 per copy). This application is recommended for any users who are still working with Windows XP. At the time of printing, NetStumbler does not support Windows Vista, which makes support for Windows 7 even less likely.

Written by Marius Milner, NetStumbler runs under Windows and monitors the signal strength of nearby access points. You can select an access point and NetStumbler displays a real-time graph showing the strength.

You can use it on your desktop PC to see if it's close enough to the transmitter and if the signal is too noisy, which indicates interference or physical obstacles. Better yet, you can install the software on a laptop computer, moving around your house or business to measure signal strength in various places.

Downloading and installing NetStumbler

To download the program, follow these steps:

1. **Go to `www.netstumbler.com`.**

   The NetStumbler Web page loads.

2. **Click Downloads (located on the left side of the main menu).**

   The Downloads page appears.

3. **Click NetStumbler and save the program to your desktop or to another location you can remember.**

4. **Double-click the downloaded NetStumbler setup program.**

   The Setup dialog box displays the license agreement, once Windows Vista knows that it's fine to install the program.

5. **After reading the agreement, click I Agree.**

   The Choose Components screen appears.

6. **Select the type of installation.**

   Complete is the default type.

7. **Click Next.**

   The Choose Install Location screen appears.

8. **If the installation directory is acceptable, click Install.**

   You can click Browse to choose another directory. The program installs when you click Install.

9. **When it says Installation Complete, click Close.**

Using other apps

Windows offers some solid, yet not stellar, networking monitoring tools, as we've seen in this chapter. Some other viable alternatives are available if you want to get a second opinion.

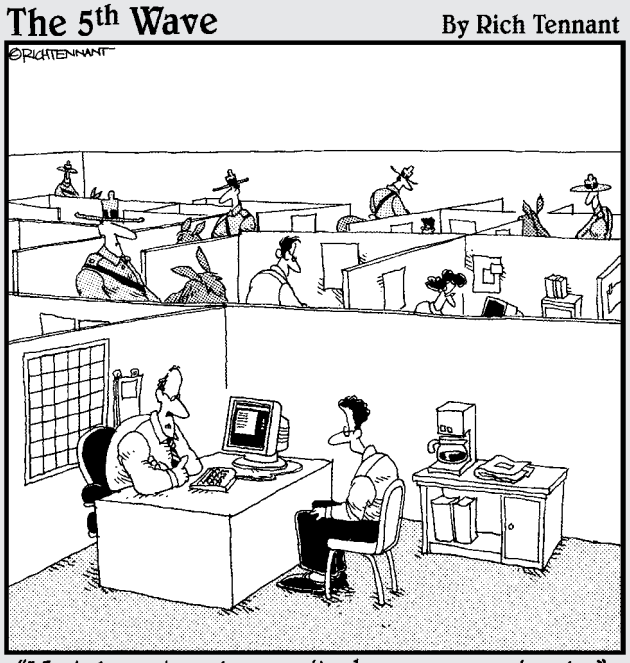
Be careful, not all third-party applications are decent quality simply because they're "not" Windows. Also, many are likely to either come at some cost and work only for a limited amount of time (either a full- or limited-access version). Be sure to check into such details before trying other applications.

For Windows Vista users, or any Windows 7 early adopters, you may want to try WirelessMon. This application, which is also available on a trial basis, works well under Windows Vista (even 64-bit). It is available at `www.passmark.com`.

The best advice I can give you is to perform a Web search for network monitoring applications and see what works best for you. Many applications offer the same or similar features for varying prices. In many cases, it's simply a question of personal preference.

Book IV

Security and Troubleshooting



"We take network security here very seriously."

Contents at a Glance

Chapter 1: Looking at Internet Threats

In This Chapter

- **Understanding the threats**
- **Discovering who the bad guys are**
- **Understanding the security tradeoffs**

The Internet is a great place; you can read about any subject you want to (and many you wish you'd never heard of). You can buy anything online and have it delivered to your door. You've got immediate access to your bank, credit cards, investments, and other financial information. Heck, you don't have to leave the house if you don't want to.

With all these new ways of doing business on the Internet come people trying to make a dishonest buck. On the Internet, some people are trying to part you from your hard-earned money without leaving their keyboard.

Not to scare you, but a whole lot of bad stuff is on the Internet. Fortunately, knowing about it goes a long way to avoiding it.

Finding Out about Bad Software

Software is the stuff you load on your computer to do work and have fun. Your word processor, Web browser, and spreadsheet are all software. Someone (or a group of people) sat down and wrote the software with the goal of trying to solve a problem you had in exchange for you buying the software.

What if those people didn't care about helping you, but thought they could write software that stole your online bank account number and password? Or what if they just thought it would be fun to delete all the files on your hard drive?

Software like this is called *malware,* which is short for malicious software. (Have you ever noticed how computer people like to make up words?) *Malware* is any software that intentionally does harm to a computer, without the computer owner's consent.

There are many different types of malware out there, and I cover these in the following sections.

Understanding viruses

In the physical world, someone gets sick, coughs on you, and the next thing you know, you're in bed for a couple of days. Computer viruses are much the same, just without the bonus of time off work.

When you happen to run a piece of infected software, the virus tries to replicate itself. Maybe it infects a few other programs on your system, maybe it hijacks your e-mail client and e-mails itself to 100 of your closest friends. Either way, the virus tries to make its way onto other machines.

Before the Internet, viruses traveled pretty slowly because you'd have to share the program over a floppy disk to move the virus around. With the advent of the Internet, viruses started incorporating network functionality.

Viruses aren't limited to programs, such as games and word processors. They can be hidden in e-mail attachments that look normal, or inside documents themselves. Newer viruses don't even need to be run; they spread by taking advantage of network services built into your machine.

One day in 1999 people started to get e-mails from friends containing a Microsoft Word document as an attachment. As soon as the document was opened, special code called a *macro* was run that made the user's e-mail software send the virus to the first 50 people in the user's address book.

This virus was very effective for several reasons:

- The e-mail came from the victim, so people were inclined to trust it.
- People weren't careful in what they opened because nothing like this had ever happened before.
- It took very little effort on the user's behalf to propagate the virus because the macros were an integrated part of the word processor.

Viruses don't necessarily do damage by themselves; what matters is the payload. If the virus' objective in life is to replicate, it's merely annoying. If the payload deletes your computer's files on April Fool's Day, that would be bad.

Getting protection from viruses

Software called *anti-virus software* runs on your computer and is constantly on the lookout for virus activity. Most anti-virus (AV) software inspect all the files on your hard drive periodically and also give a quick scan to any programs you run, at the time that you run them.

I cover AV software later in this chapter. Not only do you need it, but you need to keep it up to date. AV software works by looking for *signatures*, or patterns, of viruses. To update your AV software means to get the latest set of signatures. Fortunately for you, any decent AV package will automate this.

The second way to keep virus-free is to keep on top of your operating system patches. In late 2008 and early 2009, a virus called Conficker was running around the Internet. Conficker spread by many different means, but one of the most effective was by exploiting a problem with Windows that had been patched several months prior. Because most people didn't install the latest operating system updates, they were vulnerable. We look at patching in the next chapter.

Finally, the first line of defense against virus infection is to use your head. If you receive a random e-mail with an attachment, don't open the attachment. Only get software from reputable sources, or friends. And use your anti-virus software to scan things after you download them.

Spyware and adware

Spyware and adware are two types of malware that hide in the background and try to make money for the creator. Spyware tracks the Web sites you go to and uses that data to make money. The author might be interested in the data themselves, or they might be able to sell the information to someone who is.

Adware is software that displays advertising inside it. This initially wasn't bad — some instant messaging services originally displayed small ads to keep their service running. As usual, though, people started writing code that would force itself upon the machine and change the ads that a user saw. For example, an ad for jewelry on a Web site might be replaced with an ad for something else, with the owner of the adware getting a cut if you buy anything.

This last scenario might seem like it's not a problem; but even so, adware takes up resources on your computer and makes it slower. Adware also cheats Internet businesses out of their money.

Other types of spyware, called *keyloggers*, take your keystrokes and send them to the creator. This includes anything you typed into your online banking site.

The lines between adware and spyware have blurred to the point where it's all generally called spyware now. Whatever it's called, you don't want it on your computer.

Most of the lesser forms of spyware come from toolbars that you randomly happen across on your Internet travels. Anything offering free smileys, "free

screensavers, or something that enhances your Web browsing experience with a free deal finder toolbar probably contains some hidden nastiness. The program may work as advertised, but it will probably leave spyware that will be around long after you get bored with the software you downloaded.

These spyware packages are often distributed through a technology called ActiveX that is only supported by Microsoft Internet Explorer. There are few ActiveX components that are worth using, and a good part of the rest is spyware.

Spyware is often found in illegal downloads, especially software that purports to crack the copy protection on various legitimate pieces of software. Say what you will about the legal aspects of copyright protection, but the level of malware out there is atrocious.

Somewhat tied to the illegal downloads of software is downloads of illegal movies. The movies themselves don't contain anything bad because they're just data. However, trying to view the movie prompts you to download some software to properly decode it in the form of a piece of software called a *codec*. Guess what's in that software? Figure 1-1 shows a user being prompted to download a new codec in order to watch a copy of a new movie that was downloaded over the Internet.

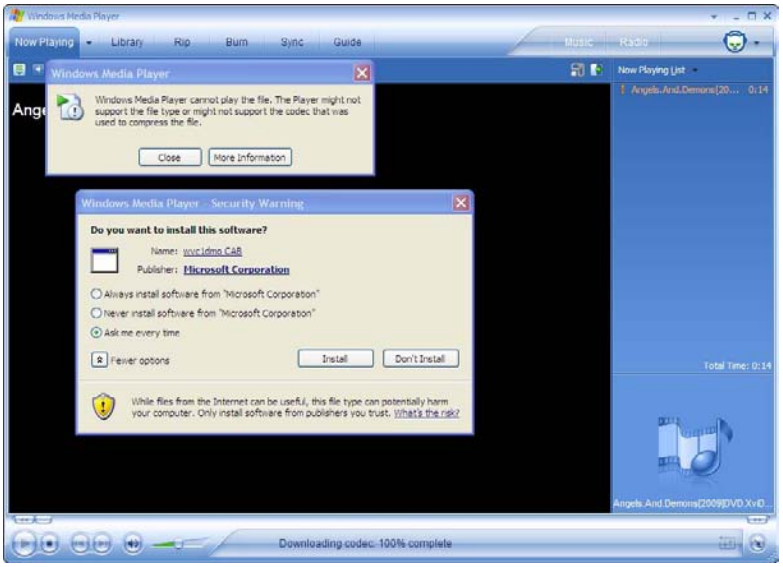


Figure 1-1: A prompt to download a codec.

Does the codec contain malware? To find out, you should enter some of the details into your favorite search engine and see what other people have to say. Or, just stay away from media files like that.

Be selective about what you download and run. No matter what the ad says, you can't download a current version of Microsoft Office for only $4. Even if it does contain an illegal version of Office, it's bound to contain a bunch of nasty malware that you don't want.

Try to find an anti-virus package that includes anti-spyware functionality, too. This software tries to block the installation of the spyware and also prevents spyware from calling home to transmit the sensitive data that was stolen.

Don't download any extensions to Internet Explorer. In fact, don't run Internet Explorer at all. Firefox is a much faster browser and does not suffer from as many attacks as Internet Explorer. Whichever browser you choose, make sure you're up to date.

Be careful when installing software that has been suggested from a recent download. When you are prompted to download anything, take a moment to research what is being offered to make sure it's not malware.

Zombies and botnets

The final stop in our whirlwind tour of bad software brings us to zombies and botnets. In the movies, zombies are dead people that have been reanimated and spend their time looking for tasty human brains to eat. They're especially fond of groups of people who decided to split up so that they could find a way out of the abandoned building faster. I've never understood why people do that.

Anyway, a zombie computer is one that has been infected with some sort of malware that allows it to be controlled remotely. The infection is such that the owner of the computer doesn't know what's going on because the computer operates normally (but maybe slower).

Take a few thousand (or a few hundred thousand) of these zombified computers and you have yourself a *botnet*. The people who run these botnets make their zombie computers send e-mail spam, try to defraud advertisers, and even try to take down major Web sites. They may do this for their own uses or rent out their botnet to people who are in need of such services.

Needless to say, you don't want your computer to be a zombie! There's no upside, and you don't want to be giving out system resources for sending spam and taking down Web sites.

Zombie software gets on your computer the same way that other malware gets there, such as through strange e-mail attachments or in infected files taken from unscrupulous Web sites.

Avoiding Bad People

The last section talked about bad software. Bad people made that software, but there's another class of bad guys that are out to scam you directly.

Most of these schemes aren't new; they're just some old classics that have been adapted for the Internet. People have been writing bad checks for decades: the Internet just allows them to expand their reach.

Spam

If you've had an e-mail address for more than 10 minutes, then you've seen some spam. Spam is an *unsolicited commercial e-mail*, which is a fancy way of saying that someone you don't know sent you an e-mail trying to sell you something.

The nature of e-mail means that it costs about the same to send out a million e-mails as it does a handful. There are no stamps to buy, no envelopes to stuff, and no address labels to print. A single computer can generate thousands of spam e-mails per hour, and if you use the services of a botnet, you can blast out a few million e-mails in no time at all.

Spam is sometimes hard to differentiate from regular commercial e-mail. Sometimes you get added to a mailing list from a company that you dealt with, and you start getting a monthly newsletter. As inconvenient as it is, spam is a much bigger problem.

The idea behind spamming is that the spammer sends out an offer for a product. The types of products usually associated with spam are

- Pharmaceuticals, especially male performance enhancing pills
- Knockoff watches or clothing
- Illegal software
- Financial products such as loans
- University degrees

All good stuff, right?

Spam is bad for several reasons, including

- The sheer volume of spam makes your ISP do extra work to process the e-mail, and you do more work to find the e-mails you're really looking for. This makes e-mail less efficient as a communications medium.
- The way that spammers send the e-mails out is often destructive to mail servers.

- The products being sold are usually a scam, illegal, or just plain low quality.

As tempting as it may be to be able to lose weight with only a small pill being sold at a ridiculously low rate, stay away.

Also be careful about how you give out your e-mail address. Posting to public forms sometimes exposes your address, which spammers harvest for their lists. Free Web-based e-mail providers are plentiful; it helps to have a separate account for posting to public forums.

Spam is often the vehicle for phishing attacks, which I look at next.

Phishing

Ever received an e-mail from your bank telling you that it was important that you go to their Web site and fill in some missing personal information? Ever received the same information from a different bank, one that you don't deal with?

These e-mails were probably part of a *phishing* scam. Phishing is a play on fishing, as in "fishing for suckers who will give me their bank information" (and another made up word!) With this personal information the bad guy can get into your bank account or can get credit cards in your name (also called *identity theft*).

Here's a step-by-step look at a scam:

1. Bad guy sets up a Web page that looks a lot like a particular bank's Web site, with a form asking for your credit card number, social security number, mother's maiden name, bank PIN, and anything else he can think of.
2. The bad guy sends out millions of e-mails that look official and that ask you to visit your bank's Web page using the link in the e-mail.
3. You just happen to use that bank, so you click on the link and fill in the form.
4. The bad guy cleans out your bank account from the safety of an Internet café in a foreign land.

That e-mail from the bank may look authentic, but here's what you might not know:

- Making an e-mail look like it came from whoever you want, including your bank, is easy.
- Making an e-mail look official and important is easy.

- Making the link shown on the screen take you to a different site is easy.
- Scammers can use many ways to trick people into thinking they're on their bank's Web site, when in fact they're on the bad guy's site.

Figure 1-2 is an e-mail that looks like it came from an auction site I use. It looks a lot like other e-mails that come from the site, but if you look where my mouse is hovering on the link, and the link that shows up in the status bar, they're different!

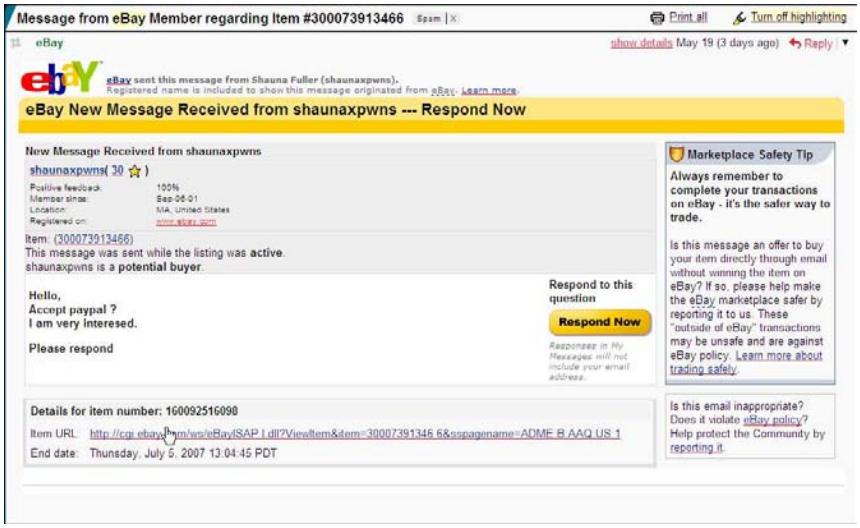


Figure 1-2: An e-mail from an online auction site. Or is it?

What's happening here is that the phisher is trying to trick me into going to his site, where he'll try to get me to log in using my real username and password, at which point he can do bad stuff.

That hover trick is not always reliable, though. The only way to be certain is to copy and paste the URL that shows on the screen instead of clicking.

If you are presented with such an e-mail, it pays to view it with some skepticism. Keep the following in mind:

- Some sites that are especially prone to phishing attacks will include your username in the subject or e-mail to show you it's not a phishing scheme. If you don't see this, beware.
- Banks will not request personal information over an e-mail or on a random Internet page. When in doubt, call your bank and ask.

- Most Web sites that deal with sensitive information post a policy on their Web page describing whether or not they do send such e-mails out and what sort of protections they use.

When in doubt, pick up the phone or just delete the e-mail.

If you use the Firefox Web browser, or Internet Explorer version 7 or later, it adds some additional phishing protection. Clicking on the link in the previous figure brings you to Figure 1-3.

Figure 1-3: Trying to view a phishing site.

This screen is presented by your Web browser, and it indicates that the site in question is known to be a phishing site. It's not perfect, but it's an additional layer of protection.

Be very careful about what private information you give over the Internet, no matter what format. Scammers are getting cleverer. Identity theft is serious and can cause you a lot of trouble.

Rebills

The rebill, or the *negative option billing* scam, is usually legal but very shady.

The essence of the scam is that you sign up for a free trial of some product and only have to pay a couple of dollars shipping. What you missed in the reams of fine print is that after your trial expires, you'll be charged a hefty sum every month to continue on the program. It's usually a couple of months before you know and can get off the program.

This type of deal has been around for a while, especially for music clubs. The scammy version is different, though:

- The terms of the agreement are not made clear. You might have to go to another page or scroll down to see the catch.

- Often the trial starts from the day you sign up, not from when you get the product. People find that their credit card has been billed for the first month before they've even received the trial item.
- The product itself is poor, either by not living up to the medical claims made or, in the case of make-money-fast type offers, is simply public domain information.
- The company's contact information is not made clear in case you want to complain or cancel your subscription.
- It takes several hours of dialing to get through to customer service to get off the product.

These types of scams are all over, from advertising on popular Web sites to spam. Often you see the product on a personal Web site from a person purporting to have used the product to lose weight or make thousands of dollars. This person probably doesn't exist; the seller has just made them up to try and get you to sign up for the trial.

Beware of anything offering a free trial that requires a shipping charge, and always check the fine print. Check your credit card balance online periodically (having a separate credit card for Internet purchases is also helpful), and call your credit card company at the first sign of abuse.

Another version of this involves your cell phone. You are given a free ring tone, or told that you need to provide your cell phone number to get the results of a test you just did. After you provide your cell phone number you are quietly signed up for a service on your cell phone that bills you every month.

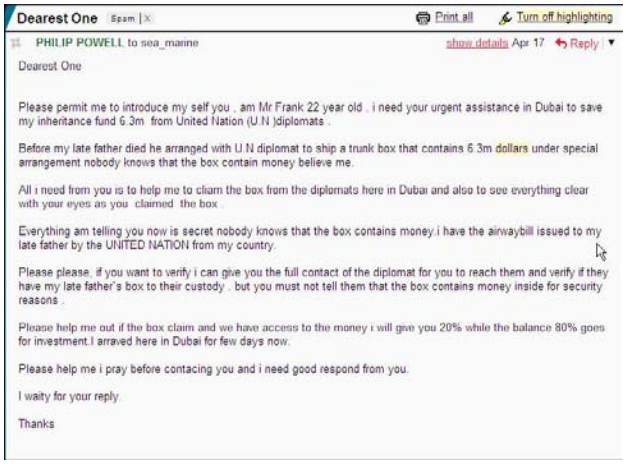
You won the lottery!

Ever got an e-mail like one of the following?

- Congratulations! You won the Internet lottery!
- You have just inherited $1 million from a long-lost relative.
- I need you to help me get $5 million out of my country. You can have 40 percent for your efforts.

These are all scams.

The way these go is that you chat back and forth with the person, and at some point, they come up with a story for needing a few dollars, such as $50 to process some paperwork. If you pay that, more charges keep piling up for various things until you realize you've been had. This is called the *advance fee scam*. See Figure 1-4 for an example.


Dearest One Spam | x Print all Turn off highlighting

PHILIP POWELL to sea_marine show details Apr 17 Reply

Dearest One

Please permit me to introduce my self you , am Mr Frank 22 year old . i need your urgent assistance in Dubai to save my inheritance fund 6.3m from United Nation (U.N)diplomats .

Before my late father died he arranged with U.N diplomat to ship a trunk box that contains 6.3m dollars under special arrangement nobody knows that the box contain money believe me.

All i need from you is to help me to claim the box from the diplomats here in Dubai and also to see everything clear with your eyes as you claimed the box .

Everything am telling you now is secret nobody knows that the box contains money.i have the airwaybill issued to my late father by the UNITED NATION from my country.

Please please, if you want to verify i can give you the full contact of the diplomat for you to reach them and verify if they have my late father's box to their custody . but you must not tell them that the box contains money inside for security reasons .

Please help me out if the box claim and we have access to the money i will give you 20% while the balance 80% goes for investment.I arraved here in Dubai for few days now.

Please help me i pray before contacing you and i need good respond from you.

I waity for your reply.

Thanks

Figure 1-4: The advance fee scam.

I really don't think that Mr. Frank has the $6.3 million dollars. Just ignore e-mails like this.

These types of scams have been around for years, but the Internet has made it easier for scammers to find their victims. At one point many of the scammers were based out of Nigeria, so you will find this called the *Nigerian scam* or the *419 scam* (419 is the section of the Nigerian criminal code dealing with such fraud). An Internet search for these terms uncovers a variety of different ruses used for the scam, along with some hilarious stories of people getting the scammers to do all sorts of silly things.

Looking at the amount of spam I get involving this scam, I can only assume that people are still falling for it. Indeed, I have seen a few stories in the news. One person was taken for $150,000, which gives you some idea of how bad it can get.

Check washing and the overpayment scam

Check washing is a process where a check that has been written on has the payee and amount removed (washed off), and a new value and payee put on. This was around before the Internet, but again, the Internet has made it easier to find victims.

Intercepting the check is surprisingly easy, so the scammers have a wide variety of potentially blank checks to choose from.

This scam generally works two ways. The first is that you are offered a job to process paperwork at home, which ends up being to cash some company

checks. You send the money to your "employer," sometimes minus a small commission to you.

What has happened is that a legitimate check has been intercepted and washed, and your name has been put on it with a new dollar amount. You deposit the check, your bank advances you the funds, and then you send the money away. Usually you are told to use Western Union, which is an untraceable system.

Eventually the bank finds out when the check bounces and takes the money back from you. But you've already sent the money away!

The second way this happens is that you offer something for sale online, and someone buys it from you. When it comes time to pay they try to give you a check for more than the sale price with some excuse for why. You are asked to send the difference back to them.

Of course, the check bounces, and you're out whatever you sold and the cash.

To avoid this scam:

- ✦ Beware of any deal where you get a check and have to send money back.
- ✦ Never accept a check in response to an online dealing unless you know the person. Look into trusted systems, such as PayPal.
- ✦ Never send any payment to someone you don't know by an untraceable method, such as Western Union.
- ✦ Keep your checkbook safe and watch your bank account for the checks you issue. This will help prevent one of your checks from being used for the scam.
- ✦ Remember that if it sounds too good to be true, it probably is.

Credit card stealing

Compared to all the other types of scams, this one is downright uninspiring:

1. You buy something online using your credit card.
2. The Web site you bought it from is hacked into and your credit card number is stolen.
3. Your credit card number is used to buy stuff, sticking you with the bill.

Fortunately, most countries have laws dealing with credit cards such that if you notice the fraudulent transaction before your bill is due, you can dispute the charge and not have to pay it when it's shown to be fraudulent. Still, it's an inconvenience to have this happen.

One sign to look for when paying over the Internet is that you are using a secure connection. A secure connection means that anyone watching your traffic will not be able to see the information inside because it is encrypted. Figure 1-5 shows an Internet Explorer window that is using a secure connection.

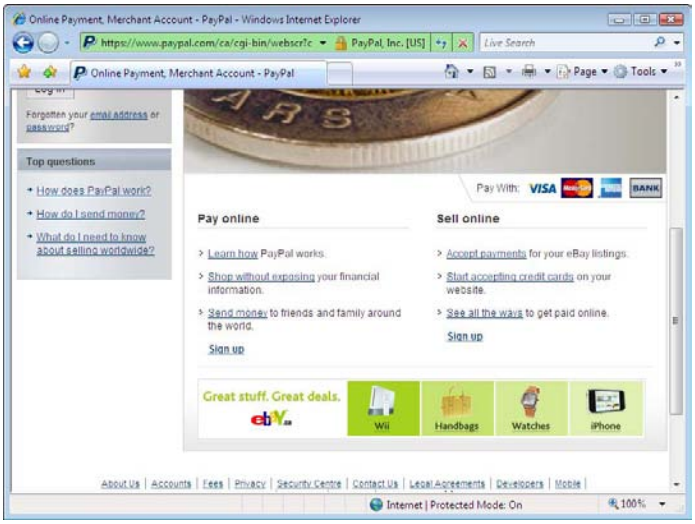


Figure 1-5: A secure connection.

In the address, note that the URL begins with https instead of http. This indicates the connection is encrypted. Also note the picture of the lock. This indicates that the site you are browsing is the same one that was certified to use the security. Some older Web browsers place the lock in the bottom status bar instead of in the URL.

The certificate itself is no protection against someone coming in after the fact and stealing the data. This is an unfortunate part of the Internet and security. The credit card companies are still rolling out their security standards across their merchants, which will enforce rules protecting your information.

It is a good idea to keep a credit card for use only on the Internet, and to keep the limit fairly low. This makes it easier to spot fraudulent transactions and limits your liability should problems arise.

It's Not All Doom and Gloom

This chapter has shined a spotlight on some of the darker parts of the Internet. I didn't lead off with it to scare you. In the next couple of chapters, I cover tools you can use to protect yourself.

Tools by themselves won't help you, though. You need to be smart before you open that attachment, or get your credit card out. The bad guys prey on greedy people. Don't be one of them.

You can find a lot of good stuff on the Internet, and the bad guys shouldn't keep you from it.

Chapter 2: Using A Safety Net

In This Chapter

- **Understanding why your network should stay private**
- **Using your router's security features**
- **Protecting your wireless network**

When networks were all wired, you'd know exactly who was on your network because they'd be connected by a cable to your switch. Unless someone snuck a 200 foot cable out your window, you could rest pretty soundly knowing that you and your family were the only users on the network.

With wireless, your neighbor's teenage son (never did trust the kid. . .) could be sneaking into your files, or that strange, white unmarked van across the street could be spying on you. Maybe I'm just getting paranoid. Or am I?

Knowing Your Network

If you want to defend your network, then you need to understand how it's put together. Each component has different properties and is defended differently. You can look at your network as if it were made up of two parts:

- The Internet connection
- All the stuff on the inside, like your computers

The next sections cover each of these in turn.

Protecting the Internet connection

What happens on your Internet connection is your responsibility. If someone on your network does something bad, willingly or unwillingly, then the Internet service provider has your name on their billing records and will talk to you first. If cops get involved, you get the first interview.

Problems are not unheard of. Consider the following scenarios:

- ISPs sometimes implement a cap on the amount of data that can be transferred on a given connection as part of the monthly rate, after which they charge a fee based on usage. Most people will never touch this cap, but if someone were to use your connection to download movies all month, you could blow past this limit without knowing.
- You've been following the advice in this book about keeping your computer safe, but the person borrowing your Internet connection hasn't. They get infected, their computer becomes a zombie, and the next thing you know you can't send e-mail because your provider has turned off your e-mail because of spam complaints.
- A scammer finds that they can use your Internet connection if they park their car across the street. They use it to commit fraud, and the police get involved. The ISP traces the messages back to your address.

Although the scenarios may seem far-fetched, they have happened.

I'm not saying you can't share your Internet connection with your neighbor, or that you should rigorously inspect everyone's computer that enters your door. You can still lock down your network and share the password so that just your neighbor gets on while keeping the bad guys out. If the neighbors aren't that computer savvy, maybe you could lend them this book (or better yet, get them their own copy!).

War driving

War driving is a play on a pre-Internet activity called War Dialing. In War Dialing, someone dials every phone number in a particular range of telephone numbers, looking for computers that answer instead of humans. This technique used to be very effective at finding unprotected computers because the systems administrators used to use dial-in modems as a way to remotely manage their systems and were often not very thorough in their security practices.

If you've ever seen the movie *War Games* you'll recognize this. If you haven't, you should look it up. Despite being over 25 years old it's still a great flick!

War driving involves driving around a city with a computer and a wireless card, looking for open (or easily crackable) wireless networks. It's been refined to the point where you can tie in a GPS unit and end up with a map of all the networks, with the exploitable ones highlighted.

The bad guys will use war driving to find open access points they can use and abuse. Make sure you're not on their list!

Hackers versus crackers

Throughout this chapter and others, I might use the term hackers and crackers. You've probably heard the term hacker before and have heard it being used in the context of a bad guy trying to break into your computer.

The word hacker has a long and distinguished history, however. Hackers were the people that advanced computer science not by exploiting weaknesses and doing harm, but by using their intelligence to pull off feats of skill (called hacks). Hackers would build computers out of spare parts or come up with brilliant ways around limitations.

As other intelligent people used their skills for evil, the media applied the name of hacker to them. These are the bad guys: the people writing software to steal information, or coming up with ways to game systems to their advantage. It's insulting to the hacker community to associate these bad people with them, so we use the term cracker, much as in a safe cracker.

In this book, I don't have the need to refer to people in the hacker sense, so I'll just use cracker, attacker, or, even better, bad guy.

There's a third class of people that I'll call researchers. These people try to find weaknesses in systems in the name of improving them. They're trying to break the security systems before the crackers do, so that the systems can be fixed. These guys are on your side.

Unfortunately, the public nature of research means that the crackers eventually learn about the problems and use them to their advantage.

The stuff on the inside

Your network may include your computers, video game consoles, and maybe a file sharing device or two. If someone can connect to your wireless network, then they can connect to your computers and file storage servers.

More sophisticated attackers can pretend to be your gateway and force all your Internet use through their computer using a process called *spoofing*. Anything you look at on your computer is passed through the attacker's computer. Even though your bank uses encryption when you view their Web page, you still have to be careful to make sure that the attacker isn't feeding you bad information.

Your computers have files on them that you'd probably rather keep private. You may not have anything to hide, but you still don't want to share all your files with people. Tax returns? Letters to the lawyer? If you wouldn't stick it to your front door, then it's worth spending some time to protect.

People from the Internet

So far I've been talking about people trying to get into your home network over the wireless connection. There are also people trying to get in from the Internet. Fortunately your firewall blocks any connections from the outside coming in, unless you deliberately turn that feature off. Don't do that!

Most of the attackers coming from the Internet are computer programs that are scanning your service provider's network, looking for vulnerable hosts. Your firewall protects you against these scans because it only allows connections that your computers make out to the Internet and not new connections from the Internet to the inside of your network.

All that said, if you run a program that's got a virus in it, all bets are off. We talk about getting anti-virus protection in the next chapter.

Choosing Wireless Security

Wireless networking, by nature, involves throwing your data over the airwaves and hoping only the recipient is the one listening. As more people used wireless, more important information was carried over the air. As more important information was sent, the incentive for people to try and listen to it increased. As people tried to listen, the engineers in charge of the wireless standards tried to keep up.

Here's a summary of the wireless security protocols available to you.

WEP

When 802.11 was introduced by the Institute of Electrical and Electronics Engineers (IEEE) in 1997, the standard called for vendors to optionally provide security through *Wired Equivalent Privacy* (WEP). WEP encrypted the data that was sent over the radio so that people listening in couldn't read it without the key.

WEP had some problems from the start. The key used to decrypt the data was static, meaning it never changed. To get on a WEP-protected network, everybody had to share the same key. As you can imagine, it became easy to figure out the key because it often got posted to the wall so people wouldn't forget it.

Secondly, the United States had some rather peculiar regulations at the time dealing with the export of encryption capable products to other countries. Back in 1997, encryption fell under the International Traffic in Arms Regulations (ITAR), which regulated the export of weapons out of the country. You couldn't export missiles, nuclear weapons, night vision goggles, and any encryption the government couldn't break.

As such, WEP went out the door with pretty weak encryption, even for 1997. But it was all we had. Some people used it, some people didn't.

Fast-forward a few years, and people are starting to look closely at the security of WEP. The U.S. government relaxed their position on encryption, and WEP was upgraded to something less embarrassing. However, some researchers found that by listening to enough traffic you could deduce the shared key. As people poked deeper into WEP, they found that even less traffic was needed, and you could even cause the access point to generate it if the clients weren't generating traffic. The time to crack a WEP key is now down to a minute, even with the stronger encryption in use.

Yes, you heard me right. Someone can listen to a WEP-protected network and have the key before you even notice they're there. With the right antenna, they could be farther away.

This isn't going to do. Something better is needed.

WPA

The IEEE started work on the 802.11i standard, which dealt with wireless security. As usual, trying to get a bunch of engineers to agree on something takes its time, so the Wi-Fi Alliance took some of the in-progress work from 802.11i and came up with the *Wi-Fi Protected Access* standard (WPA).

WPA solves the key problems that were the downfall of WPA with a protocol called the *Temporal Key Integrity Protocol* (TKIP). TKIP's job is to rotate keys constantly so that the problems WEP had won't happen again.

WPA had a major constraint in that it was intended to run on older access points by means of a firmware upgrade. This was because WEP was so broken that the industry wanted to protect access points in the field. Therefore WPA uses some of the same encryption techniques as WEP, just implemented in a better fashion.

WPA also introduced the concepts of a pre-shared key mode (PSK) and an enterprise mode. PSK mode requires a key that's known to all participants in the wireless network, just like WEP. Enterprise mode allows you to use your enterprise login credentials to log in to the wireless network, eliminating the need for a shared key.

Even though enterprise mode is better security, it requires servers and services that people at home just don't have. The acronyms and standard names required to implement this mode are astounding. So, you'll always want to use PSK mode if you're ever given the option.

WPA was a significant improvement upon WEP. Eventually, researchers found ways to mess with WPA networks. WPA is not as completely broken as WEP, but it is possible to inject packets into a WPA-protected network. With this ability, an attacker could still redirect the entire network's traffic through a computer of his choosing.

WPA2

Third time's the charm, right?

The IEEE finally finished 802.11i, and the Wi-Fi Alliance called it WPA2. The Alliance also made implementation of WPA2 a mandatory part of Wi-Fi compatibility testing. Without WPA2, vendors couldn't put the Wi-Fi logo on the box.

WPA2 got rid of TKIP and went with the *Advanced Encryption Standard*, which is the same that the U.S. government uses for protecting its secrets. The earlier WPA standard was also revised to allow AES to be used instead of TKIP.

To date, there are no direct attacks against WPA2. That hasn't stopped people from trying, though!

Even though the bad guys can't exploit weaknesses in WPA2, they can try to guess your password. So pick a good one!

Deciding what to choose

If you're setting up a wireless network, you want to be using WPA2. Most access points have a mode that allows both WPA2 and WPA to be used. If you have older clients that only support WPA, then this mode will work.

It's easy enough for me to say "use WPA2" when you're setting up your own network, but what about when you use other people's networks?

Hotel networks generally have no encryption or security at all. Anyone can connect, anyone can read the packets in the air, usually called *open mode* or an *open network*. Access to the network is usually protected by a *captive portal*, which intercepts you when you first start using the Internet, and only lets you through after you've registered.

Captive portals provide no protection for you; they're there only for the convenience (and usually, profit margin) of the hotel.

Connecting to these unprotected networks is okay as long as you've protected your computer (see Chapter 3) and realize that anything you send over the network is visible by anyone. Browsing the Web is fine. Logging into your secure bank account is secure as long as you validate the site's certificate like I showed in Chapter 1.

WEP should be considered in the same boat as an open network.

Exploring Network Security Features

As technology advances, the CPUs going into routers get faster and faster. The processing power required for the basic routing and firewalling is negligible, so there's ever increasing room left for more features.

You'd think that manufacturers would cut back and put the bare minimum CPU in, but the way the industry works is that older chips cost more to buy, so it ends up being cheaper to put more oomph inside the box.

Most manufacturers have several features in common, though some may implement them slightly differently. Some features are handy, some not so much, and some will completely expose your computer to Internet attackers. In the following sections, I identify when and where you'd want to use them.

Understanding the SSID and password

The network name (SSID), password, and security protocol (such as WPA2) are your first line of defense against attackers. You've seen earlier how WPA2 is currently the best protocol to use, and you probably gathered that the password is important.

The only known way to break into a WPA2 PSK (pre-shared key) network is to guess the password. The crackers know this and have come up with ways to guess passwords at incredible speeds.

The WPA/WPA2 key that encrypts all the data in the air is derived from both the password and the SSID. One of the optimizations the crackers use is to pre-compute these keys by using a list of popular SSIDs and popular passwords.

If you make sure that your SSID is unique, such as the name of your street, your pet's name, or something else unique, perhaps followed by a number, you'll be sure to stay off this list.

The most important thing to do is to choose a complex password. If you're using Wi-Fi protected setup (WPS), you don't even have to remember it!

Figure 2-1 shows where you configure the SSID, protocol, and password for the network. Here the SSID is "walberghome," the password is "W1r3l3ssB00k," and the network uses WPA2.

Search the Internet for "top 1000 ssids" and you should find, surprisingly enough, a list of 1000 of the most common SSIDs out there.

With a unique SSID and an unguessable password, the crackers will have to find another way in!

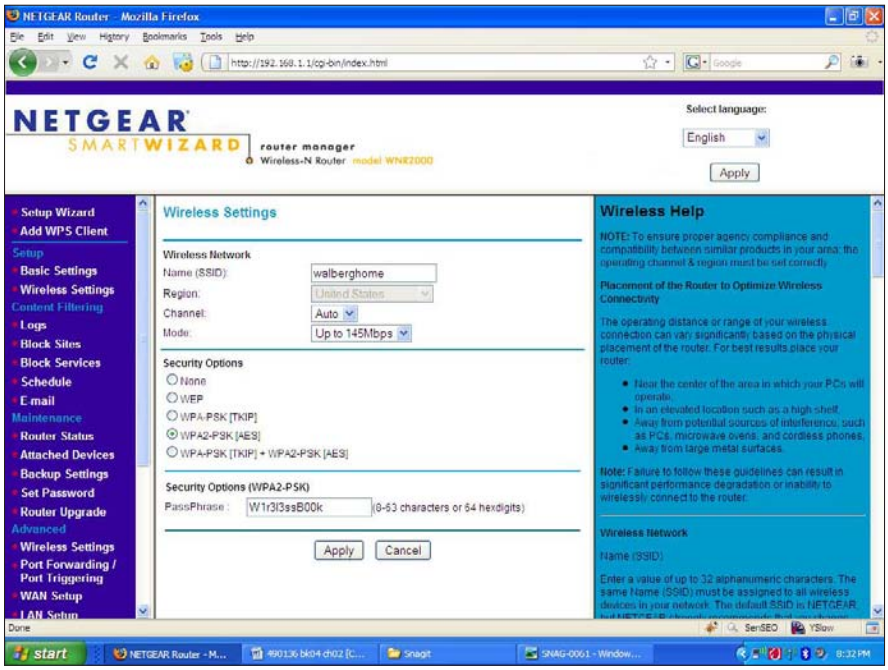


Figure 2-1: Configuring the SSID, password, and protocol.

SSIDs and passwords are case sensitive. Use a lowercase SSID, and work in some uppercase letters and some numbers into your password.

Using advanced wireless settings

When wireless first came out and the low-strength version of WEP was all that was available, people came up with a few methods to increase the security of their network.

Security is always a tradeoff between protection and convenience. As you add more security measures, it becomes more complex to use whatever it is you're protecting.

And so, too, it is with wireless. Two ideas that people came up with were

- Hide the existence of the SSID
- Find the hardware addresses of the machines you want to connect and only let those in

With today's technology, both of these are poor protections against attack. Not only do they make your wireless network terribly inconvenient for you to use, but they don't improve your security.

On the surface, hiding your SSID makes some sense. Your wireless access point broadcasts its network name periodically so that your computer can know when it should connect. Turning off this feature means that someone driving by won't know the access point is there and won't try to break into it.

The problem with this is that it is still possible to deduce the presence of a wireless network because of the wireless traffic. After that, there are various ways to figure out the SSID.

The second idea involves making a list of the hardware addresses of the wireless cards and telling the router to only allow those addresses to use the network. Figure 2-2 shows the properties of a wireless card. The hardware address is the same as the physical address.

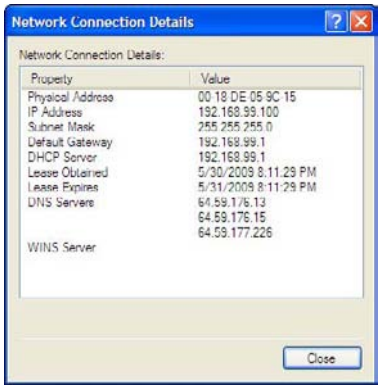


Figure 2-2: Showing the hardware address of a wireless NIC.

Not only is it a pain to administer, spoofing a MAC address is trivial. *Spoofing* in this example means that the attacker is using your MAC address instead of his; your access point is none the wiser.

Browse to Wireless Settings to see where these features are configured (See Figure 2-3). The Enable SSID Broadcast controls whether or not your SSID is broadcast. Click the Setup Access List button to set up the MAC addresses that can connect.

These features don't do much to protect your network but do cause serious usability concerns. At one point, using these features were requirements for companies transmitting credit card data over wireless networks, but the requirements were dropped in late 2008 because the tradeoff wasn't worth it. If even the credit card companies don't think it helps security, then it's not worth doing.

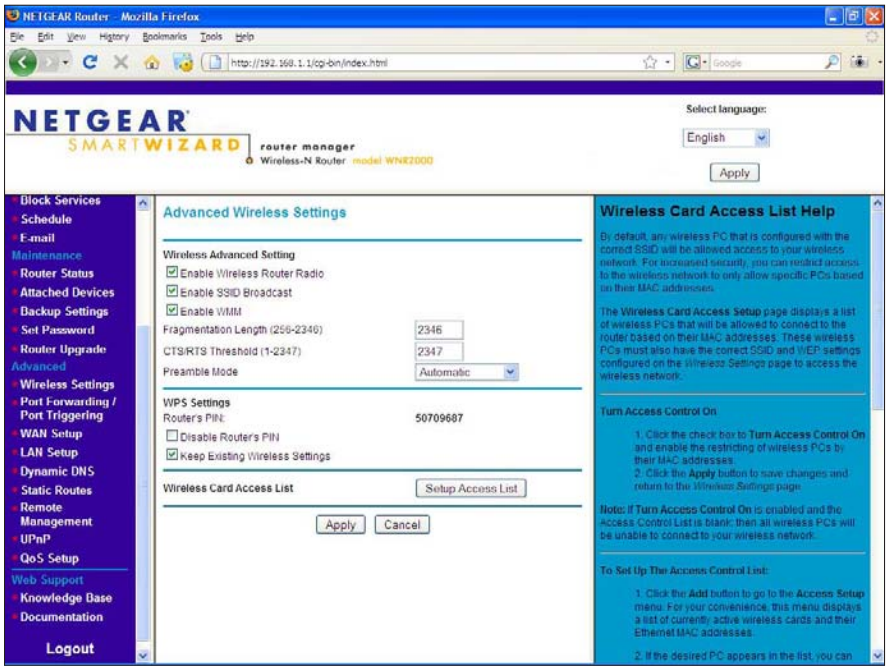


Figure 2-3: Advanced wireless settings.

So why did I even bring it up? If you do some reading on the Internet, you may come across a page talking about it. I wanted to make sure you knew the reasoning and history behind the recommendation and the tradeoffs involved.

Allowing incoming connections

A firewall's job is to block bad packets and allow good packets. At the very simplest level your router's firewall does this by blocking any connections that were initiated by outside hosts and allows anything that was initiated from the inside. That's why you can request Web pages from your computer, but people can't open your file shares from the outside.

Most applications behave under these circumstances. Firewalls have been around for ages, even before the first home router. The nature of the Internet is also *client-server*, which means you (the client) request stuff from the server, and not the other way around.

That's not to say there aren't applications that break this mold. Peer-to-peer file sharing and online gaming are two notable examples. In these applications, the server sometimes has to push data to you, or you must accept a connection from another client to pull a piece of data. The firewall prevents this.

Port forwarding is a feature that lets you take certain inbound connections and forward them to a particular host on the inside of your network.

The firewall is preventing incoming connections for a good reason — they're usually insecure. When setting up port forwarding, be careful to only forward what you need.

To set up port forwarding, follow these steps:

1. **Determine the port to be forwarded, which should be provided by the application or its documentation.**

   Figure 2-4 shows a dialog from a file-sharing program, indicating that the incoming port is 59534.

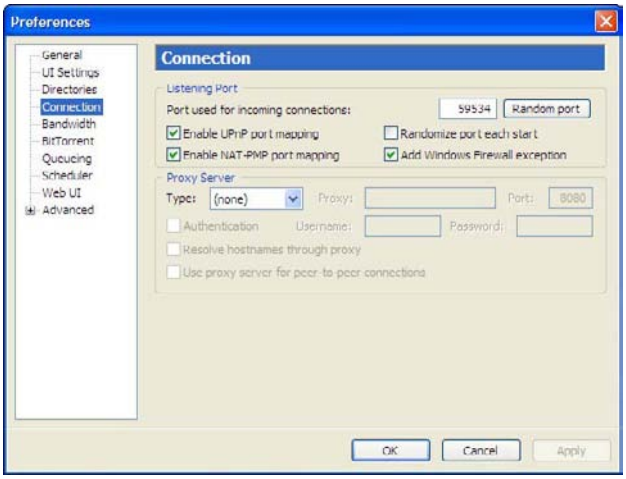


Figure 2-4: Determining the port to be forwarded.

Every application is different, and some (like the one above) choose random inbound ports. Just because the example above uses port 59534 doesn't mean that your application will.

2. **Navigate to the Port Forwarding menu in your wireless router's administrative interface, which is shown in Figure 2-5.**

3. **Ensure that Port Forwarding is selected. Check under Service Name to see if the name of the protocol is there.**

   (If it is, skip over the next section.)

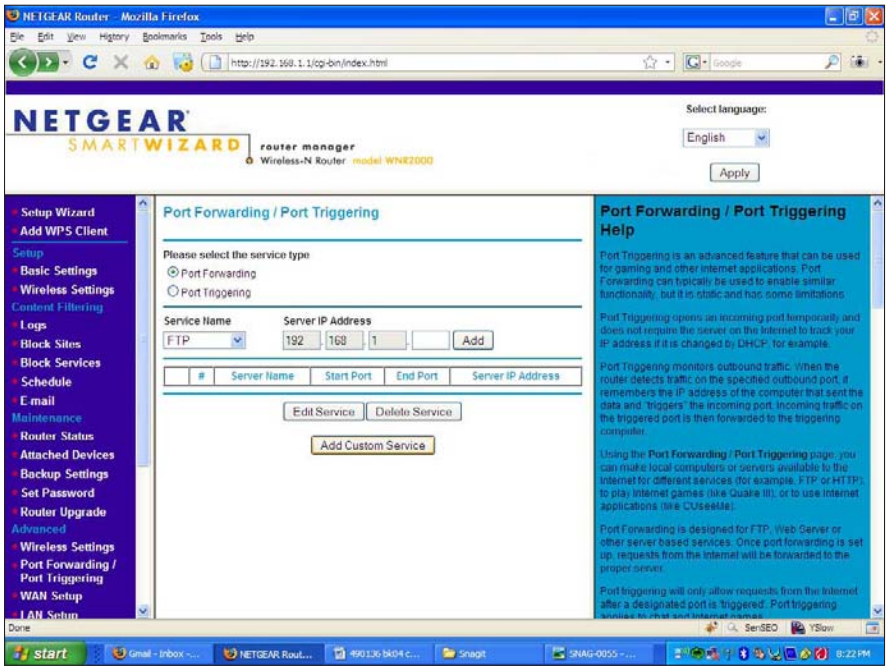


Figure 2-5: The port forwarding configuration screen.

Adding a custom service

The NETGEAR router comes with some predefined port forwarding protocols. If your protocol isn't on the list, you have to add it.

1. **Select the Add Custom Service button to get to the screen shown in Figure 2-6.**
2. **Fill in the details about the port to be forwarded.**

   The name of the service is what you want it to be. In this case, I used the name of the application.

   There is only one port to be forwarded, so I've put that in as both the starting and ending ports. Finally, the traffic is to be forwarded to 192.168.1.100, which is my laptop.
3. **Click Apply, and you are taken back to the port forwarding screen showing your new configuration (see Figure 2-7).**

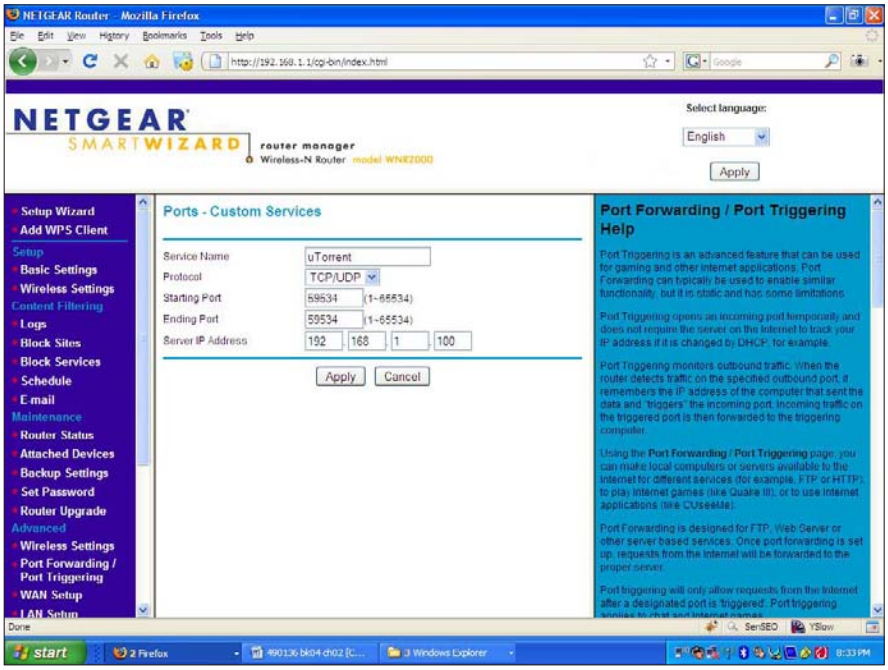


Figure 2-6: Adding a custom service.

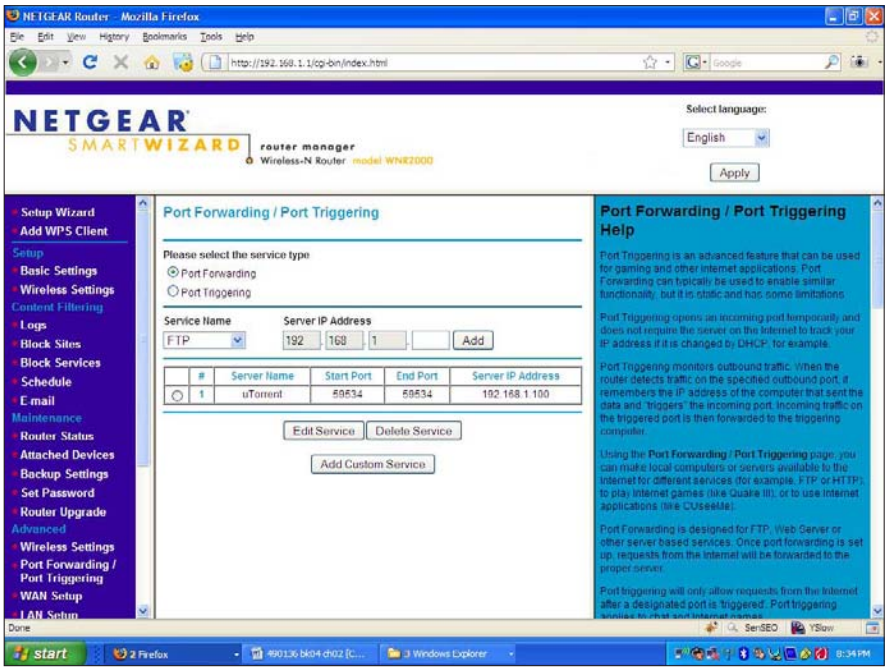


Figure 2-7: The port forwarding screen showing the new configuration

Forwarding a known service

If the service is already known to the router, such as FTP, then you can select it from the main menu and enter the address of the server. Allowing incoming FTP traffic would be helpful if you wanted to set up a file server on the inside of your network.

Port triggering

The downside to port forwarding is that you have to know the address of the computer that wants to use the forwarding. This inconvenience is usually minor, but if it is a problem for you, then port triggering is an option.

Port triggering waits for an internal computer to make a predetermined type of connection to the outside. Upon seeing the connection, the router sets up a port forward to that computer.

The configuration of a port trigger is similar to that of a port forward, except that you must identify the outbound traffic, and you don't need to specify an internal host.

Usually a port forward will suffice, though, and if you need a port trigger, then your application's documentation will specify that.

DMZ server

In the security field, a demilitarized zone (DMZ) is a network that's in between the inside and the outside, and all traffic must pass through a firewall. Companies put servers that they want to be Internet accessible in there, such as Web and e-mail servers. The servers can't be trusted as much because they're exposed to the Internet, so the firewall also dictates how the server can talk back to the company's internal network.

The DMZ server on a home router is the catch-all host that all unknown traffic gets sent to. Think of it as a port forward of all the ports to one server. Good or bad, incoming traffic gets sent to the server you specify.

Browse to the WAN Setup screen shown in Figure 2-8 to set up a DMZ server. Select the check box and type the address of the server, and all the bad guys can talk to your internal device.

Avoid using this feature. That computer is going to get a lot of attacks. That same computer is also free to talk to any computer on your internal network, so if it gets compromised, you can expect more to follow.

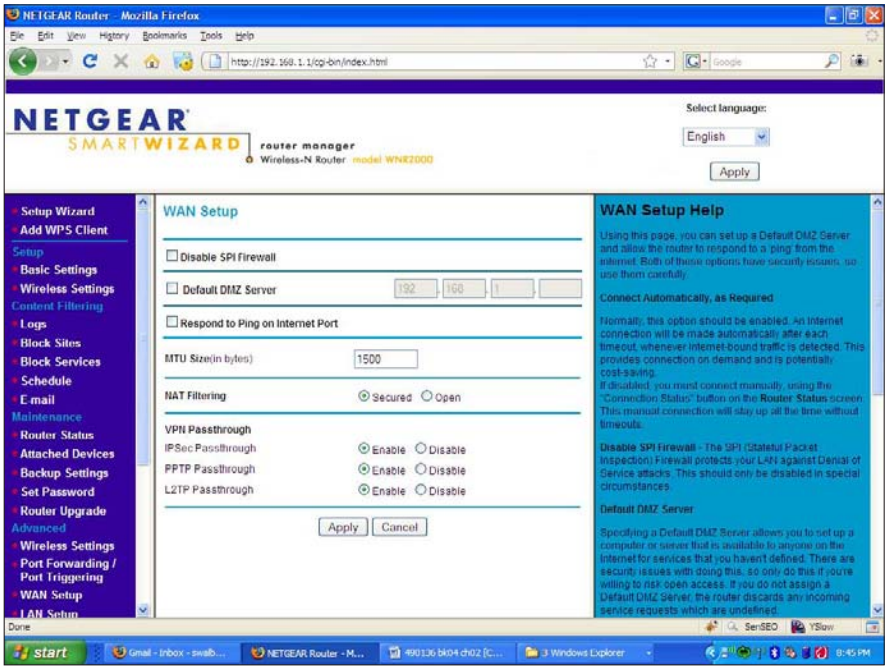


Figure 2-8: The WAN setup screen.

VPN passthrough

Your employer might let you work at home using a virtual private network (VPN) tunnel. This gives your computer a secure tunnel over the Internet back in to your place of employment.

VPNs don't always play nicely with home routers. If you're having problems with your VPN, check to make sure that the VPN passthrough options are enabled (also shown in Figure 2-8).

Reviewing Internet policies

Your router is likely able to perform some more extensive filtering on what goes in and out, rather than just assuming everything that goes out is good. Some of this functionality is rather advanced and specialized, but some of it falls under the "why didn't they think of that before?" category.

One of the more handy features allows you to block Web sites based on keywords in the site's name, or in the page itself. If you've got kids around, this is especially helpful to make sure they don't wander into some of the seedier parts of the Internet.

It is technically possible to block other applications, such as instant messaging, but chances are your router won't be able to do it. Chat programs are notorious for evading firewalls, even going so far as to masquerade themselves as Web traffic. For that matter it is possible to get around the Web filtering, so it should not be considered a substitute for proper supervision.

To block sites based on their content follow these steps:

1. **Navigate to the Block Sites menu, which is shown in Figure 2-9.**
2. **Enable blocking by selecting the Always option.**
3. **Enter your keywords one by one into the keyword box where indicated, pressing Add Keyword in between each one.**

   Figure 2-10 shows a screen where blocking has been enabled and netgear has been added. If the word netgear appears in either the URL bar or the page itself, the site will be blocked.

   Different routers are configured differently. For example, the Linksys routers maintain two separate block lists, one for the URL and one for keywords in the Web page.

   If you know the name of the site you want to block, you can enter it as a keyword. If you just want to block individual words, that's fine, too. You can do both at the same time.

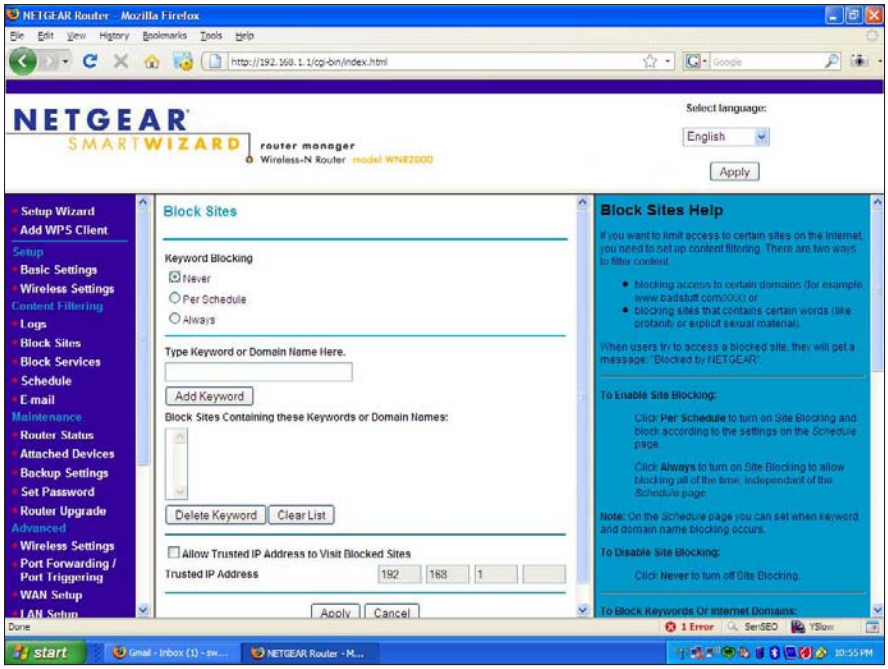


Figure 2-9: The "block sites" configuration screen.

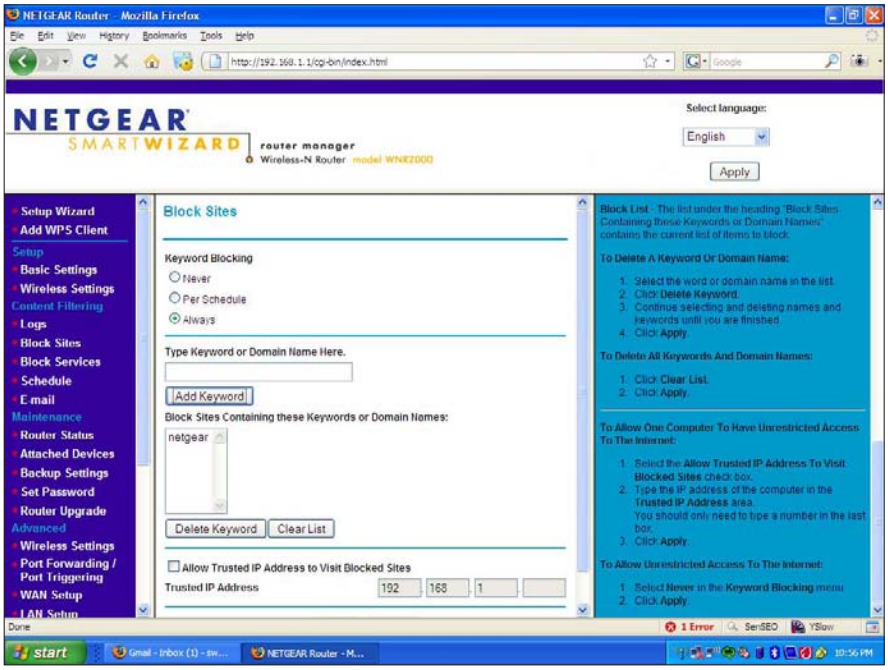


Figure 2-10: Enabling site blocking, and adding a keyword.

4. **When you're done with the list, click the Apply button at the bottom of the screen.**

   You can always come back and adjust the list.

If someone attempts to go to a blocked Web site they will see the message shown in Figure 2-11.

This message, in no uncertain terms, tells you the site has been blocked.

Some routers do not display a message. Instead, they reset the connection to the Web server, triggering an error in the Web browser. It's not as obvious to the user but still has the same effect.

Finally, if you would like to know what sites that people are going to, and if there were any blocks, click on the Logs menu (see Figure 2-12).

Here, you can see that someone tried to go to netgear.com but was blocked. The time of the infraction and the address of the computer are also logged.

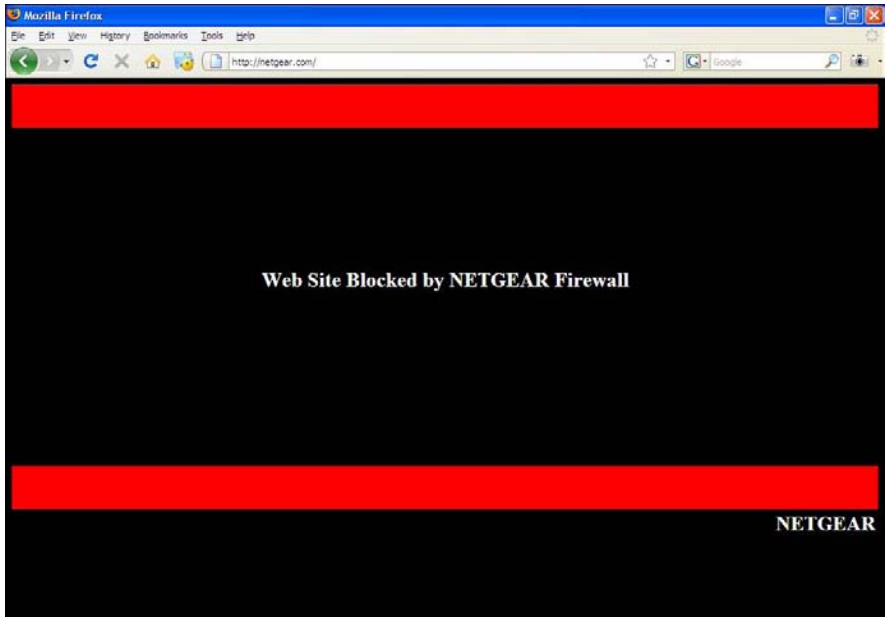


Figure 2-11: A site that has been blocked by the firewall.

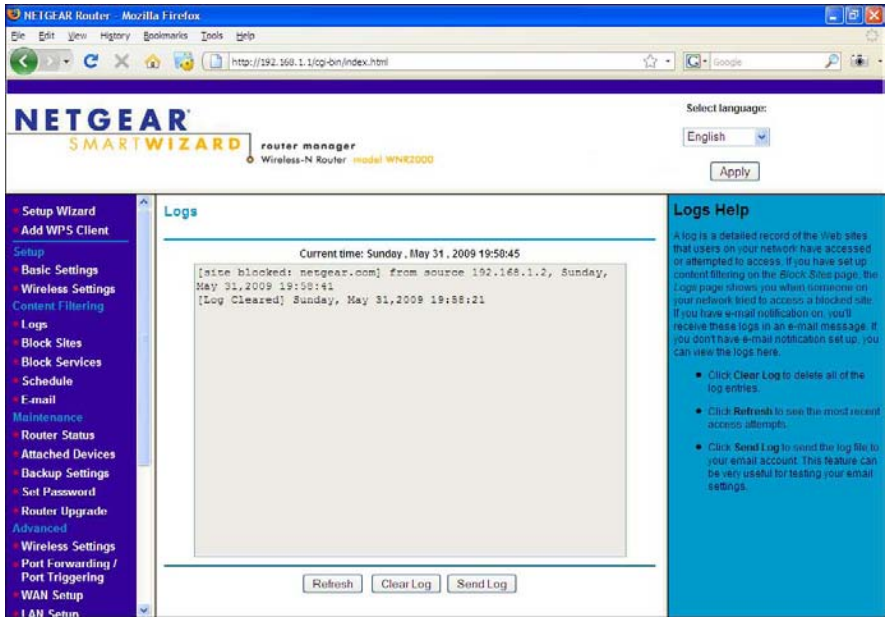


Figure 2-12: Reviewing the logs.

If you need more control

Blocking Web sites containing one of a handful of keywords is a pretty simple way of attacking the problem of keeping your kids from bad Web sites. If that's not good enough for you, then consider a subscription service that categorizes Web sites and lets you decide which categories are good and bad.

These services are used by either installing software on the computer that's to be filtered or by integrating with the router. Few routers support this integration, so go looking for a router that supports URL filtering with an external service if you want that option. Be forewarned, the router will probably cost a bit more than a router without the feature.

In addition to the cost of the router or software, you'll probably have to pay a regular subscription fee for use of the block list, which would include updates to the list.

Many business grade routers with integrated firewalls are starting to incorporate Web filtering, virus scanning, and more advanced (and automatic) firewalls. It's only a matter of time before this technology makes its way into home routers.

Whatever software or hardware you use, it's not a substitute for proper supervision. Putting the family computer in the living room, where everyone can see it, might be a cheaper and easier option.

Chapter 3: Protecting Your Computer

In This Chapter

- **Keeping your computer up to date**
- **Getting the right security software**
- **Understanding browser security**
- **Working with the User Account Control**

Security is a process, not a product. Even the best software out there won't protect you if you don't use it properly. Fortunately, there's a lot of good software built right into the operating system, and this chapter focuses on making it work for you.

Security is also a tradeoff between convenience and risk, so I look at a few places where you can choose to take a less aggressive security posture in return for less intrusion on your life. It's a fair trade — there are no wrong answers.

Throughout this chapter, I focus on the Windows Vista security tools. Other than a basic firewall, the older Windows XP has virtually nothing built in and therefore relies on third-party tools. Vista isn't perfect, but it's leaps and bounds ahead of XP.

Visiting the Windows Security Center

The Windows Security Center (WSC) was introduced to Windows XP in Service Pack 2, and was improved as it was carried forward into Vista. The job of the security center is to monitor the status of various security-related settings and to give you an easy-to-read view of your security posture.

The picture of the shield with the exclamation mark in Figure 3-1 is your first indication of a problem.

Figure 3-1: The Windows Security Center alert in the system tray showing a warning.

If your computer has a more serious security problem, you see a red X instead of a yellow shield, as shown in Figure 3-2.

Figure 3-2: The Windows Security Center alert showing a serious problem.

The difference between warnings and serious problems in this case is subjective. Either case should prompt you to check and see what's going on, though.

Double-click on the Security Center alert icon to bring up the security center, which is shown in Figure 3-3.

The WSC is broken down into four separate areas:

- **Windows Firewall:** This area protects your computer against incoming and outgoing connections, which is an additional layer of defense if you've already got a hardware firewall.
- **Automatic updating:** This service automatically downloads and applies patches if you'd like, which ensures your computer is always up to date.
- **Malware protection:** This area shows the status of both anti-virus and anti-spyware software.
- **Other security settings:** This area is a grab bag of extra security features.

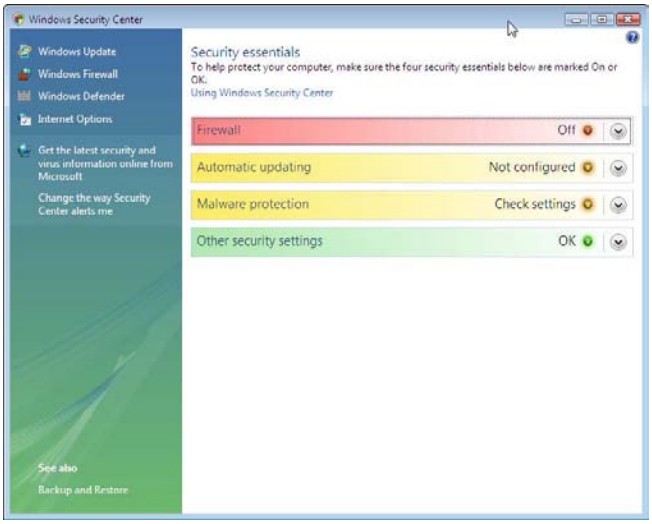


Figure 3-3: The Windows Security Center.

Each item in the Windows Security Center is shaded according to its status and also provides a line of text to further describe the status. Based on the dark shading, you can see that Figure 3-3 has a serious problem with the firewall because the firewall is turned off. The other elements seem to be healthy.

If you don't see an icon in your system tray, your computer probably meets all the requirements of the Windows Security Center. If you still want to check, go to the Control Panel and then click on the Check this computer's security status link.

Exploring the Windows firewall

The Windows firewall's job is to inspect the network packets that go in and out of your computer and to decide if they're allowed or not, based on the configured policy. The policy is changed over time based on feedback from the user. For example, using a new program might prompt you for permission to allow that particular program to make the network connections.

The firewall tracks down connections to the application. One application may be permitted to make a Web request, but another application might not. By doing so, you have an increased chance of spotting malware because you will be prompted when the application tries to make a request that is out of character.

Turning on the firewall

Turning on the firewall is a straightforward process.

1. **From the Control Panel, click the security icon to take you to the security menu within the control panel.**

   This is shown in Figure 3-4.

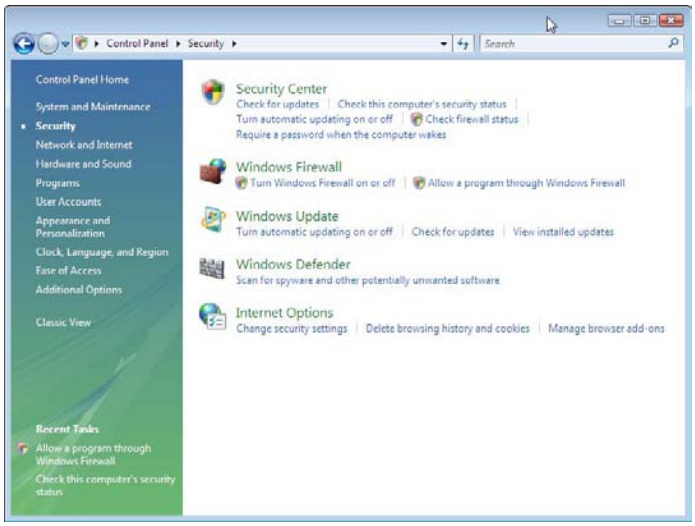


Figure 3-4: The Security menu.

2. **From the Security menu, select Turn Windows Firewall on or off to take you to the firewall settings menu shown in Figure 3-5.**
3. **From the Firewall Settings window, select the On (Recommended) option and click the OK button.**

   Your shields are now up!

Living with the Windows Firewall

If firewalls were foolproof, then you'd never have been given the option of turning it on — it would be just a part of Vista you never thought about.

Unfortunately, the firewall is not perfect, and it can't react to every situation. By default, the firewall blocks incoming connections. But what if you need a connection to come in?

When an application requests the ability to listen for incoming connections, and the policy would block that, you are given the opportunity to override the block through the dialog box shown in Figure 3-6.

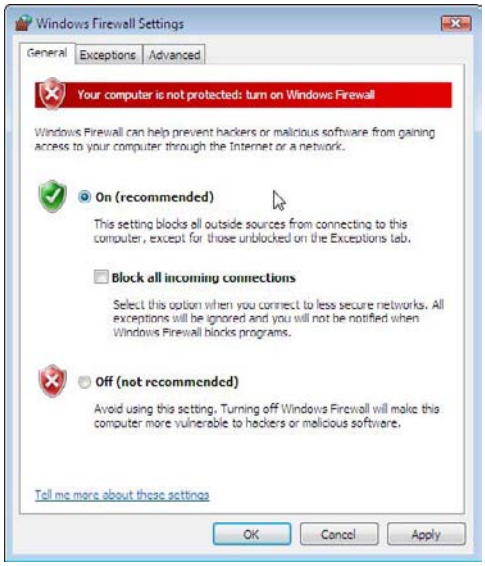


Figure 3-5: The Firewall Settings window.

Figure 3-6: Vista prompts to allow a connection.

The dialog box shown in Figure 3-6 is light on details. You're being asked to decide whether or not an application should accept connections. If you allow it, the Windows firewall will allow incoming connections into this application.

To be clear, the application has requested the privilege of accepting connections. The first question you should ask is "Did I just launch that application?" If the query came while you were in the middle of browsing the Web, then you should be extra cautious. However, in this case, I ran the program. If you're not sure which program generated the alert, then check the dialog box because it's listed there.

After you determine that the alert was as a result of a program you chose to run, you should ask "Is this the type of program that accepts network connections?"

On the Internet, a client (your computer) connects to a server to get some information. The connection is always made from one side to the other, and having a connection come in to you if you're a client is rare.

Therefore, if you see an alert asking you if you'd like to accept connections, you should qualify the last question by asking yourself why someone would want to connect to me.

You want incoming connections on the following scenarios:

- When you're running some server software such as an FTP server.
- When you're running a peer-to-peer (P2P) file-sharing program that shares out parts of the file as you download the rest.
- When you're running some remote control software and want people to be able to control your computer.

It's also important to note that if you're behind a router, then people from the Internet can't make direct connections to you and wouldn't be able to connect to the application anyway. There are exceptions to this, such as if you've enabled port forwarding (see Book IV, Chapter 2).

If you want to allow the application to receive connections, then click Unblock. If not, click Keep Blocking.

Using automatic updates

Software isn't perfect. Actually, if you spent some time as a software developer, you'd be continually surprised when it works at all. A popular quote among developers is "If we built buildings the same way we built software, the first woodpecker that came along would destroy civilization."

Despite Microsoft's biggest efforts, bugs exist in Windows. Some of them are pretty tame such as "screen doesn't redraw properly." But some of them are pretty bad like one that surfaced in late 2008 that allowed anyone that could connect to your machine to take it over. Oops.

Patches are pieces of software that fix bugs. Think of using patches as patching up a hole in a wall, or in a bike tire. Microsoft releases these patches every month, and you can download them to make sure your computer's software is up to date.

The problem is that Microsoft software often has bugs and, therefore, it tends to release a lot of patches. Chances are you won't remember to download every single patch every month. Figuring out which patches are necessary is also a problem. So Microsoft introduced Windows Update some time ago, and more recently, made it install patches automatically, should you allow it.

In Figure 3-7, the line corresponding to automatic updates has been pulled down to show some more details.

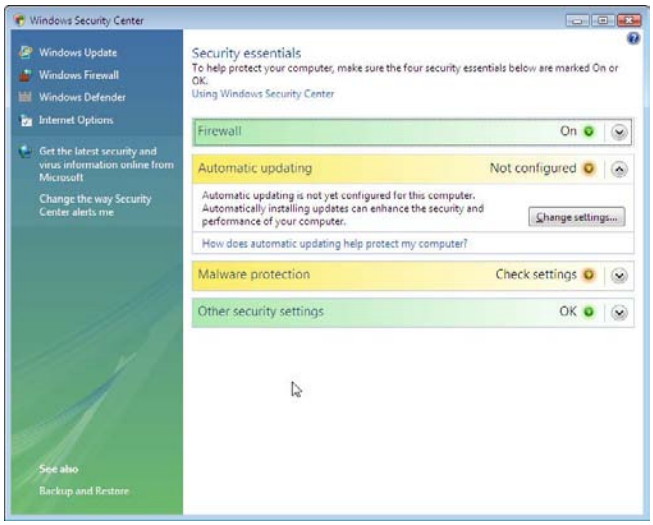


Figure 3-7: The Windows Security Center showing the automatic updates option

Click on the Change settings button to bring up the automatic updates configuration, which is shown in Figure 3-8.

From here, you have two options:

- **Install updates automatically:** In this mode, Windows checks for updates periodically and installs them.
- **Let me choose:** Gives you more flexibility on how you apply your updates.

If you choose the Let Me Choose option, the screen in Figure 3-9 appears. You can select one of the following options:

- **Install automatically:** This option is almost the same as the one in the previous menu. Updates are downloaded and installed without your intervention. The difference between this and the previous menu is that you get to choose the time the updates happen.

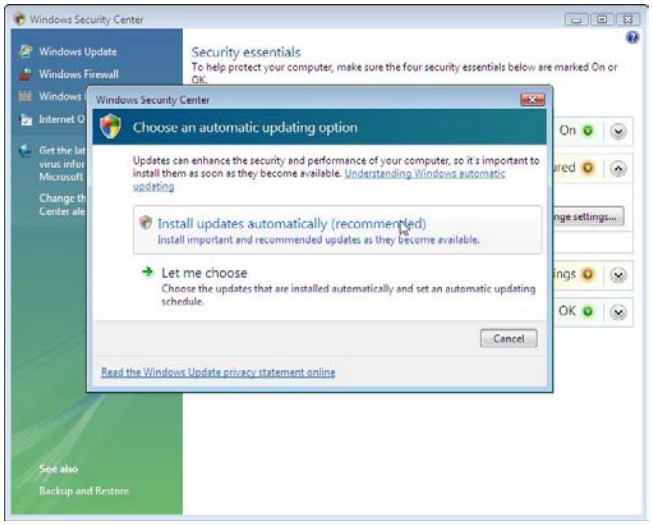


Figure 3-8: Configuring automatic updates.

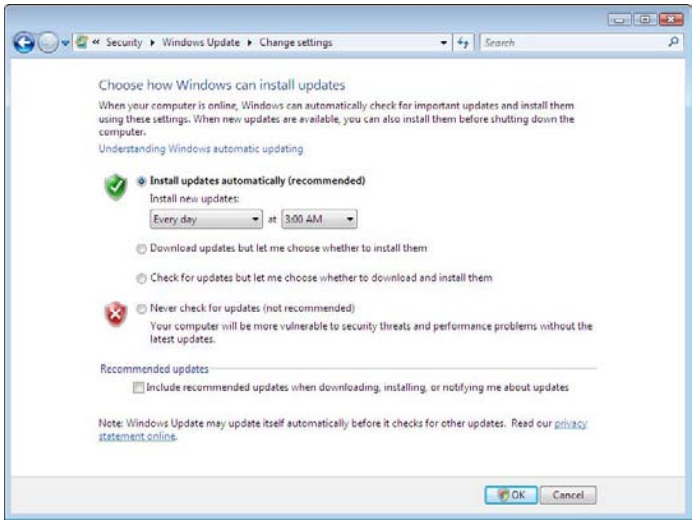


Figure 3-9: Showing the available options for Windows Update.

- **Download updates but let me choose whether to install them:** If you're not comfortable with updates happening without your knowledge, choose this option. When new updates are released your computer downloads them and then prompts you to download them.
- **Check for updates, but let me choose whether to download and install them:** This option is similar to the last option, except that the updates

aren't downloaded automatically. I find this option to be troublesome because I like having the updates happen when I'm not using the computer.

- **Never check for updates:** If you want to do it by hand, choose this option.

I recommend setting your system up for automatic updates, so you won't miss an update.

Checking for updates manually

The automatic updates only download the patches that Microsoft deems critical. Every so often, check for updates manually; doing so lets you download all the optional updates.

Going through the process manually after you first install your computer is a good idea. Usually, you have some updates that require the presence of earlier updates, so even after going through the updates once, you may find that you're not fully patched. Only the manual process gives you the confidence that you're up to date. To do so, follow these steps:

1. **From the Control Panel, select Check for Updates from the Security menu.**

   The screen shown in Figure 3-10 appears.

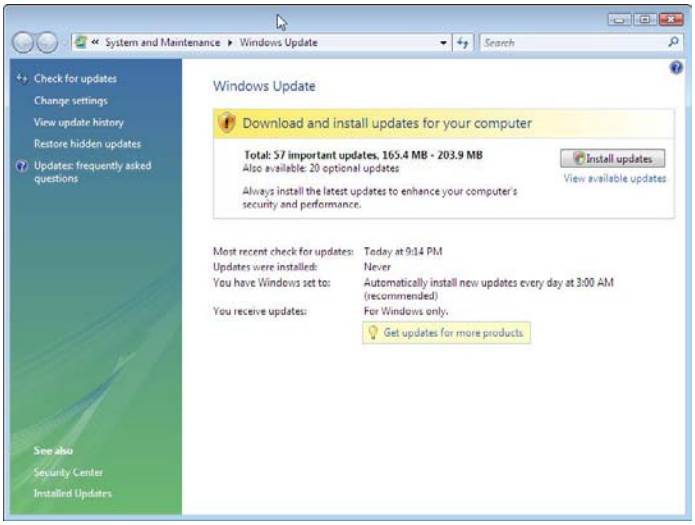


Figure 3-10: Showing the available updates.

In Figure 3-10, you can see that the system has 57 important updates to download. If you are curious about what they are, you can click the View available updates link.

This screen also lets you confirm your automatic update settings. Here you can see that the system is configured to update nightly at 3 a.m., and that it's never been updated.

2. **Ignore the optional updates for now and click the Install Updates button to begin the update process.**

   Sometimes the updates come with a license that you must accept to use. In Figure 3-11, the license is for the Windows Malicious Software Removal Tool, which is the built in anti-spyware product. I look at this later, but for now, you have to accept the license terms and click Finish.

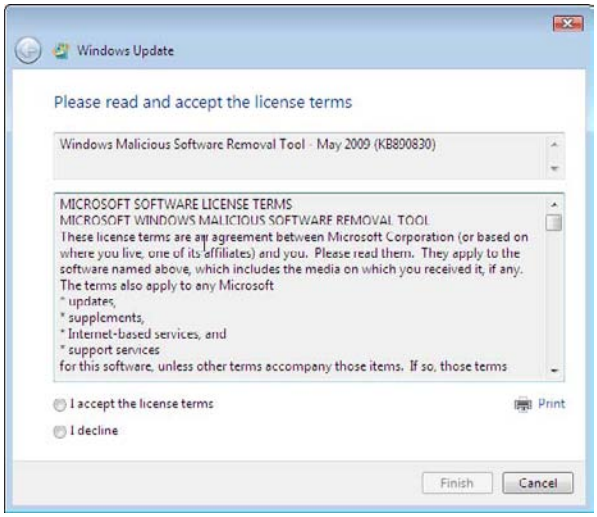


Figure 3-11: Accept the license terms.

3. **Wait while your system downloads and installs updates.**

   The time it takes to do this depends on the speed of your computer and how many updates you have.

Your computer will be usable during the update process, but don't expect peak performance. There's a lot going on during the update process, and at times your computer might feel sluggish.

After the updates are installed, you get confirmation, as shown in Figure 3-12.

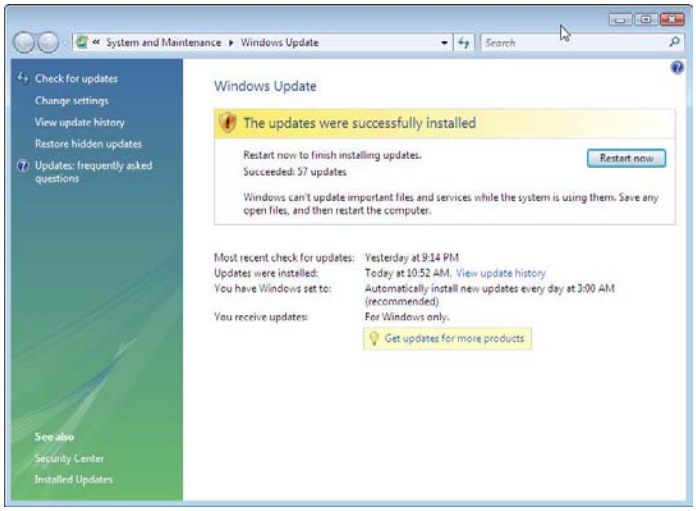


Figure 3-12: A confirmation that the updates were successfully installed.

If you read the message on the screen, you can see that you're being prompted to reboot to finish the updates. You can do so now, or close the window to reboot later.

If you choose to reboot later, then you are periodically reminded to reboot by means of a dialog box that pops up from the system tray, shown in Figure 3-13.

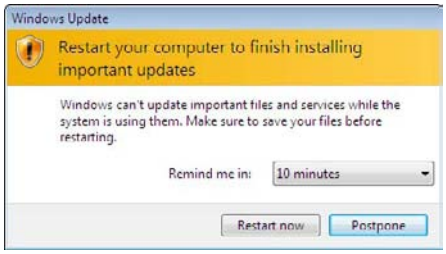


Figure 3-13: Vista prompts you to reboot.

You can continue to postpone the reboot as long as you want.

When you finally reboot, the process takes longer than normal because updates are being processed.

Some updates depend on other updates already having been applied. The first time you apply updates you should go back and check to make sure all updates were applied correctly.

1. **After the reboot, go back to the updates window by going to the Control Panel and selecting Check for Updates from the Security menu.**

   Figure 3-14 shows that there is one important update and 20 optional updates.

2. **Click on View available updates to get details of these 21 updates.**

   Figure 3-15 shows the available updates. The important update is a security update, and most of the rest are regular system updates. If you are curious, you can enter the identification next to the update, such as KB931099, into the search engine at Microsoft.com to find out the details.

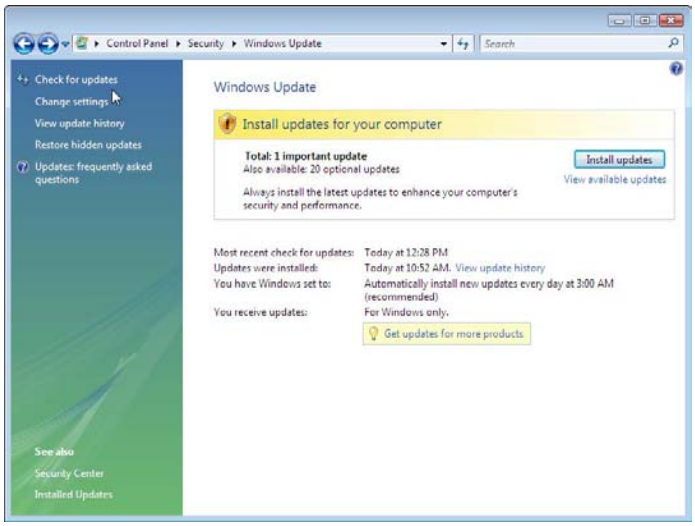


Figure 3-14: There are still more updates.

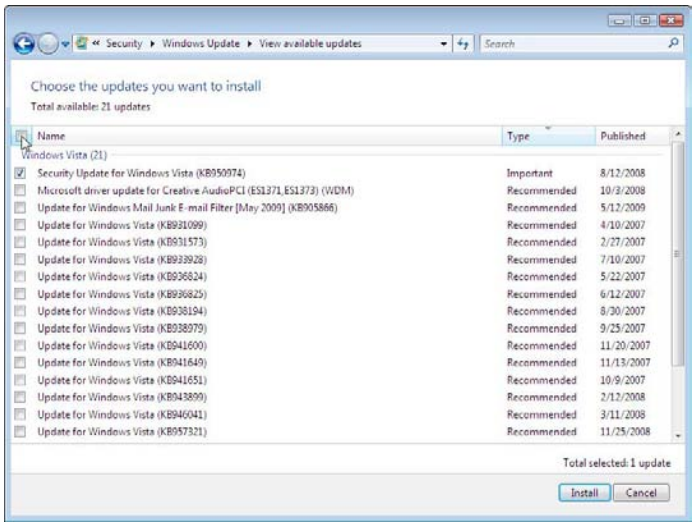


Figure 3-15: Viewing all the updates.

3. **Choose the updates you want to install by checking the box next to the name. If you want to select them all, you can check the button at the top of the dialog.**

4. **Finally, click on Install to begin the update process.**

   You might have to go through this a couple more times before you're all up to date. However, after you're done, you are told that there are no new updates available, as in Figure 3-16.

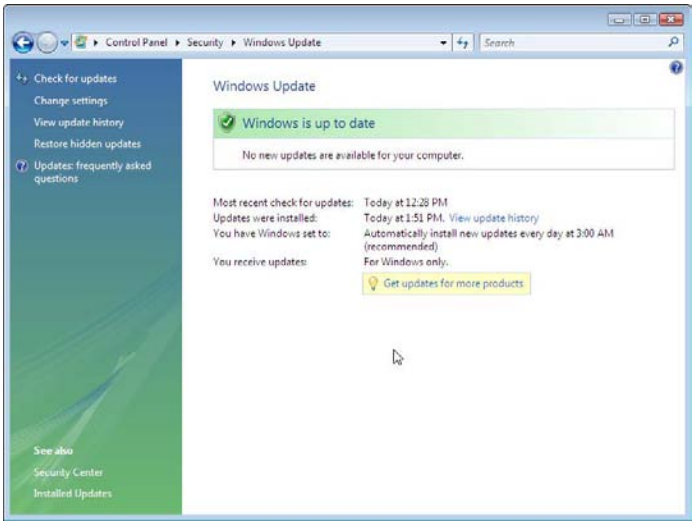


Figure 3-16: No new updates are available.

After all of that, your automatic updates take care of you, and all you have to worry about is performing the odd reboot.

Protecting against malware

Microsoft Windows spawned an industry of malware authors eager to make a buck off of computer users. The malware authors were fairly successful, which itself was the drive behind the good guys to come out with anti-malware products.

Anti-virus products have been available long before the Internet was commonplace and have managed to keep pace with the virus authors. Anti-malware software has not been as successful as its anti-virus brethren. Finally, with the release of Windows Vista, Microsoft bundled its own anti-malware software with the operating system.

Microsoft calls this software Windows Defender. It is bundled with Vista and also downloadable from Microsoft.com for Windows XP and 2003.

Bundled security software

If you've bought a computer recently, especially from a retail outlet, you might find that it comes with anti-virus and anti-malware software. If so, great! But, please check carefully, because many of these are time-limited trials and will stop working after 30, 60, or 90 days.

If, after the trial, you're happy with the software, then by all means buy it. Windows Vista was designed to work with third-party anti-virus and anti-malware products. Make sure that you understand what you're signing up for, such as recurring billing.

If you don't want to keep the software, make sure to uninstall it to avoid being nagged about buying it.

Sadly, Windows Defender doesn't do anything for viruses. You're on your own there, so I've got a free alternative for you later on in this chapter.

Looking at Windows Defender

1. **From the Control Panel choose Security and then click on Windows Defender to open Windows Defender, shown in Figure 3-17.**

   In the figure you can see that everything is just fine according to Defender.

2. **If you want to scan your computer right away, click the Scan button at the top. If anything pops up, you can deal with it right there.**

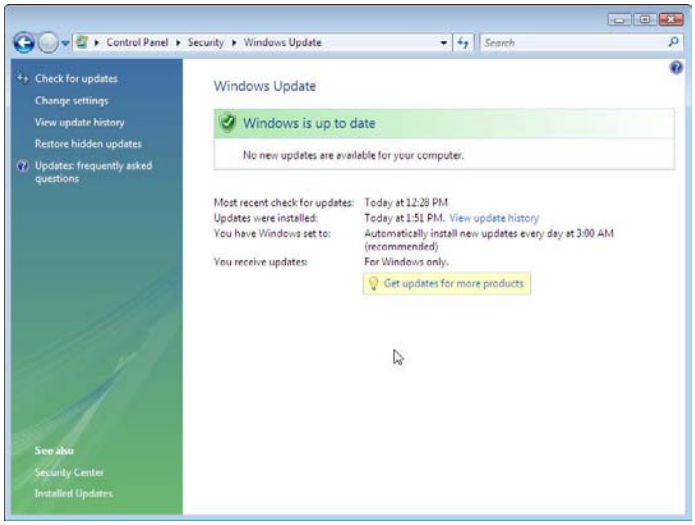


Figure 3-17: The Windows Defender main screen.

Other than that, Windows Defender doesn't provide a whole lot of options. It's nowhere near as interesting as anti-virus.

Installing anti-virus software

Many companies are selling anti-virus software. You can expect to pay around $30–$60 for the software, depending on the features, and to pay that every year for upgrades and updates to the virus signatures. Packages at the upper end (and higher) include more than just anti-virus and anti-spyware; they help you with spam, identity theft, and a whole host of other problems.

There is, however, a free anti-virus package out there. AVG is a company that produces anti-virus and anti-spyware software with various features. They offer their base package free for noncommercial use. If you don't already have anything else, I highly recommend AVG.

If you scroll to the bottom, you can see the download link, which is shown in Figure 3-18.

Upon clicking the download link, you are redirected to another site for the download. If you are using Internet Explorer, you might get the warning shown in Figure 3-19. If so, click on the warning bar and then click Download File.

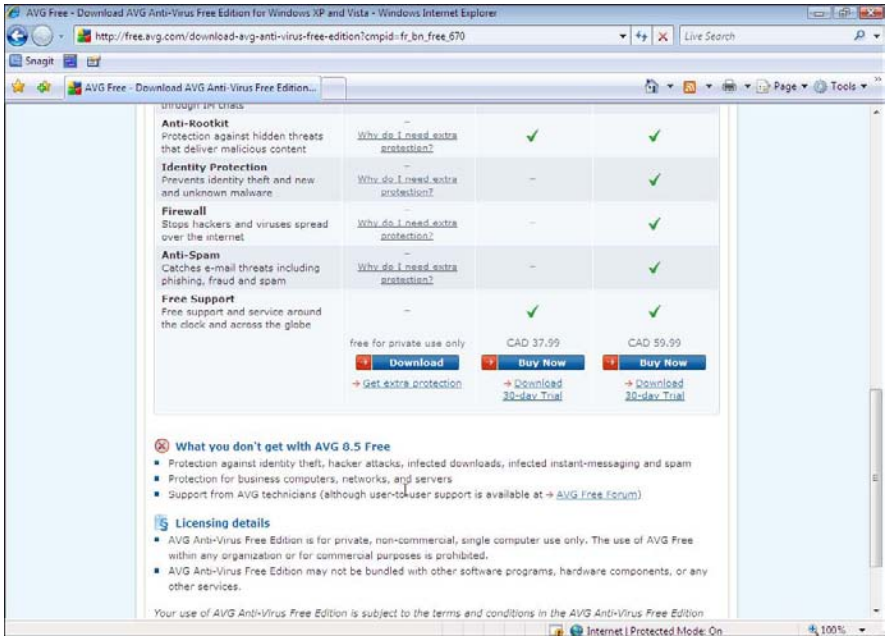


Figure 3-18: The download link at free.avg.com.

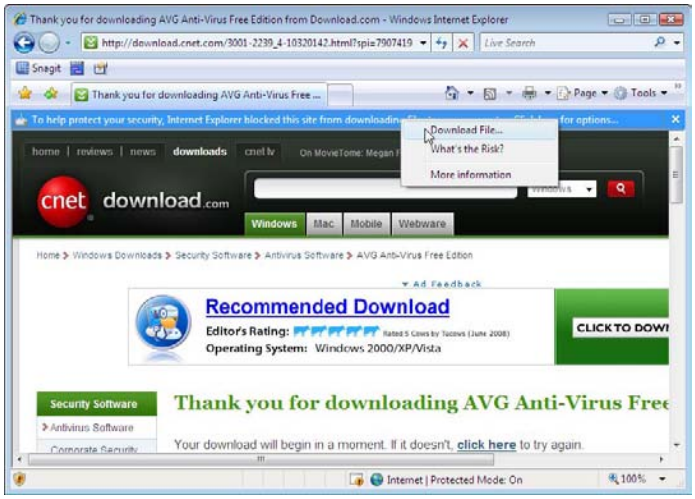


Figure 3-19: Internet Explorer showing a download warning.

Warning or not, the next dialog box you get prompts you to save or run the file, as shown in Figure 3-20. Clicking Run is easy.

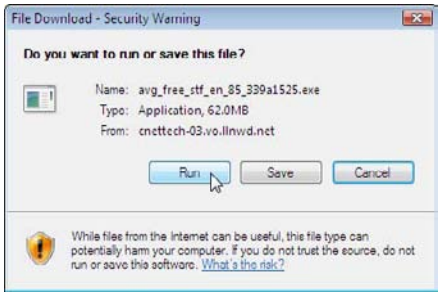


Figure 3-20: The Run or Save dialog box.

Grab a coffee, because the download takes a couple of minutes. If you want to grab one for me, I take mine black, please, and thank you.

Configuring AVG

The installation program starts as soon as the download begins and you see Figure 3-21.

The next few screens prompt you to accept the license and remind you that you are using the free edition of the package. Click Next to advance screens until you come to Figure 3-22.

Figure 3-21: Beginning the AVG installation.

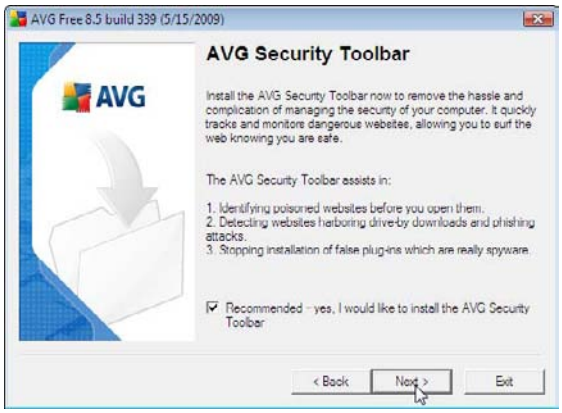


Figure 3-22: Installing the AVG toolbar.

The AVG toolbar provides some enhancements to Internet Explorer that can help keep you safe, so it is worth installing the toolbar.

Be careful about which toolbars you install because you don't know if they contain malware. The AVG toolbar is a helpful toolbar and alerts you if you try to install a toolbar containing malware.

Continue following the prompts until the software reports that installation is complete.

Configuring the first run

After you install the AVG anti-virus software, you are prompted to configure it through the first run wizard. For the most part, you can accept all the defaults, though there are a couple of screens where you might choose to select an alternate option to the default.

The first screen is shown in Figure 3-23. Click Next to continue.

Figure 3-23: Beginning the first run wizard.

The next screen is the most important, because it schedules the periodic update and daily scan (see Figure 3-24). One update a day should be enough.

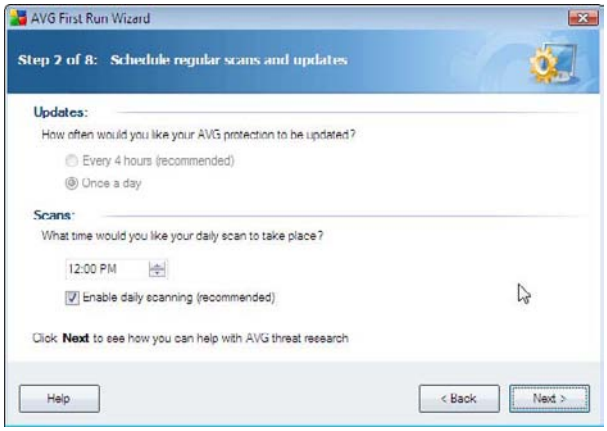


Figure 3-24: Configuring the time and type of scan.

Configure the scan for a time that works for you and make sure that the Enable scanning check box is selected. Your computer is slower than normal because of all the disk reads, so pick a time where you don't expect peak performance. Lunchtime works well for me.

Follow the instructions on the screens to complete the installation. You may or may not want to choose the following options:

- **Agree to provide information about detected threats to AVG:** This option is disabled by default, and you may want to consider enabling it. Turning on this option sends information about what the software finds back to AVG for product improvements and virus research. Any information that could identify you is stripped before it is sent.
- **Change my default search engine to Yahoo!:** If you installed the toolbar, this option changes your default search engine to Yahoo!. By default this is selected; if you prefer a different search engine, then deselect it.

You go through a few screens, the software updates itself with the latest virus definitions, and then you are protected.

Verifying that you're protected

You know you're protected from viruses two ways, as shown in Figure 3-25.

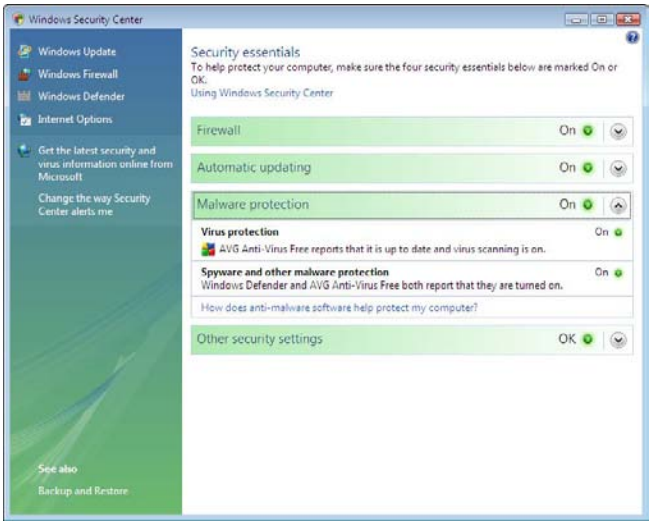


Figure 3-25: Verifying that the anti-virus software is working.

The first indication is that the Windows Security Center isn't complaining about the anti-virus (go to the Control Panel and then find Check this computer's security status, or see the earlier section called Visiting the Windows Security Center). In fact, if you look at the Malware protection section, you see the following:

- **Virus Protection**: AVG Antivirus Free reports that it is up to date and virus scanning is on.
- **Spyware and other malware protection**: Windows Defender and AVG Anti-Virus both report that they are turned on.

Finally, look in the system tray to see the new AVG icon (the four colored boxes).

You've got virus protection. You've got spyware protection. Let's move on.

Other security settings

By now you've set up some pretty good defenses. Your computer updates itself regularly. It has a firewall, and its anti-virus and anti-spyware sensors are busy looking for any signs of malware.

You could stop right here and be fairly worry free when browsing the Internet. But being safe on the Internet is much more than the software you run; it's also the decisions you make.

I'm pretty sure you're going to approach the Internet with a cautious eye and make good decisions, but even the best of us clicks the odd dialog box without reading it too closely. So, I'm going to show you a couple of safeguards that you can use to further protect yourself against the bad things out there.

Creating separate accounts for administrators and users

Windows Vista is a multiuser operating system. This means that the system recognizes that you are different from someone else based on a username that you provide. Vista recognizes you by your *account*, which has a name and a password.

Using separate accounts means that you can keep your files separate from other people that use your computer. Maybe you want to protect stuff from being deleted; maybe you want your nosey sister to stay out of your stuff. Either way, one user can't touch another user's stuff.

Accounts also have privilege levels — either a standard user or administrator — in Vista. The account you're using now is probably the one you created when you set up the system and is an administrator. In this section, you create a standard user account for day-to-day use which limits your exposure if something gets by your malware filters. Follow these steps:

1. **Go to Control Panel and select Add or Remove user accounts.**

   The list of user accounts appears, as shown in Figure 3-26.

   In the figure you see that there is a user called Sean, who is an administrator and has a password. You can also see a disabled guest account that you will not use.

2. **Select Create a new account to start creating the new account.**

   The form you see is shown in Figure 3-27.

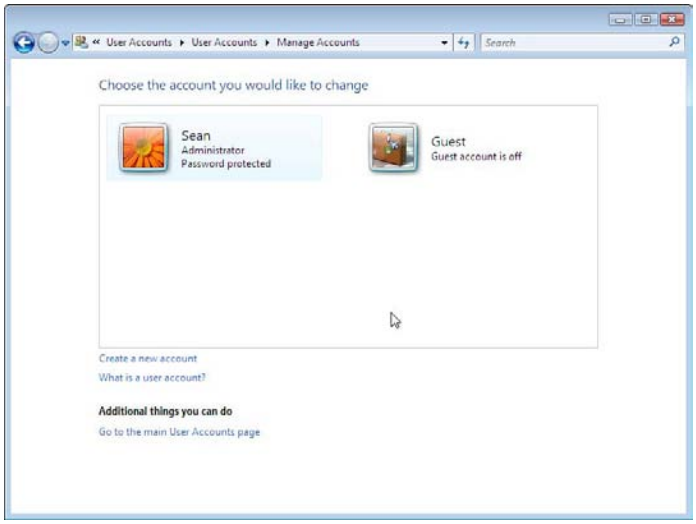


Figure 3-26: The initial list of user accounts.

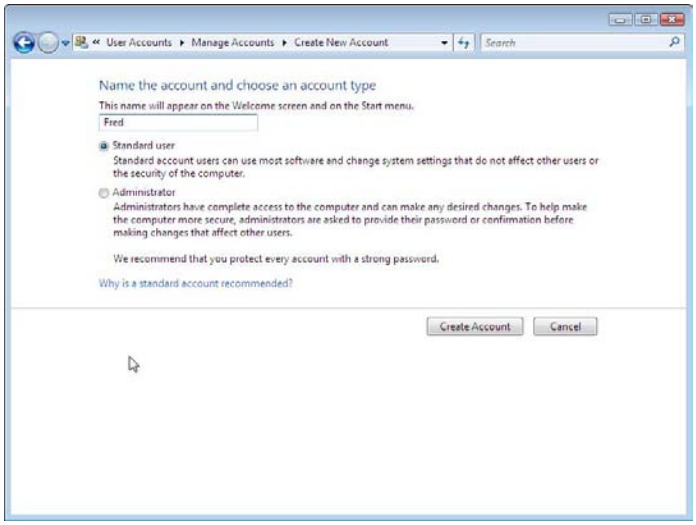


Figure 3-27: Creating an account.

The username I have selected is "Fred." Note that the account is to be created as a standard user rather than an administrator (which is the default).

3. **Click on the Create Account button to continue.**

   You are taken back to the previous menu, and you can see the new user (see Figure 3-28).

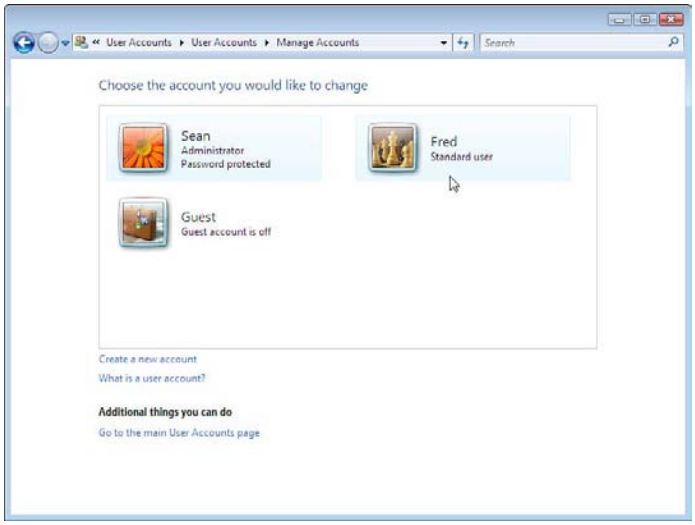


Figure 3-28: The user list showing the newly created user.

4. **Click on the new user's name and then click the Create Password button, shown in Figure 3-29.**

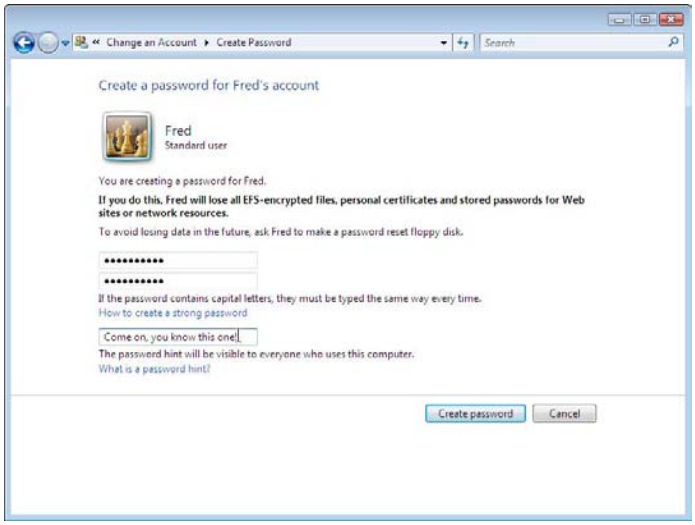


Figure 3-29: Setting the password on the new account.

5. **You must enter the password twice, and you can also give a password hint to be used if you forget the password.**

It is possible to reset passwords as an administrator, but heed the warning in Figure 3-28. If you end up using the encrypted file feature, you risk losing your files.

Logging in

The next time you start your computer (or if you select Logout from the Vista menu) you will see your new user available to use. Log in with that user and do your work as normal.

Should you need to assert your administrative might, you don't have to log out and back in again as your administrative user. Simply right-click on the icon you want to run, and select Run as administrator, just like in Figure 3-30.

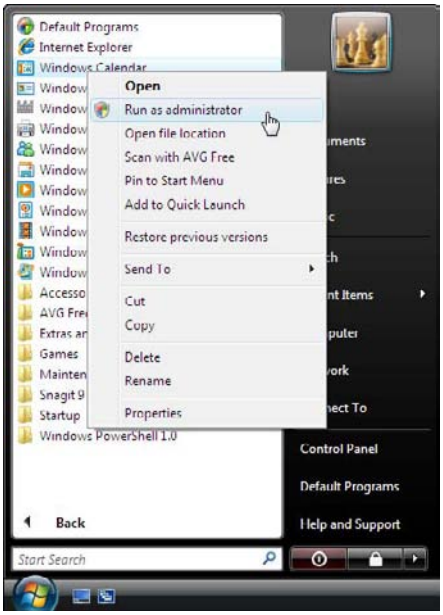


Figure 3-30: The Run as administrator option.

After you release the mouse button, you are prompted to log in as your administrative user, as shown in Figure 3-30.

Simple, eh?

Running as a regular user makes sure that any software you run can't do too much damage. It's just a good thing to do.

Figure 3-31: Logging in as the administrator.

User Account Control

User Account Control (UAC) was introduced in Vista. Formerly, if you were an administrator, you had rights to modify anything on the system. If you weren't an administrator, you were constantly running into problems because, well, you couldn't modify anything.

As a result, people just logged in as administrators because it was the path of least resistance. UAC tries to solve this problem by withholding administrative access from a user (even an administrator) until they approve the action.

You've probably noticed dialog boxes like the one in Figure 3-31.

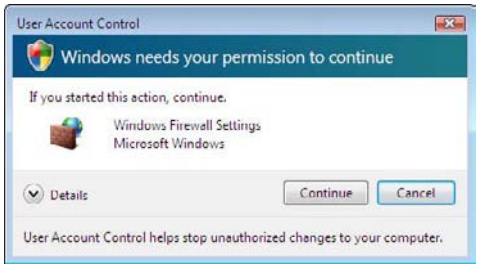


Figure 3-32: The UAC dialog box.

If you see something like that, then you know you're being asked to do something at the administrative level. Programs that need administrative access have a special shield icon next to them in the control panel.

Go ahead and click on Continue if you had run the program indicated. If it pops up for no reason, or on a file you downloaded from the Internet, it's time for caution! Fire up your anti-virus software and scan the file first.

Chapter 4: Troubleshooting Network Problems

In This Chapter

- **Verifying your settings**
- **Checking hardware**
- **Finding information about a Web site**
- **Exploring the command line**

Web sites can be temperamental. Sometimes they work, sometimes they don't. I think it's related to how badly you need the information on the page, but the scientific community is still undecided on that one. Either way, we live in an imperfect world, and not everything works all the time.

In this chapter, I present a few ways to find out if Internet problems are your fault or that of the other end and provide some general guidance on how to proceed after that.

If a Web site isn't working for you, the most obvious thing to do is try a different one. If that one works, then maybe you should just try your first Web site later.

Confirming Your Network Settings

Before you go blaming the other guy, look at your network settings to make sure that you're actually connected to your network.

1. **From Vista's Control Panel, select the View Network Status and Tasks option.**

   This takes you to the Network and Sharing Center, shown in Figure 4-1. The Network and Sharing Center is the starting point for configuring various aspects of Vista's networking features.

Figure 4-1: The Network and Sharing Center.

2. **From the Network and Sharing Center, select the View Status option on the right side of the window.**

   You can view details about the Local Area Network, as shown in Figure 4-2.

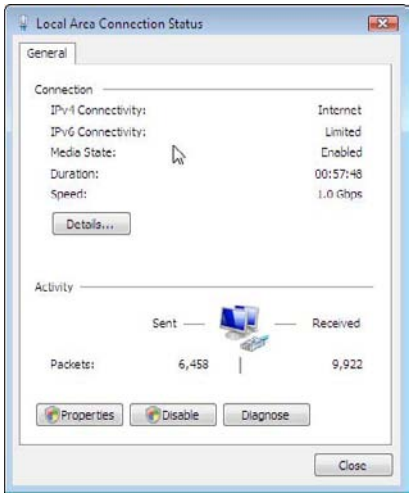


Figure 4-2: Local Area Connection Status.

From this window, you can see that Windows Vista considers that you have Internet access to the IPv4 network.

IPv4? IPv6?

Computers and networks are constantly evolving. Network *protocols* are standardized ways of talking between computers. Standardized protocols let your mobile phone request a Web page from a supercomputer across the ocean — they're both speaking the same language.

When the Internet as we know it began, it ran a protocol called IP — the Internet Protocol — Version 4. Guess what version we're running 30 years later? That's right, Version 4.

IPv4 works great, but the problem is that it wasn't designed to be used as much. The addresses used in the protocol, which identify the sender and the recipient of the packet, are only 32 bits long, which roughly works out to be a number between 0 and 4 billion.

Therefore, you could have 4 billion hosts on the Internet. However, various rules governing how hosts get laid out and how stuff works together bring that number down significantly.

With something like 6 billion people in the world, cell phones, and multiple computers per house, a lot of pressure is placed on those 4 billion addresses. It's not possible to make the address field bigger, so something has to be done.

The smart people that keep the Internet going managed to tweak the way the protocol works to extend the life of the addresses. One of these ways is the use of private addresses like 192.168.1.1 that you see in your home network. Private addressing has done a remarkable job of extending the time before all the IPv4 addresses are depleted. The so-called "death of the IPv4 Internet" has been predicted for years, and somehow we always make it through another year.

In the early 1990s work was started on the next-generation IPv4, which was eventually called IPv6 (IPv5 is something completely different and isn't used). Windows Vista supports IPv6, but chances are your service provider doesn't, nor do most of the Web sites you want to go to. So for now, don't worry that your IPv6 network doesn't work.

Even though Vista thinks you have Internet access, you want to verify this yourself. Click that Details button at the bottom of the window to see the network details shown in Figure 4-3.

There are a few important numbers here:

- **IPv4 IP Address:** Your Internet address
- **IPv4 Default Gateway:** Where you send all your packets to in order to get onto the Internet
- **IPv4 DNS Server:** The machine that takes care of resolving names like http://www.dummies.com to the IP address of the machine

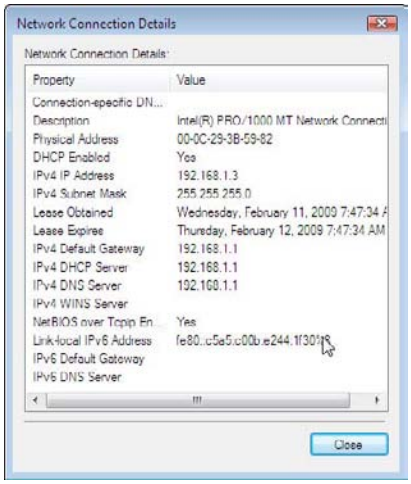


Figure 4-3: Network connection details.

Your IP address probably starts with 192.168, but don't fret if it doesn't. However, if it begins with 169.254, then you've got a problem.

169.254.x.x is called the DHCP Autoconfigure Network. If a computer isn't given a proper address by the network, then it makes up an address in the 169.254 space. An address like this is a sure sign that your computer can't find its DHCP server.

If you're getting one of these addresses, then the problem is between you and your ISP. Begin by rebooting your wireless router and then your computer. If that doesn't solve the problem, refer back to Book II, Chapter 8 for instructions on how to troubleshoot your computer and wireless network.

Pinging Around

Underwater sonar relies on measuring sounds to determine where an object is and what it looks like. Active sonar generates sounds and measures the reflections that come back.

The Internet has its own version of a sonar ping called the ICMP Echo Request (ICMP being the Internet Control Message Protocol, which is like the traffic signals of the Internet). If you want to see if a host is alive, you send it an echo request. If it responds with an echo reply, then you know the host is there.

Of course, no one goes around saying "I'm going to send an ICMP Echo Request to that host and see if it comes back"; they say, "I'm going to ping that host." Unsurprisingly, the command to initiate these tests is called *ping*.

Your host generally responds to pings automatically unless this feature is disabled or blocked.

Be careful about relying on negative ping results. If a ping doesn't come back, then it's possible that the site is down or that the pings are being blocked somewhere. It's a fairly common (but not terribly effective) security policy to block ping requests going to servers.

Ping is a command line tool, which means it doesn't have a point-and-click interface. But don't worry, it's easy to use.

Getting to the command line

The first step is to open up a command prompt (sometimes called a shell, DOS prompt, or command line).

Choose Start➪All Programs➪Accessories➪Command Prompt.

You are rewarded with a black window, like the one you see in Figure 4-4.

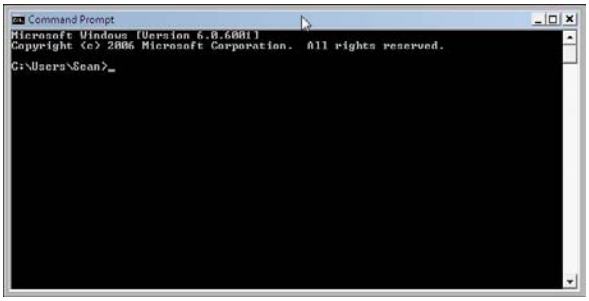


Figure 4-4: The command prompt.

This window is the command prompt. Way back when, you used to interact with a computer by typing in commands rather than using a mouse. Things have changed since then, but Windows maintains a command line for the benefit of people managing the computer and troubleshooting.

Pinging your default gateway

The first order of business is to make sure that you can ping your gateway. You know the gateway's address from when you looked at the network connection details earlier.

Simply type **ping** followed by the IP address of the gateway, separating the two with a space. Then press enter. You should see something like Figure 4-5.

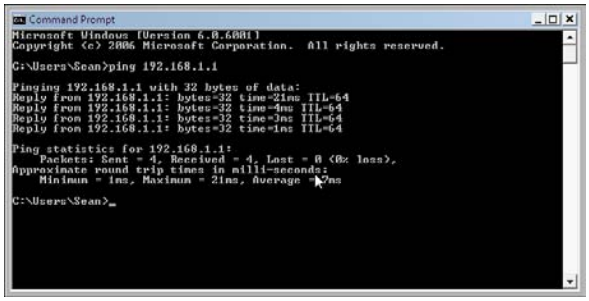


Figure 4-5: A successful ping of the gateway.

By default, the ping command tries four times and reports on the status of each one. In Figure 4-5, you can see that all four tries are reported as successful because the ping program indicated that the replies were received. The bytes and TTL (time to live) are uninteresting now, but the time field tells you how long each ping took from the time the request was issued to the time it was received. The first ping took 21 milliseconds, and the rest took 4 ms or less. It is normal that the first one takes longer.

If you lose some or all of the pings, you see a message like the one in Figure 4-6.

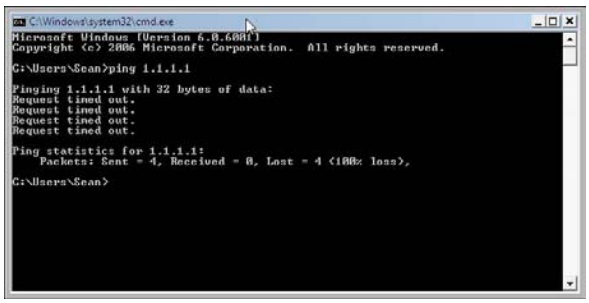


Figure 4-6: An unsuccessful ping.

"Request timed out" means that no response came in the allotted time, which is usually 2 seconds. Most sites on the Internet are within 350 ms of you, so 2 seconds is almost like forever! Because you're pinging the gateway, you should expect less than 10 ms, except possibly for the first response.

If you receive a few replies and a few timeouts, that's usually a sign of packet loss. Losing a few packets here and there is normal, but again, if this is the gateway, then you might have interference and should go back to Book II, Chapter 8 for instructions on troubleshooting interference.

Pinging your Web site

Now that you've got this magical tool that can tell you whether or not a computer is alive, you can apply this to test if your Web site is there or not.

Ping only verifies that the computer is there; it doesn't check to see if the Web site works.

When pinging a Web site, ping only the name of the Web site. For example, with `www.dummies.com/some/page.html`, the name of the server is `www.dummies.com`. The http:// says that the address describes a Web page, and everything between that and the first slash (/) is the server name. The rest, including that first slash, is the path to the file. In this case, it's /some/page.html.

Behind the scenes, ping is going to translate `www.dummies.com` into an IP address. If it is unable to do so, then you will get the error message shown in Figure 4-7.

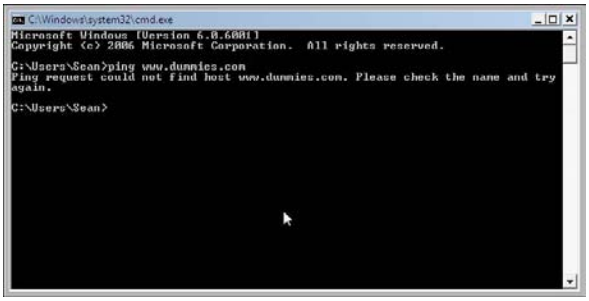


Figure 4-7: Ping is unable to resolve www.dummies.com.

Both Figure 4-6 and Figure 4-7 show unsuccessful pings, but they were unsuccessful for two different reasons.

Although the pings that timed out knew the destination address, they just never came back. When ping couldn't find `www.dummies.com`, that meant that it had no idea who to send the pings to.

If you get the second error about the hostname, then it means you've either typed in the hostname wrong or you're having a problem with your DNS server.

DNS, the domain name system, resolves names like `http://www.dummies.com` to an IP address that your computer can communicate with. If that link isn't made, then you're not going to be able to reach the Web page.

Assuming that you can ping your gateway, you should reset your ADSL or cable modem and then your wireless router. Doing this resets the path between you and the name server.

If the name resolution is successful, you either get your replies back or you won't. If you get your replies back, then you know you can reach the other side. If not, it's possible that the site is blocking the pings, or they might really be down.

If you don't receive any replies to your ping, try a couple of other Web sites to see if the situation is more widespread.

Tracing the route

The Internet is made up of big, expensive computers called *routers*, and their sole purpose is to send your traffic to an adjacent router that's one step closer to your destination. Therefore, you're sending your data to your ISP's edge router, who will forward that inside their core, probably to another provider, and so forth, until it's time to send the response back the other way.

You can trace the path to your Web site to see how far along the path you get. Keep in mind that these traces are meant to be read by network engineers, but you can still get an idea if the problem is close to you or not.

Use the curiously named *tracert* command to trace the route. You must also specify the name or address of the site to trace.

Why not *traceroute*? If you were on pretty much any system other than Microsoft Windows, you would use *traceroute*. But way back in the old days, Windows only allowed file names to be eight characters long. That requirement has long been eliminated, but you still see a few commands with slimmed-down file names.

The first example is a site that successfully works. Figure 4-8 shows the path from my home to `www.unpluggedandonline.com`, a site by the author about consumer wireless.

The first hop is 192.168.1.1, which is the wireless router, and then to the wireless router's default gateway. Hops 3, 4, and 5 have names (on the right) ending in shawcable.net, which is my Internet service provider. The traffic is then handed off to ThePlanet, which is another service provider. The final hop, number 11, is the Web server itself.

The trace completed successfully, which means we know there is end-to-end connectivity. We could have just used *ping* to find the same information, but *tracert* gives the whole path. The numbers on the left give the cumulative

latency (maximum, average, and minimum) up to and including the particular hop. Between hops 3 and 4, you can see latency takes a jump, presumably because it is a long haul link from my city to the coast.

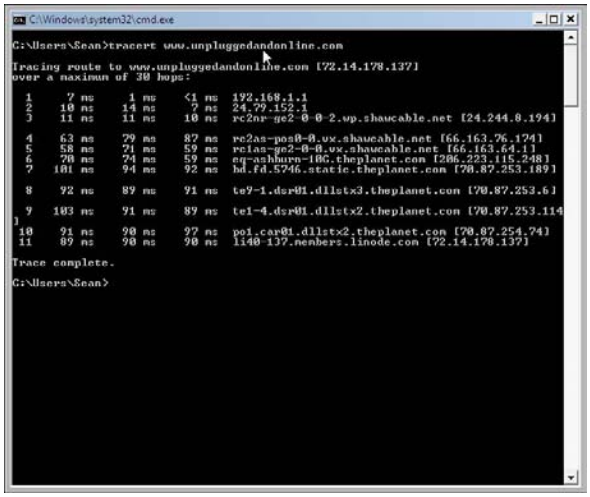


Figure 4-8: Tracing the route to www.unpluggedandonline.com

Remember earlier that site that could not be pinged? Figure 4-9 shows a trace route to it.

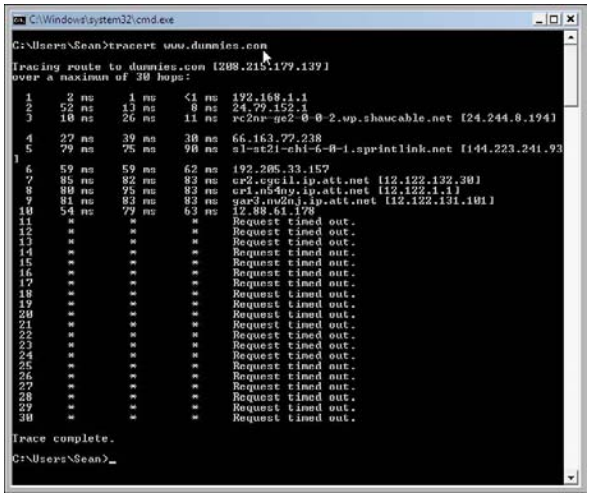


Figure 4-9: Tracing the route to `www.dummies.com`

The trace starts the same and then diverges at hop 3. Hop 11 claims that the request timed out, which is the same response that *ping* gave. *Tracert* will look for up to 30 hops, so the rest of the path is more timeouts.

Even though the *tracert* failed, you can conclude that the packets are getting out of your Internet service provider and out onto the Internet. Any problems are likely going to be out of the control of your service provider.

The names on the right generally give some idea of where that hop is. For the path to `www.unpluggedandonline.com`, the path was probably going East to Asburn, Virginia, then to Dallas, Texas, where the server is located. www.dummies.com seems to be going Chicago to New York to New Jersey. It's entirely possible that you might see paths crisscrossing the country.

Figure 4-10 shows a trace to an address that dies right after hop 2. This is generally the point where all the subscribers are collected into the ISP core network, so for the trace to die here indicates your provider is stopping something.

In this case, it turns out the address being traced is unknown.

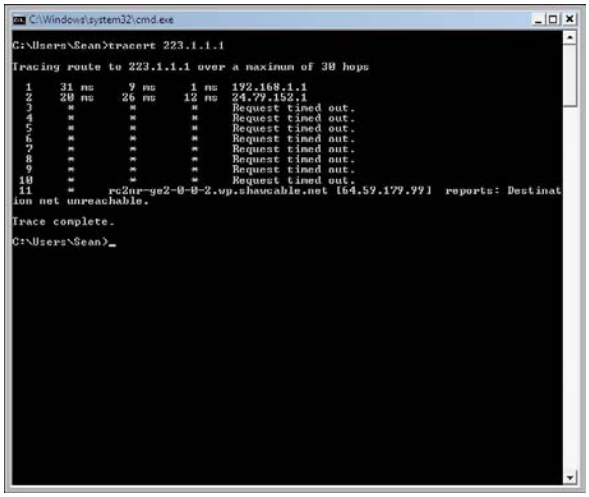


Figure 4-10: The traceroute dies very quickly.

The final pattern you see is called a *routing loop*. The trace bounces between the same few hops until the trace times out. This occurrence is rare; if you see it you should just wait for it to clear itself out.

Finding Out if Other People Are Having Problems

I've suggested earlier that one way to check if a Web site is really down is to ask someone else. If you can't get to it, and they can't get to it, chances are the problem lies closer to the Web site than it does for you (for this to work, the other person should really be in a different house).

That said, it's somewhat intrusive to keep on asking someone to check a Web site for you whenever you have a problem. That's why I really like `http://downforeveryoneorjustme.com`. This is a Web site where you can type in the name of another Web site, and it'll happily tell you if it can reach the site or not.

Figure 4-11 shows `http://downforeveryoneorjustme.com` loaded, with `www.dummies.com` typed into the input field.

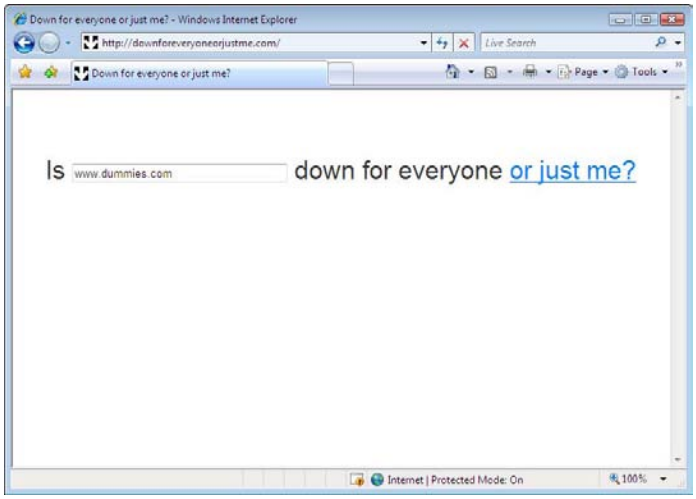


Figure 4-11: http://downforeveryoneorjustme.com about to check a site.

Press the Enter key to check your Web site. Figure 4-12 shows that `www.dummies.com` was up when the Web site checked it, so the problem must be on my end.

However, if you check a site that is actually down, you get a different message shown in Figure 4-13.

When using this service, you can get reliable results without having to bother your friends!

Figure 4-12: Dummies.com is up.

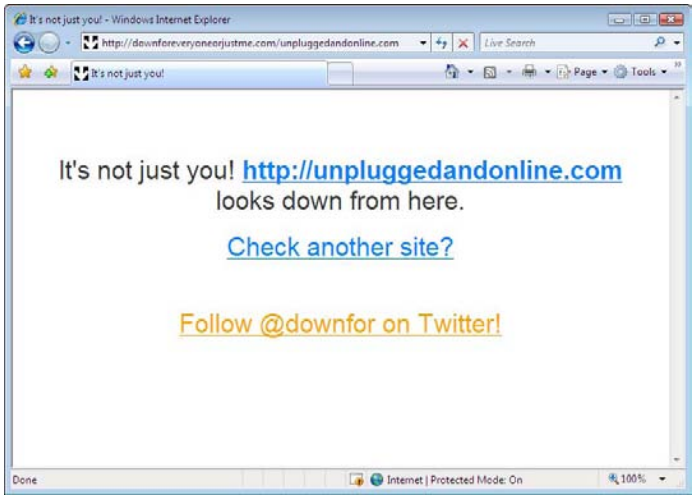


Figure 4-13: unplugged andonline.com is down.

Getting Information About a Web Site

Have you ever wanted to contact the owner of a Web site, but couldn't find out whom to call or e-mail? Maybe you're trying to get more information about a product, or get in touch with the owner of a Web page. Sometimes it's hard to get someone on the phone.

I've got two ways for you to find a name.

Using a search engine

Search engines are huge farms of computers that comb the Web and keep track of what's out there. When you need to find something, the search engine looks in its index of Web pages and pulls out what you're looking for.

Most people go to a search engine and type in query phrases such as "real estate agent," which tells the search engine to find all the pages that are about real estate agents. Search engines also support some other ways of querying them that let you be more specific.

One of these ways is to use the *site* operator, which limits your search to a given Web site. You then look within the site for common strings like "contact us" or "e-mail."

Most search engines support the site operator, which is simply the word site, followed by a colon (:), then the name of the web site you're looking for. To look for the phrase "contact us" on the dummies.com Web site, you would search for site:dummies.com contact us, as shown in Figure 4-14.

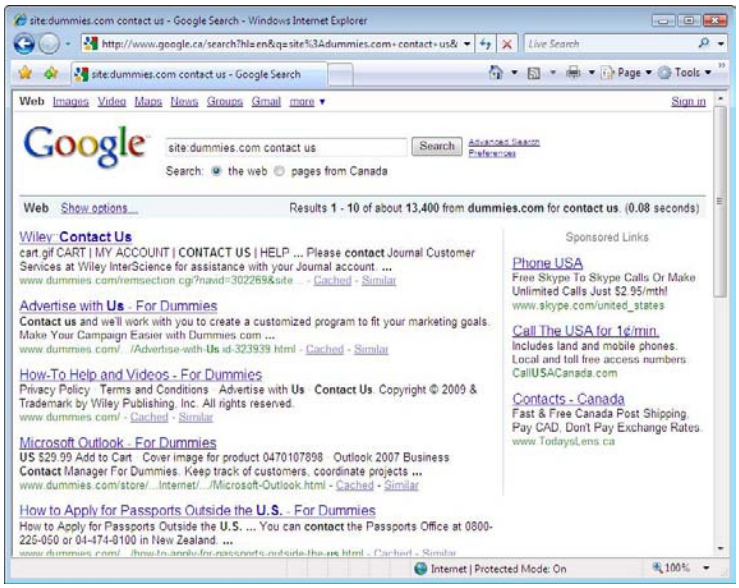


Figure 4-14: A Web search for site: Dummies.com contact us.

Fortunately for me, the first result was the one I was looking for. Sometimes you have to try some of the other results or try a variant of "contact us," but if the page exists on the Web site, you'll find it.

This technique is also good for finding other information. If you were to search for "site:dummies.com wireless all in one," you would see all the results for this book on the Dummies.com Web site.

Checking the domain registration

If you were to get a domain name of your own (as opposed to using space on someone else's), then you'd have to register the name. The registration process requires that you give some contact information, which is stored in a public registry. People can query this registry, called the *Whois database,* in order to find out how to contact the owner of a domain.

Depending on the company that owns the domain, the name you get back might be a generic phone number or it might be the owner of the company. Most larger companies will register as a generic entity like "Name registrations," but the e-mail address and phone number will go to a real person. This prevents the company from having to update all their domains when people change jobs.

That's no problem, because half the battle is finding a living, breathing, human being to talk to. After you've got someone on the line, a few kind words should get you the person you're looking for.

Figure 4-15 shows the front page of http://dnstools.com, which is a site that automates the lookup of a domain's owner. Browse to the site and enter the name of the domain you want to search. You can see that I've already filled out "dummies.com" and have made sure that the *Whois (Domain Name)* check box is checked.

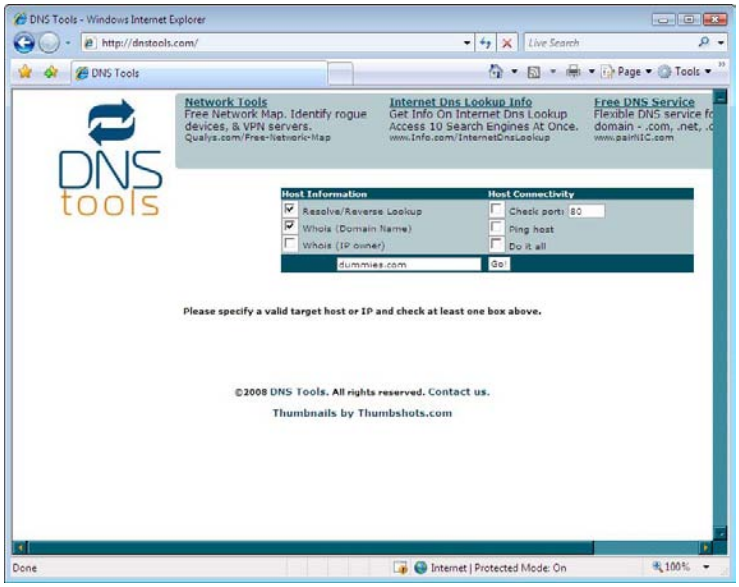


Figure 4-15: Searching for the owner of Dummies.com.

When you click the Go! button, you are given the registration information for the domain. You usually get several names back:

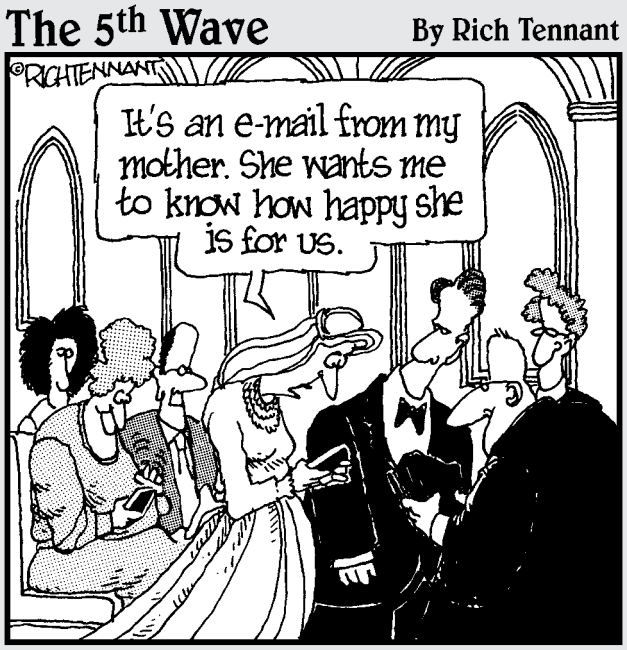
- **Technical contact:** This is the person you're supposed to call with technical problems about the name, so it usually leads to the company's IT department.
- **Billing contact:** This is usually the accounts payable team. "Billing" refers to who pays the bills for the cost of the domain registration and not about customer billing.
- **Administrative contact:** This is a generic business contact.

If you don't see all of these, don't fret. Sometimes, companies combine several of the roles into one contact record. Doing this makes it easier for you, as there are fewer people you have to try!

When contacting these people, explain how you found their name and what it is you're looking for. Chances are this person won't be the exact person you need, so try to get them to put you in touch with the person you do want to talk to.

Book V

On the Road Again — But Without Wires



Contents at a Glance

Chapter 1: Putting a Network in Your Lap (top)

In This Chapter

- **Installing and using a wireless card**
- **Power backup on the road**
- **Printing while on the road**
- **Feeling at home**

If you think of the network as only being something that you have in your home, you're missing an awful lot. Having the ability to connect your laptop PC to a network opens up whole new worlds for you. A networked laptop PC not only shares files on your home network, but connecting a networked laptop PC is also far easier while you're on the road. In this chapter, you read about a number of options that make your life on the road with a laptop a lot more convenient.

In many ways, a networked laptop PC is identical in operation to a networked desktop PC. Topics such as network security, user accounts, and basic network setup, covered earlier, also apply to a networked laptop PC. Therefore, this chapter concentrates on topics that are specific to your laptop PC and its use while you're away from home.

Discovering Your Options for Wire-Free Access

Connecting on the road is not necessarily the same thing as connecting at home. You have different options that might work better in some circumstances than in others. To some extent, the options that are best for you depend on a number of factors that you have to weigh carefully.

Before choosing your on-the-road connection options, you should ask yourself a number of questions:

- Do I need to be able to connect wherever I am?
- How important is my connection speed?
- Do I need real-time Internet access?
- What is my budget?

The following sections take a look at a number of options that are based on your answers to these questions.

Choosing the expensive option

Wireless data plans sure have come a long way over the years. With the arrival of 3G and 3G+ in the United States and in Europe, wireless broadband cards for PCs are all the rage. Most often this means setting up an account with a provider, such as AT&T Wireless, Sprint, or Verizon Wireless. With this type of service you can connect wherever there's network service — almost any urban/suburban area and even in rural areas. If you need to get broadband service from the top of a mountain in the heart of the Rockies, then perhaps you need to learn what vacation is all about.

Each network provider offers a similar plan, but you should definitely do your homework and make sure that you pick a provider that's right for you. You should research things like equipment compatibility with your machine, network coverage, and terms of the contract. As with most things in life, the devil is in the details.

What makes this type of connection more expensive than most other options is the service contract that you have to sign with the service provider. Not only do you get the oppressive service contract, but you might also be stuck with a rather high monthly rate and potentially limited service. For example, you may have download restrictions, in order to prevent network saturation, or your monthly fee may go up, depending on your bandwidth usage. Even though you might not think that you download a lot of data, if you enjoy streaming video or audio, then you likely use more than you think! Also, you're likely to spend a monthly fee compatible to the price of a mobile phone subscription. Therefore, if you don't end up using your wireless broadband card much one month, your price per megabyte becomes quite costly!

This option is good for road warriors, but it's really not a viable option for a full-time home solution. You'll want to enjoy the benefits of a traditional high-speed internet connection, which is still much, much faster than the speeds offered over wireless internet broadband.

Choosing somewhat limited option

If connection speed is the factor that's most important, you probably need to consider a solution that trades off long range to provide higher speed. In this case, a Wi-Fi connection is probably your best option.

Wi-Fi hotspots are pretty easy to find, especially in most large cities. Coffee shops, fast food restaurants, hotels, and even quick print shops offer access. In some cases this access is free, while in others you have to pay a small fee.

Many mobile phone providers also offer hotspot coverage on their network on a monthly or per-use basis. This option is good for those who travel occasionally or work at coffee houses.

If you have a home network, you probably already have all of the equipment you need to connect to a Wi-Fi hotspot. You know that this type of connection provides speed, but that the signal only travels a limited distance. You can't, for example, generally expect to connect several miles away from the hotspot.

Choosing the gimme-it-all option

Okay, I can hear you saying, "I want it all." In other words, you want to connect wherever you are and you want high speed, but you don't want to spend a lot of money.

I wish I could offer that option. What I can offer you is the good news that wireless is now a widely embraced technology in the United States, which means it's hard to go someplace and not have a wireless connection within earshot, or phone/computer shot.

Many of these services are free, but some still require some sort of payment. Most travel-oriented places, such as hotels, airports, and convention centers, offer free Wi-Fi connections to customers. Eventually, we should get to a point where free connection is always available, even if it isn't always the best option.

Getting Carded

Installing and using your wireless card is very similar to installing and using any other PC Card in your laptop. The process consists of three main steps, but the order of those steps depends on a number of factors. The steps (in no particular order) follow:

- Install the necessary driver software in your laptop PC.
- Insert the card into the slot on the side of your laptop.
- Configure your laptop for the selected service.

Reading the user manual that came with your wireless card is extremely important. That manual tells you the correct order for performing the installation steps, and the order is often dependent on the operating system version that's installed on your laptop. That is, you may have to install the software drivers first on some operating system versions, and you may have to insert the card first on others — and this is for the exact same wireless card!

No matter what type of wireless card you use, you can greatly extend the battery life in your laptop PC by either turning the card off or removing it when it is not in use.

Using a wireless data card

If you've ever bought a mobile phone, you're probably aware that each device that uses the network has to be activated before it can be used. Buying a wireless data card and installing it into your laptop is only the first part of the task.

Although different mobile carriers follow different procedures, generally once you sign up for service you have to provide the unit ID for your wireless card to the carrier, who activates the card. As is the case with cell phones, the activation is specific to a particular unit ID, and this means that if you replace the wireless card, you need to cancel the old activation and then activate the new wireless card.

Wireless data providers offer a broad range of service plans (just as they do for voice service). In general, though, you sign up for either a specific amount of monthly data transfer or a specific amount of connect time. Running over your allocation can become quite expensive, so it's important to not only sign up for the correct plan but also to monitor your usage to ensure that you don't run up huge overage charges. Of course, any provider worth its salt also offers unlimited plans at a robust price.

Depending on the network that you're connecting to, you'll likely find that the wireless cellular data card functions much like a dial-up modem, only without wires. That is, you'll use a small application (provided by your service provider) to connect to the cellular network as needed and then disconnect once you no longer need the connection. These days, most wireless data cards are USB, so plug-and-play technology means that you're up and running in no time.

Using a wireless network card

Using a wireless network card in your laptop is really the same thing as using your wireless home network on any of your PCs. The primary difference with a laptop PC is that it's portable, and this enables you to take your laptop places where you can connect to other networks besides your home network. In fact, this means that the whole world of Wi-Fi hotspots becomes available to your wireless networked laptop PC.

Before you buy a wireless network card for your laptop PC, remember that many laptops now come with a wireless network adapter built in. Also, Windows Vista has quite capable wireless networking features built in, so you probably don't need to rely on additional applications to help you locate

Wi-Fi hotspots. In fact, you're not likely to find many laptop PCs made within the past couple of years that don't already have a sufficient network card already built in. However, if you are using a laptop PC that is older, it is possible that it might not have an integrated network card, or even more likely, it might not be compatible with today's more advanced wireless protocols.

You may have read about wireless security in previous chapters. Wireless security when you're on the road with your laptop PC can be somewhat of a mixed bag: Some Wi-Fi hotspots are wide open, and others use the full range of available security features. In some cases you may be given a username and password that function for a limited period of time, or you may need to enter a security key to match that in use by the access point.

Even when you have all of the information that you need, making the connection can sometimes be a bit difficult — especially if you need to enter the WEP or WPA security keys, because the configuration methods for wireless network cards can be rather confusing. In the past, a third-party application may have proved helpful in managing your wireless networks on your laptop PC. However, Microsoft has gotten their act together, and Windows Vista offers a wonderful Manage Wireless Network window, as shown in Figure 1-1.

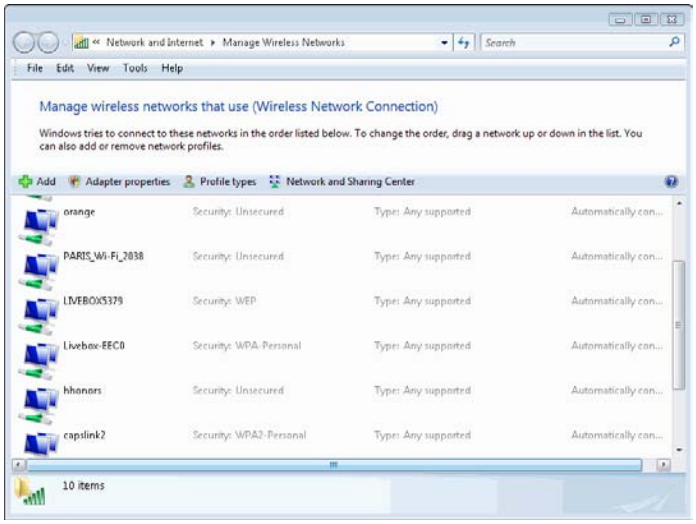


Figure 1-1: The Manage Wireless Network window helps you keep track of all those hotspots.

Not only does it remember all those routers to which you've connected over time, but it remember vital connection information, such a security keys, and keeps a pecking order, so that you always connect to the right network and the right time.

Getting Out and About

Laptop PCs are made for travel, but that doesn't mean life on the road is always easy. After all, a lot can go wrong — especially if you're depending on your laptop to help you do business or even just keep you from becoming lost in some strange locale.

I won't bore you by repeating a bunch of pretty obvious information, such as how attractive laptop PCs are to thieves. Rather, look at some topics that can help you get more use from your laptop while you're on that road trip.

Finding Wi-Fi hotspots

Because this book's focus is on wireless topics, it makes sense to begin the discussion on traveling with a laptop PC with the subject of finding Wi-Fi hotspots. Quite simply, Wi-Fi hotspots are likely your primary means of connecting to the Internet and for sending and receiving e-mail.

A number of Web sites have lists of Wi-Fi hotspots. A quick Google search produces hundreds of hits. Some of these sites are better than others, but none of them are up-to-date enough to be your single source of information. Most of these sites depend on information supplied by volunteers, although some use lists of hotspot providers that are in some way affiliated with the site. Still, the lists do give you a starting point.

If you're going on a road trip you may want to print out a couple of hotspot lists for your destination before you set out. That way, you have some idea of where to begin looking for an Internet connection.

Once you're in the general area of a Wi-Fi hotspot, you have several choices for locating a usable signal:

- Break out your laptop PC and see if the built-in software can find the Wi-Fi signal and allow you to connect.
- Fire up your laptop and use a program or feature like Manage Wireless Network window (as mentioned earlier in this chapter) to locate any nearby Wi-Fi signals and then to make a connection to one of them.
- Visit a Web site, such as `www.thegobutton.com`, and download a Wi-Fi finder. This quickly finds any free hotspots for you to connect or shows you the strongest ones available.

Of these three options, they are all equally good. Again, it comes down to a question of personal preference. There are some users who prefer using the out-of-the-box solutions that Microsoft provides. Other users may feel more

comfortable using a third-party application, such as the Go Button, as shown in Figure 1-2. At the end of the day, these options all provide the same services, even if they don't always follow the same path to get there.

Figure 1-2: The Go Button quickly finds the availability and strength of Wi-Fi signals.

Power backup on the road

Although not strictly a wireless issue, keeping your laptop powered while you're on the road can be a challenge. Even the most power-stingy laptops don't last through a full day of constant use on battery power, and if you've opted for one of the more power-hungry units, you are lucky to get more than about two hours on a full charge.

When you're traveling, the weight of all of your equipment can become a real issue. It seems like the longer the trip, the heavier all of those separate little power adapters and cables seem. Sure, each one might weigh just a few ounces, but when you're dragging everything down a long airport concourse to the farthest gate, that can feel like pounds.

One way to cut down on your travel weight is to buy a single power supply that works with all of your portable devices and with the power outlets in your hotel, your rental car, or in an airplane. While it's true that the manufacturer of your laptop probably doesn't offer such a great power supply solution, some companies do. For example, iGo Mobility Electronics, Inc. (`www.igo.com`) has just such a product. You can see it in Figure 1-3.

If you're really going out to get away from it all (but can't quite give up on your laptop), you might want something like the Notebook Solar Laptop Computer Charger from Sierra Solar Systems (`www.sierrasolar.com/manufacturers.php?manufacturer_id=144`) shown in Figure 1-4. This

handy unit can charge other devices like your cell phone when it isn't powering your laptop and does good things for the planet by using solar power, too.

You may find that the higher-capacity solar charger is a good investment because it charges your laptop's battery faster.

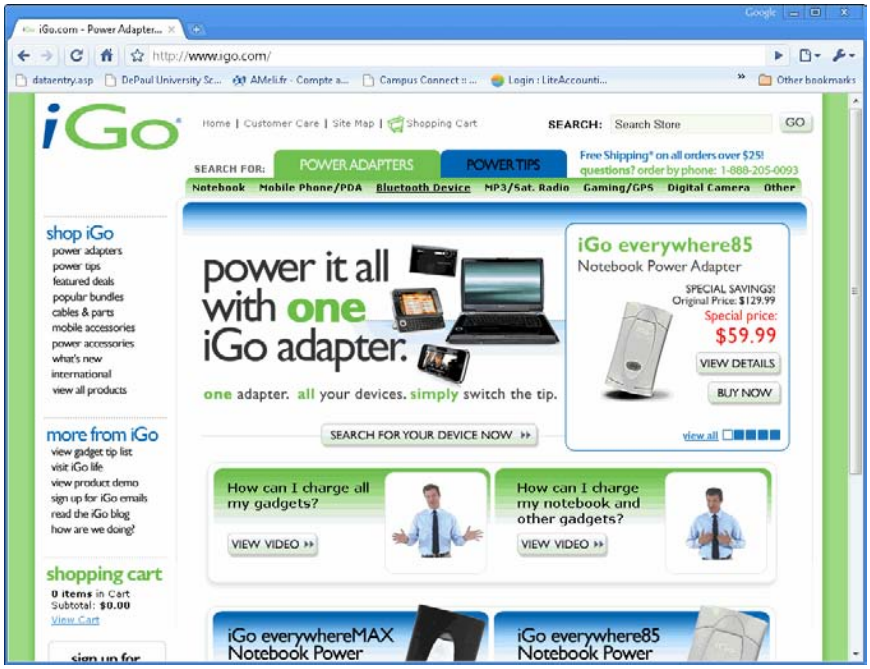


Figure 1-3: The iGo Web site offers power solutions that every road warrior needs.

Figure 1-4: Power your laptop from the sun and you never worry about finding an outlet.

Printing while on the road

Some years ago when e-mail was first becoming popular, a number of pundits predicted that we were rapidly moving toward the "paperless office" of the future. It probably would have been a good idea to invest in the stocks of paper companies at that time, because it's pretty clear that we're a long way from eliminating paper.

When you're on the road, it can be difficult to find a convenient way to print those documents that simply can't wait until you get back home. Sometimes there simply is no choice — you have to get a printout.

Carrying your own printer

There are those who like to carry their own printer with them on the road. Personally, I think it's a great idea weighed down by reality. Even the most travel-compatible personal printers still require space in my travel bag.

If you do opt to bring along a printer, you shouldn't expect the sort of print speed or paper-handling capabilities in a portable printer that you take for granted with a desktop printer, but then I really don't want to try packing along my HP Color LaserJet on a trip, either.

The available models are always changing, but you can find a quick list of what's available on Amazon.com and by searching for "small travel printers." It's hard to stay one step ahead of technology, where new hardware is always becoming smaller, cheaper, and offering better performance.

For true road warriors, you are better served by using the print services that are available in your hotel.

Using a printing service

Another on-the-road printing option you may want to consider is a printing service such as PrintMe (`www.printme.com`). This service is available at some Wi-Fi hotspots, and it enables you to print to a printer at the hotspot without loading any printer drivers.

If a FedEx Kinko's print shop is nearby, you may find their printing service pretty handy, too. See `www.fedex.com/us/officeprint/main/index.html` for more information on getting signed up for this service.

Printing using a USB key

Any office you visit probably has a printer you could use if only you had a way to get your document to that printer. Few people are likely to want to open up their network so you can access it, but there's no reason you can't use a little innovative thinking to get around that problem.

One very simple solution is to use a USB memory key such as the SanDisk MiniCruzer (www.sandisk.com), shown in Figure 1-5, to transfer your document to a PC on the network and print it from that PC. You can even open the document directly from the USB memory key so that you aren't storing a copy of the document on the PC connected to the printer.

Figure 1-5: A USB memory key makes it very easy to transfer data between different PCs.

USB memory keys are extremely handy because they enable you to quickly exchange data between different PCs using a very tiny package that easily fits into your pocket. All modern PCs have USB ports, and the USB key simply appears as an additional disk drive. To a great extent. USB keys have replaced floppy disk drives, and they've become very popular because they hold so much more than a diskette and work with any PC.

Faxing: Your last resort

If you can't find any other way to print but absolutely must have a printout of an important document, the desperate have one last resort: sending a fax to a nearby fax machine. True, the quality of the printout probably won't win any awards, but when you're out of options, it pays to be resourceful.

To send a fax, you either need a modem in your laptop PC and access to a phone line or Internet access and an account with an Internet-based fax service, such as eFax (www.efax.com).

Lounging at Home

Thus far this chapter has primarily focused on the mobile uses for a networked laptop PC. However, no law says you can't have a little fun with your

laptop when you're at home. Consider the following ways that having a wireless laptop PC might enhance your home life:

- On a nice, summer afternoon when you're stuck working on a report for that boss who always drops a bomb on you just before the weekend, why not take your laptop out to a shady spot in the backyard and work out there? You still can do your online research, thanks to your wireless Internet connection, and who knows — maybe the fresh air will inspire you.
- If you're having some friends over for a cookout on your deck, take your laptop and a set of speakers out, too. Then you can listen to an Internet radio station and never have to worry about changing CDs on your stereo system.
- It's amazing how much information is available on the Internet these days. If you need to recalibrate your underground sprinkler system, tune up your furnace, or track down the wiring harness layout in your car so that you can add a CD changer, the information is probably online somewhere. If you take your laptop to your job you can view the information onscreen as you work and have easy access in the event you need a bit more detail.
- When you're absolutely out of ideas of what to make for dinner, bring your laptop into the kitchen. With the multitude of cooking-related sites, you can quickly find a whole bunch of ideas for recipes using ingredients you have on hand.

Wireless laptop PCs are awfully handy, whether you're a road warrior or simply want a convenient PC that you can move anywhere in your home without a second thought.

Chapter 2: Connecting Wireless Devices to Networks

In This Chapter

- **Connecting a wireless device**
- **Configuring your network**
- **Using advanced configurations**

It's hard to believe how widespread the use of wireless devices is these days. In fact, not so long ago (try as few as five years ago), you were pretty limited in options. At the time, your options were basically limited to a Pocket PC or Palm personal digital assistant (PDA). If you we're in luck, the device may have had Wireless access but likely few places to actually use it.

Fast-forward a few years to the present and, my, has the world changed! First, the former market leaders barely have a seat at the table anymore. Technology moved quickly and combined the best of both products to create a new series of smartphones. Of course, wireless devices aren't limited to souped-up mobile phones; Apple offers the iTouch, which is basically a smartphone without an actual phone. The current kings are Windows Mobile and Google's new Android operating systems.

Any device that is Internet-driven offers wireless capability. If it doesn't, it's not worth discussing. After all, even printers offer wireless capability these days! Wireless devices offer widespread Wi-Fi connectivity, so that you can connect to your network or a wireless hotspot while at home or on the road. These devices let you truly organize and manage your life, which may be a troubling sign for our future, if you think about it.

In this chapter I talk about connecting both a handheld computer and a functioning router to a wireless network. After you're on the network, you can do just about anything you can on your desktop computer:

- Check your e-mail.
- Surf the Internet (albeit on a much smaller screen).
- Access PC files located on your network. This includes documents, as well as video and music files.

You also can skip the cradle you normally use to synchronize information between your handheld computer and desktop computer. Instead, you can do it over your wireless network.

Want to check your mail but the ballgame is in the ninth inning? No problem, as now you can connect to your network and access your messages (and the scores of other games) while lying on your couch. It's a rough life, and I feel your pain.

Reaching Out to the Wireless World

Connecting your wireless device to a wireless network is very easy. In fact, the wireless connectivity aspect is so important to wireless devices that it's been that device makers minimize your role in connecting to a network. For more devices, connecting to the Internet isn't much different from how you do it with your personal computer.

Here's how you connect your wireless device to a network:

1. **Turn on wireless networking if it's not already enabled.**

   This step is different for each device. Some devices may require you to call up a connectivity-related settings page or perform some sort of key manipulation to turn on your wireless connection. For example, in Figure 2-1, an HTC mobile device simply offers a switch-type button. Alternatively, you can also use Start➪Settings➪Connections➪Wi-Fi and select the check box to enable wireless connectivity.

2. **Select an available hotspot that is detected by your wireless device and validate it.**

3. **Select Internet Explorer or any other Web browser of your choice that is supported and available on your wireless device.**

4. **Browse to a Web page to confirm your wireless connection is working. That's all there is to it.**

When traveling, your mobile device can connect to a Wi-Fi network as easily as Windows Vista can since Windows Mobile and Vista share similar zero-configuration technology. This makes it simple for them to detect and connect to nearby Wi-Fi networks.

This saves you the hassle of configuring your device every time you're in range of a wireless network. Of course, as with Windows Vista, once you connect to a wireless network with your wireless device, most devices will remember the security key (WEP/WPA) so that you can quickly recall a frequently used network. If you connect to a new network, you'll still need to know the security key to connect the first time.

Figure 2-1: The connectivity option.

Using other devices

The first section of this chapter was designed for those of you using Windows Mobile devices. However, accessing your network is just as easy, or sometimes even easier, using other platforms.

For example, if you are using an iPhone, simply access the Settings button on the touch screen and select Wi-Fi. From this page, you can opt whether or not to turn it off. When Wi-Fi is enabled and connected to a network, the standard Wi-Fi connection icon appears on the phone. What's particularly cool about the iPhone is that it always tries to connect to the last connected network. If it can't find it, it will go through its list of known networks until it finds one that works. Otherwise, you can always select the desired network and enter its password (if necessary).

If you're using Android, things can be even easier. If you use Android's Wi-Fi Toggle widget, it's as simple as clicking a button on the phone's toolbar. Otherwise, you have to go through the Settings menu, which is accessible from Home➪Menu➪Settings➪Wireless controls. The Wireless controls page lets you turn on or off your wireless connection.

Manually configuring your network

You can manually configure the wireless network settings if you are using Windows Mobile, which is helpful if the automatic network connection feature is not working or you have some special situation. Here's how you access the configuration settings:

1. **Click the selectivity icon, shown in Figure 2-2, at the top of the screen.**

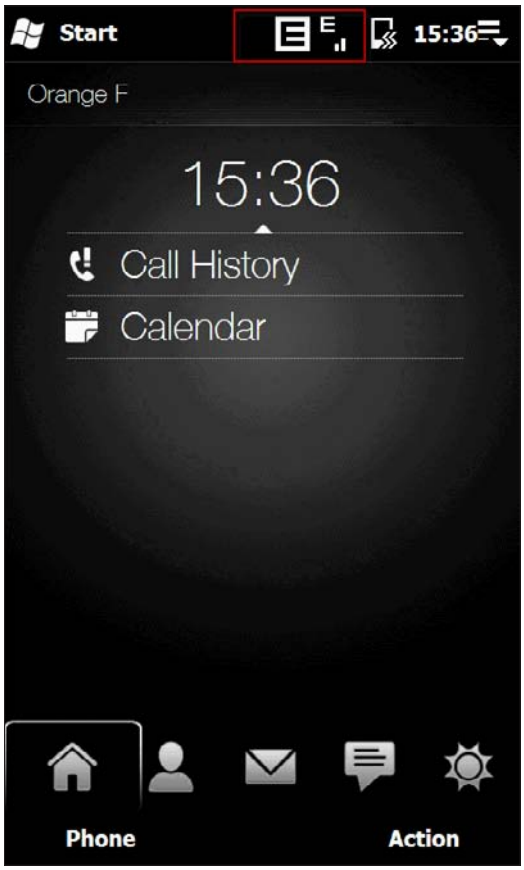


Figure 2-2: The selectivity icon.

A connectivity window appears, as shown in Figure 2-3.

2. **Click Wi-Fi to bring up the wireless network settings.**
3. **Click Settings.**

   The Wi-Fi screen appears, as shown in Figure 2-4.

4. **Click the name of the wireless network to configure. Enter the network key.**

   The current strength of your connection is also indicated, as shown in Figure 2-5.

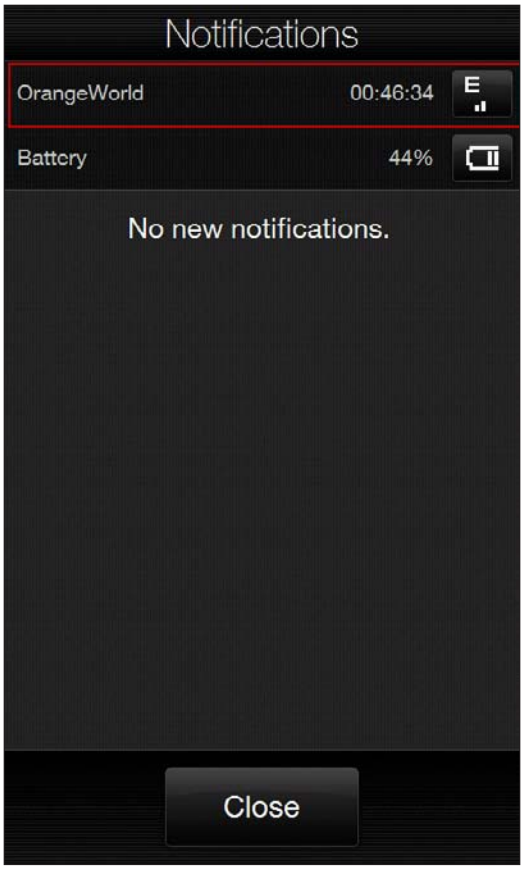


Figure 2-3: The connectivity window.

Figure 2-4: The Wi-Fi screen displays the list of available networks.

You can click Wireless Networks to perform advanced configurations. However, these configurations should only be performed by advanced Windows Mobile and networking users. Most readers of this book will likely not need to use these configurations.

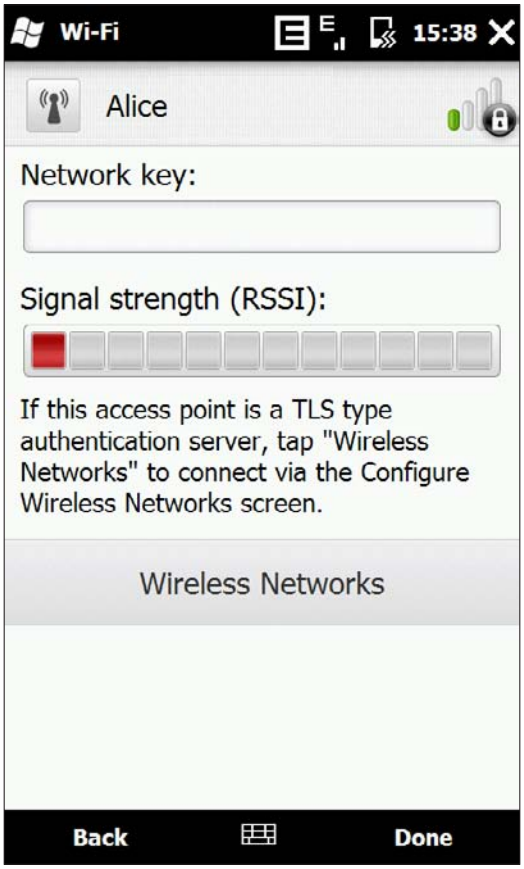


Figure 2-5: The strength of your network connection.

Using Advanced Configuration

If you want to manually add a new wireless network from a Windows Mobile device, you can do so by choosing from the list of wireless networks and selecting Advanced. If you can do this, you are either very patient, have nimble fingers, or surgeon-like accuracy with a stylus.

Go back to of the list of wireless networks, which is accessible from the Wi-Fi settings page. Click Advanced to open the Wireless LAN window, as shown in Figure 2-6.

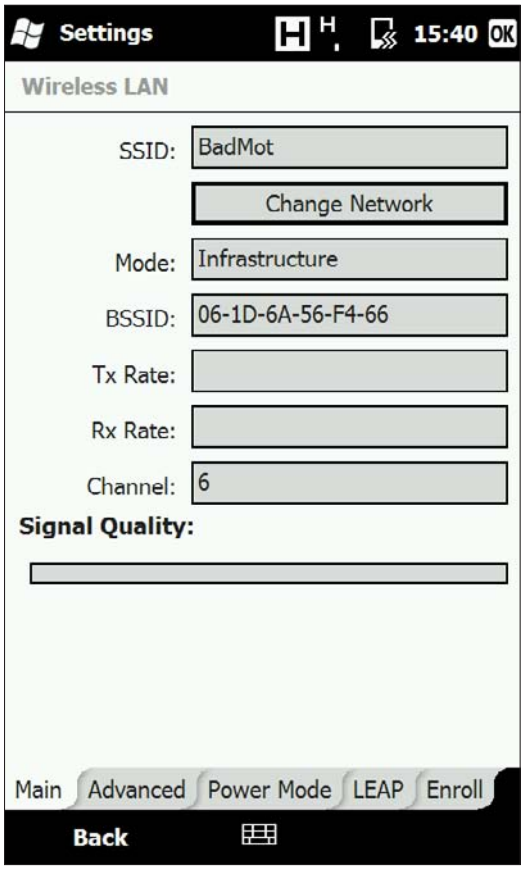


Figure 2-6: The Wireless LAN screen.

Select LEAP from the tabs that appear across the bottom of the window, as shown in Figure 2-7. The Wireless LAN window appears, as in Figure 2-8. Then do the following:

Figure 2-7: Let's add our own wireless network manually in this next procedure.

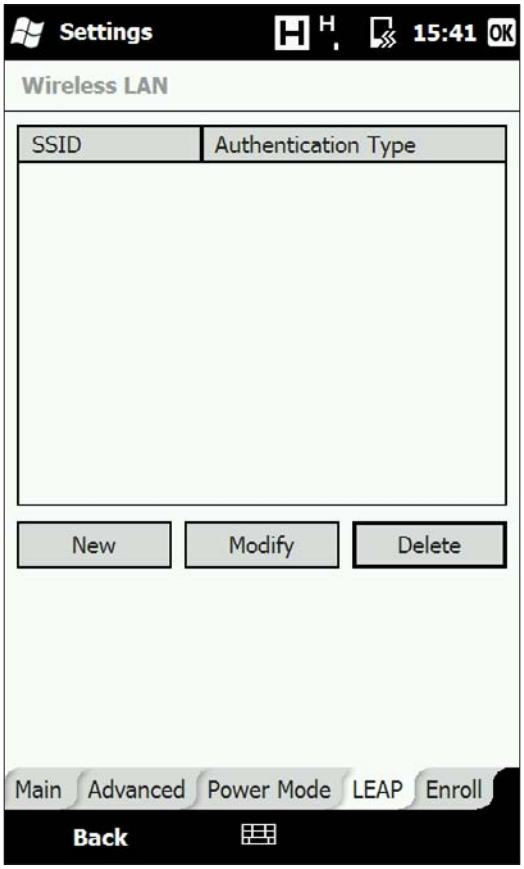


Figure 2-8: The Wireless LAN window is your starting point.

1. **Click New.**

   The Wireless LAN Settings page appears with empty fields.

2. **Add a SSID, domain, username, and password as shown in Figure 2-9.**

3. **Select whether or not the new wireless network should be open (no key) or require authentication.**

   If you want to encrypt (a good idea), select EAP.

4. **Click OK.**

If necessary, refer to your device's manual for troubleshooting tips or contact the manufacturer for help.

Figure 2-9: Enter a SSID and username at the very least.

Chapter 3: Synchronizing Devices over a Network

In This Chapter

- **Synchronizing with Windows Mobile**
- **Synchronizing with other operating systems**
- **Using RSS feeds**

I'm assuming that you've successfully connected your wireless device to your wireless network and are ready for the next step: actually using that wireless link to move data across the network. If you're not there yet, check out Book V, Chapter 2, which provides the instructions for connecting.

In this chapter, I discuss synchronizing your wireless device with information on your desktop PC. Wireless synchronization has made some progress, but it has also taken a few steps back at the same time. While that may sound contradictory, it's very much true. For example, most systems (hello, Symbian and iPhone) don't have any wireless synchronization options available at the time of press. Windows Mobile, on the other hand, does offer a wireless synchronization, but not everyone can use it.

I also tell you how you can add content to your wireless device (such as news and articles) using RSS feeds and your RSS hub. You can update your wireless device using the RSS hub and take reading material when you travel.

Getting Windows Mobile to Coordinate

You can synchronize your wireless device using Windows Mobile with your computer in two ways. You can

- Connect the device to your computer using a USB cable.
- Connect wirelessly and update your device.

If you are running Windows Vista, you will use the Windows Mobile Device Center to synchronize your device with your computer. The version that shipped initially with Windows Visa has been updated, so be sure to update. It's important to make sure you have the most up to date version for compatibility with the most recent wireless devices, which is available at `www.microsoft.com/windowsmobile/en-us/help/synchronize/device-center-download.mspx`.

How often you synch really depends on how often you update your wireless device and computer. Personally, I tend to only sync data such as contacts and appointments, so I only need to sync when I update Outlook. However, I use my wireless or 3G+ connection to update other applications, such as RSS Hub, which I discuss later in this chapter.

Running with Windows Mobile Device Center

Windows Mobile Device Center is the new and improved version of ActiveSync, which went the way of the dodo bird when Windows Vista was released. It has a much more intuitive, graphic-friendly interface that is easy and comfortable to use. The first time you plug your wireless device to your computer running Windows Vista, it automatically opens the Mobile Device Center and configures your device with Windows.

If you still need to start the Windows Mobile Device Center, here's how to do it:

1. **Choose Start➪All Programs.**
2. **Select Windows Mobile Device Center.**

   The application opens and displays the name and a picture of your wireless device, if properly connected, as shown in Figure 3-1. If no device is connected, a generic image of a wireless device is displayed and says "not connected." Your wireless device is automatically synced.
3. **Select Mobile Device Settings.**
4. **Click Connection settings.**

   Make sure that Allow USB connections is selected. If you want to be able to sync wireless using Bluetooth, make sure that the Allow connections to one of the following option is selected with Bluetooth in the drop-down menu.
5. **Click OK.**

Figure 3-1: Your wireless device picked up in Windows Mobile Device Center.

6. **Click Mobile Device Settings.**
7. **Click Change content sync settings.**
8. **Select which content should be synced, as shown in Figure 3-2.**
9. **Click Save.**

Figure 3-2: The Windows Mobile Device Center lets you pick and choose what you want to synchronize.

Running with ActiveSync

You can use Microsoft's ActiveSync software to wirelessly synchronize information between your wireless device and your desktop computer. Usually I don't discuss Windows XP in this book, but since there are enough users still working with this operating system, do keep in mind that you must install Microsoft ActiveSync before you can synchronize your wireless device with information on another computer on your network. You can download the latest version of ActiveSync from `www.microsoft.com/windowsmobile/en-us/downloads/microsoft/activesync-download.mspx`.

Before you can synchronize your wireless device, make sure the settings are correct on the ActiveSync software running on your desktop PC.

Now, let's synchronize:

1. **Click Start⇨All Programs.**
2. **Click Microsoft ActiveSync.**

   The ActiveSync dialog box appears.
3. **Click File.**
4. **Click Mobile Device, if you have more than one device connected or registered with Active Sync.**

   Menu of available wireless devices appears.
5. **Select the wireless device that you want to synchronize, if necessary; otherwise your device appears as shown in Figure 3-3.**

   In this case, there is only one device, and it's called HTC87. (Sometimes even computer stuff is easy to follow.)
6. **Click File.**
7. **Click Connection Settings.**

   The Connection Settings dialog box appears.
8. **Confirm that this choice is selected: Allow Network (Ethernet) and Remote Access Service (RAS) Server Connection with This Desktop Computer.**
9. **Click OK.**

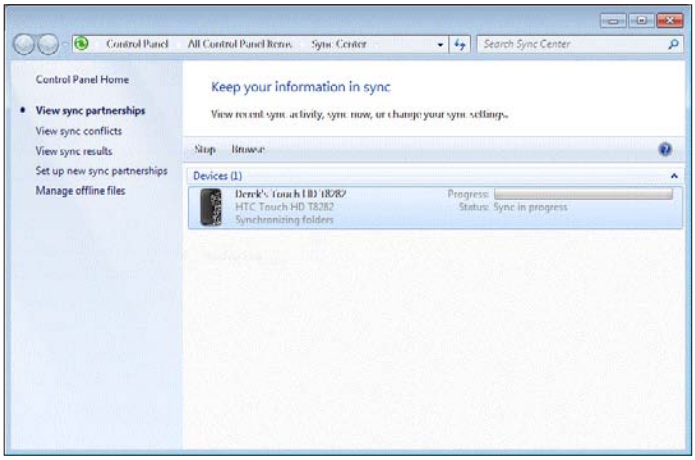


Figure 3-3: The wireless device is ready to synchronize.

Syncing information for your wireless device

Here's how you initiate synchronization from your handheld computer from your wireless device. Be careful, though, this shows you how to initiate the synchronization from your wireless device and not your computer; it doesn't show how to do it on a wireless network. In other words, you need to have a USB connection to do this. Follow these steps:

1. **Choose Start⇨System.**

   The System dialog box appears.

2. **Click ActiveSync.**

   ActiveSync screen appears.

3. **Click Sync.**

   Your wireless device shows Connecting and then Synchronizing, shown in Figure 3-4.

When it's done, the screen displays Not Connected. The ActiveSync software on both your PC and handheld show the last date and time they connected to each other. If the synchronization is not occurring, make sure you have a working wireless connection and that your Pocket PC is close enough to a wireless access point.

Figure 3-4: Windows Mobile synchronizing with desktop PC.

Make sure Microsoft ActiveSync is also running on your desktop PC.

Syncing information wirelessly

You also can synchronize your wireless device by using Bluetooth wireless technology instead of a Wi-Fi connection. Bluetooth works over a much shorter range — about 30 feet — but can be an easier way to connect your handheld to your desktop PC at close distances. In addition, with the introduction of more and more Bluetooth-enabled cellular telephones, it's also a way to synchronize information between your laptop computer and your mobile phone.

Getting Other Platforms to Coordinate

This chapter demonstrates how you can synchronize your wireless device if you are using the Windows Mobile operating system, but it's worth remembering that all mobile device platforms offer this capability as well.

Each platform has its own proprietary software package that allows you to transfer data (e-mails, contacts, files, pictures) between your computer and the wireless device. In most cases, this is done using a USB connection. I recommend using the documentation provided for your wireless device that will certainly show you how to set up synchronization.

Generally speaking, your wireless device ships with a CD-ROM that allows you to install the necessary software on your computer. Once you connect your phone to the computer using USB, your computer automatically launches and recognizes the wireless device.

For example, if you are using a Nokia N95, a suite of applications is provided to let you synchronize your data quickly and easily, as shown in Figure 3-5. Not only do these proprietary applications provide you with synchronization tools, but also additional applications to help you handle other often-used features, such as for photos and music.

If you are using a Palm-based wireless device, such as the Treo, you can use Treo Desktop to synchronize your data, as shown in Figure 3-6. This device is a little more complicated, as it also requires you to have Palm desktop installed, along with a sync user. In other words, you need two separate applications to sync your device!

Figure 3-5: Nokia also allows you to synchronize files, music, and photos.

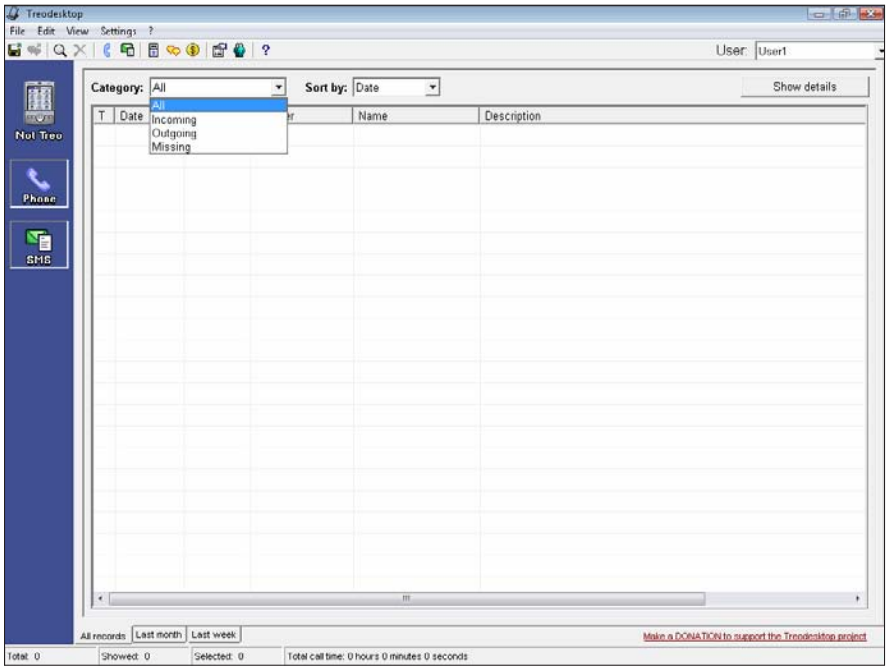


Figure 3-6: For Treo, you need two applications to synchronize data.

If you want to synchronize your device wirelessly, you'll need to make sure that both your computer and the wireless device support Bluetooth technology.

Using RSS Feeds

When wireless devices first became the rage, there was a program called AvantGo that was extremely valuable to users. It allowed you to take reading material when you traveled, or to update the information from your device while you were on the road over a wireless connection and read a miniature version of the newspaper.

Of course, like all good ideas, it became copied and was soon made obsolete by its peers. This is the sad story of AvantGo, which was made redundant and eventually stopped publishing in June 2009. Though there are a number of imitators available to take AvantGo's place, the most useful application for obtaining information on the go is the RSS feed.

This publishing format is a widely used standard for publishing Web content – including blog posts, news articles, and multimedia – as an XML file or feed that

can be read by a reader on your desktop computer or wireless device. Likewise, you can also "subscribe" to RSS feeds on Web sites that allow you to track its content easily from your e-mail client or an RSS reader.

Similar to AvantGo, an RSS reader (such as RSS hub) allows you to select content sources (for example, Yahoo and BBC News) called channels to which you can subscribe. Using your wireless network connection, you can update the channel's content, which is displayed as a list of entries, as shown in Figure 3-7.

By double-clicking the article header, you can obtain the first few lines of the article as shown in Figure 3-8, followed by a link, which can be clicked to display the rest of the article in your device's Web browser.

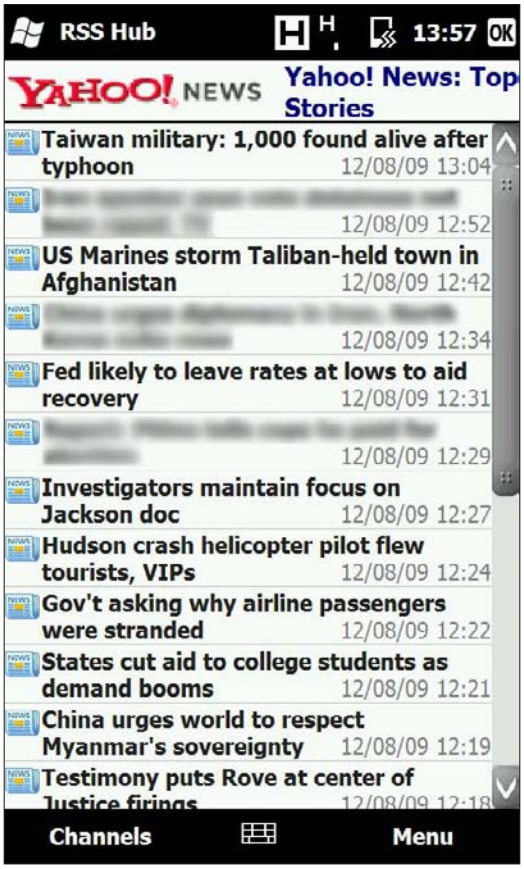


Figure 3-7: Each channel provides a list of its latest content in an easy-to-follow format.

Figure 3-8: An article header saves bandwidth by displaying just a bit of the article.

Using RSS Hub on a wireless device

A number of RSS readers are available for use with wireless devices. Most of them offer a similar group of features; the right one really depends on your personal preferences. I choose to use RSS Hub because it was included on my wireless device and satisfies my requirements for getting information quickly.

To use RSS Hub on Windows Mobile:

1. **Click Start➪Web➪RSS Hub.**

   The program launches and displays All Categories.

2. **Click Refresh to update each channel in the list for the category.**

   If you wish to organize your categories, click Menu➪Categories➪ Menu➪New. You can also use this menu to rename an existing category by clicking it and selected Rename, or to delete it by clicking Delete.

3. **Using your preferred input method, enter a name for the category.**
4. **Click Done.**

   The new category appears in the list of categories.
5. **To change categories, return to the list of channels and click the desired channel.**
6. **Click Menu➪Chanel➪Change Category and select the desired category.**
7. **Click OK.**

   If you sort the list of channels using the drop-down menu, as shown in Figure 3-9, the new category appears.
8. **Select the desired category.**

   The channel now appears in a filtered list.

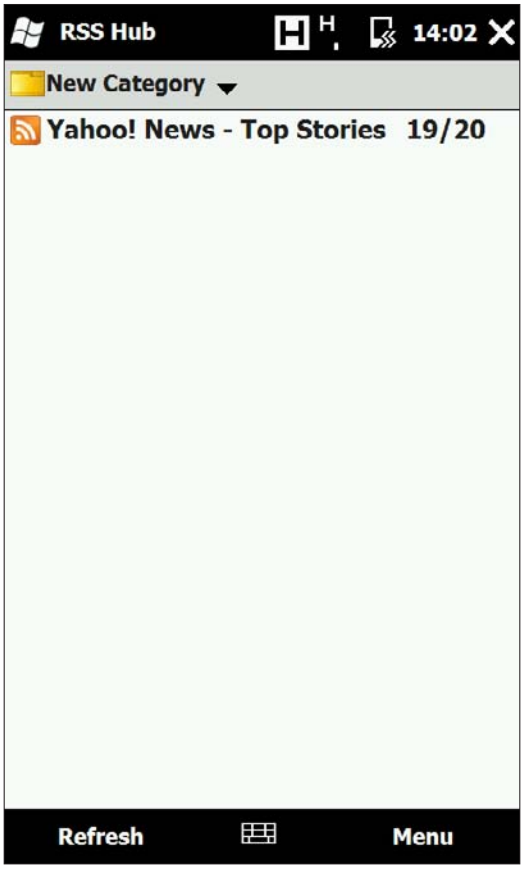


Figure 3-9: Channels can be sorted by category.

To add a new channel to RSS Hub:

1. **Choose Start⇨Web⇨RSS Hub.**

   The program launches and displays All Categories.

2. **Choose Menu⇨Channel⇨New.**

   The New Channel Wizard appears.

3. **Select how you wish to select your new channel.**

   If you do not know the Web address to the channel's RSS feed, you can either search for the channel or choose from a list of known channels. Click Next.

4. **Use the scroll bars to select the channel(s) to select, as shown in Figure 3-10.**

5. **Click Finish.**

   The newly selected channel(s) appear in the list of channels.

If you have an unlimited data plan and have the necessary battery life on your phone, you may want to set RSS Hub's options to auto-update feeds. This is of value if you find that you like to catch up on the news and read RSS feeds regularly. The advantage is that the information is always up to date (you can determine how often it is refreshed), but it can also be a disadvantage. First, if your data plan is not unlimited, you must watch that you do not download too often lest you go over your allotment for the month. Also, every time your mobile device performs a content refresh, it uses battery power. If you need to use your phone frequently during the day and don't have the ability to charge your device until the end of the day, this could waste valuable batter life.

To set auto-update settings, from RSS Hub, do the following:

1. **Choose Menu⇨Options.**

2. **From the Auto Update Mode drop-down, select the desired update cycle.**

3. **Using the next group of drop-down menus, select the frequency for the automatic update.**

Figure 3-10: RSS Hub displays an impressive list of preselected RSS feeds.

4. **Click the Notify tab.**
5. **Select how, or if, you should be notified of new content.**
6. **Click OK.**

   This button is located at the upper-right side of your mobile device, as shown in Figure 3-11.

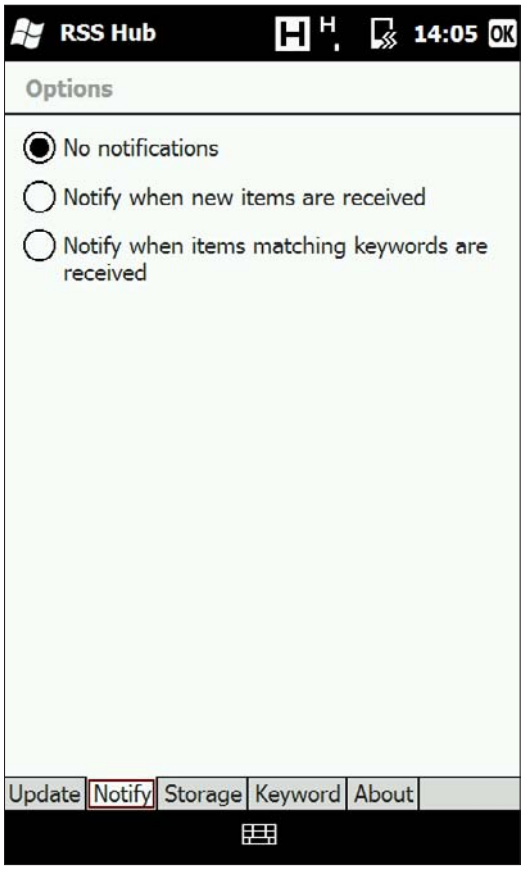


Figure 3-11: Want to validate your changes? Look up, and to the right, while you're at it.

Hopefully, now you have a good idea on how to keep your wireless device up to speed — and in sync with your desktop computer. Having a wireless device that has information, such as e-mail addresses, that isn't available when you use your desktop can be pretty frustrating. Save yourself some time, tears, and gray hair by making sure the two have the same information.

Chapter 4: Picking a BlackBerry

In This Chapter

- **Setting up the BlackBerry**
- **Grabbing your e-mail**
- **Using BlackBerry as a phone**
- **The future of BlackBerry**

Technology can be quite an amazing thing, especially when you think about how far Internet and mobile technology have come in relatively so little time. Not so long ago, a little device that hooked on your belt and could make calls around the world, surf the Internet, and send e-mails seemed like something out of the year 3000.

One device, called the BlackBerry, helped realize that future. If you look back just a few short years, sure, it lacked many of the standard features that most people take for granted today, but it still was one of the first devices out there that truly helped you go mobile!

Of course, BlackBerry faces some stiff competition from other device manufacturers. This competition resulted in BlackBerry improving and updating their offering to be more in line with what mobile office users really need today, including wireless capabilities and touch screen technology.

Whether or not to make the move to BlackBerry really depends on you, your preferences, and how you actually plan on using your mobile device. For those who like the all-in-one nature of the device (e-mail. Internet, applications), but also prefer having a keyboard for typing, you may want to check out the BlackBerry Web site at `www.blackberry.com` and see what's cooking!

Avoiding a Raspberry

A BlackBerry is a suitable way to communicate for several reasons:

- It's wireless, so you can take it with you wherever you go.
- It's small and light, fitting in a holster you can wear on your belt.
- It gives you around-the-clock access to your e-mail.
- It provides 24-hour access to the Web.

- It works well with corporate e-mail systems, so workers can easily use their BlackBerrys to stay in touch.
- Newer models provide touch screen technology, which makes navigating your device even easier

Of course, these features were once hot selling points, but now they are so standard that I wouldn't even tout these features. As I said before, what really sets the BlackBerry apart from the rest — even after all these years — is its keyboard feature.

You can read more by visiting the BlackBerry Web site at `www.blackberry.com`.

Which carriers offer the BlackBerry? Here's a short list, which doesn't include smaller telecommunications (or telecom, if you want to be sleek, too) providers:

- AT&T Wireless
- Cingular
- Nextel
- T-Mobile
- Verizon

When you subscribe to BlackBerry from one of these services, make sure you read the fine print carefully. Some providers may offer a voice and data plan that allows you unlimited Web and messaging access, as well as a certain number of minutes per month. Other plans may only offer data plans and charge you a higher-than-normal voice rate for calls made using your BlackBerry.

Picking a Model, Any Model

The decision about which BlackBerry model to use may be made for you if you have a particular cellular phone carrier in mind. Whichever model that carrier has is the one you will get. They may sell more than one model. (Models with built-in cell phones are similar to the PalmOne Treo 600, which is one of the mobile phones I discuss in Book VI, Chapter 1. They also are similar to the Sidekick II, which I write about later in this chapter.)

Ask yourself some of these questions when deciding which BlackBerry model to purchase:

- Is the newest technology important to me? Or do I just want functionality and can leave the stylish technology to the hipsters?

- Which models are available from my carrier of choice? If you like ABC Wireless, but they don't have the model you want, you may need to go with another carrier or settle with the BlackBerry model they provide.
- Do I want a color screen or is a monochrome screen okay? Remember that e-mail messages, for better or for worse, read the same either way.
- Do I want to have a touch screen to easily access my applications or can I live with the standard kind of screen?

Currently, Blackberry is definitely a competitor with other smartphone vendors; though it seems that they are more in catch-up mode than innovation. For example, the most recent model, Storm, doesn't offer Wi-Fi capabilities, something that is corrected in the upcoming Storm2 release. BlackBerry also released their first touch screen device a full 18 months after LG, then HTC.

The current series available is the 8900+ GPS Wi-Fi Series. This series includes the BlackBerry Bold (9000), BlackBerry Curve 8900, BlackBerry Tour (9630), and BlackBerry Storm (9500/9530).

What makes these models so popular is that they offer everything a professional or high-end phone should: decent graphics, high-speed Internet/wireless capabilities, e-mail (including push mail), and GPS capabilities.

Navigating a BlackBerry

BlackBerry owes much of its popularity to its ease of use. Other than the traditionally laid out keyboard — although much smaller, so get those thumbs in shape — the device has very few buttons. It has three non-keyboard buttons:

- **Phone button:** Push this button to go to the screen where you either can pick a phone number from your address book or enter a phone number from the keyboard.
- **Trackwheel:** You can whirl the wheel with your thumb and then press when you reach something you'd like to do, such as run an application.
- **Escape key:** Press this when you're in an application and want to return to the main menu. Think of it as the key that helps when you get lost: You can escape to safety.

Turning it on and off

Start where all things BlackBerry start: the on button. On some models, it's the silver button on the far-bottom right of the keyboard. On the Storm, it's the button on the side of the device. If you press and hold this button, the BlackBerry turns off. Push it again and the BlackBerry turns on.

Sending and receiving e-mail

Sending and receiving e-mail through the BlackBerry certainly is what has made the brand name synonymous with portable, mobile e-mail messaging.

You can receive e-mail through a BlackBerry three ways:

- Personal e-mail account access through the BlackBerry Web client. This is for e-mail addresses like my@emailaddress.com.
- Business/corporate e-mail access through the BlackBerry Enterprise Server, which lets workers grab their messages from Microsoft Exchange or IBM Lotus Domino.
- BlackBerry e-mail via an e-mail address that looks like mlelrick@blackberry.net. You receive messages through BlackBerry Web client. These addresses are assigned to you by BlackBerry.

Reading e-mail messages

E-mail is the first application on the BlackBerry screen, so it's fast and easy to jump right in and check for messages. Just follow these steps:

1. **Making sure the e-mail icon is highlighted, click the trackwheel.**

   The e-mail message screen appears, as shown in Figure 4-1.

Figure 4-1: The e-mail messages screen.

2. **Double-click the trackwheel to open the message.**
3. **Click the Escape button when you want to return to the main menu.**

   Otherwise, use the menu to perform another function on the e-mail message. That's it.

   The first click of the trackwheel opens a menu that, in addition to opening a message, lets you do these things:

   - File a message
   - Mark a message as unopened

- Save a message
- Reply to a message
- Forward a message
- Delete a message

Composing a message

Now you know how to read your e-mail messages. How do you send one? Just follow these steps:

1. **Scroll to the Compose icon.**
2. **Click the icon using the trackwheel button.**

   A Compose Message screen appears. Click Use Once if the address you need is not listed.
3. **Select E-mail from the menu.**

   One Time E-mail screen appears.
4. **Type the e-mail address.**

   You can use the spacebar to insert the @ sign into the e-mail address. Clicking the spacebar a second time inserts a period into the address. This lets you enter an address quicker because you don't need to press any special keys to access the symbols and punctuation keys.
5. **Press the Return key.**

   The Subject line appears.
6. **Enter a subject.**
7. **Press the Enter key.**

   The cursor moves to the body of the e-mail.
8. **Enter your e-mail message, as shown in Figure 4-2.**
9. **Click the trackwheel.**

   The menu appears.

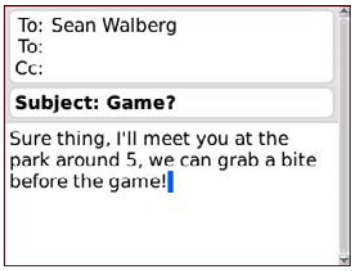


Figure 4-2: Compose an e-mail's address, subject, and message.

10. **Click Send.**

    That's how you send an e-mail message with your BlackBerry!

    You also can Save Draft or add addresses in the To, Cc, and Bcc fields. If you clicked Send, you are taken to the e-mail screen, which shows your outgoing and incoming messages.

Tables 4-1 and 4-2 provide shortcuts to help you navigate the BlackBerry landscape.

Table 4-1 General Shortcuts

Do This	*To Do This*
Press Alt while rolling the trackwheel	Scroll horizontally in any screen where you enter text
Press Alt while rolling the trackwheel	Scroll a screen at a time in the Messages, Address Book, Calendar, Tasks, and MemoPad screens
Type the first letter of an item in an option list or menu	Jump directly to the item option list or menu
Type the first letters of a name	Find a contact in the address book or To screens (or the initials separated by a space)
Press the Escape key	Exit any screen, menu, or dialog box

Table 4-2 Messages Shortcuts

Do This	*To Do This*
Press Alt + I	View all incoming messages
Press Alt + O	View all outgoing messages
Press T	Go to the top message in the Messages screen
Press B	To go to the bottom message in the Messages screen.
Press N	Go to next unread message in an open message.
Press C	Compose a new message and Saved Messages screens
Press S	Start a search for a message in the Messages and Saved Message screen
Press P	Learn the corresponding date in the Messages previous screen

Do This	To Do This
Press R	Reply to the sender with text
Press G	Return to the last cursor position (if you previously closed a message before you finished reading it)

Making a phone call

You can make a phone call from the BlackBerry a couple different ways. One way uses the dedicated phone call button on the top of the unit, while the other involves selecting the Phone icon on the device's Home screen.

To use the dedicated phone call button, follow these steps:

1. **Click the dedicated phone call button on the top of the BlackBerry.**

   The Phone screen appears.

2. **Select One Time Dial or begin entering the number.**

   The Enter Phone Number dialog box appears.

3. **Enter a phone number.**

4. **Select Call.**

   BlackBerry dials the number.

To place a phone call from the Home screen, follow these steps:

1. **Click the Phone icon.**

   The Phone screen appears.

2. **Select One Time Dial or begin entering the number.**

   The Enter Phone Number dialog box appears.

3. **Enter a phone number.**

4. **Select Call.**

   That phone on the other side should be ringing.

Clicking a telephone number in an e-mail, for example, makes the BlackBerry call that number automatically. In addition, if you click an e-mail address inside a message, the BlackBerry automatically composes a message with that address. It also works with Web addresses; clicking them fires up the browser.

Adding a person to Contacts

You can add someone to Contacts in two different ways: add a contact from scratch or add a contact from a message you received from that individual.

Follow these steps to add a contact from scratch:

1. **From the Home screen, click the Contacts icon.**

   The Find screen appears.

2. **Click the trackwheel to bring up the menu.**
3. **Click New Address.**

   The New Address screen appears.

4. **Enter information into the address book fields, which are shown in Figure 4-3.**

   Press Enter or use the trackwheel to move between fields.

5. **When you're done entering contact information, click the trackwheel to bring up the menu.**
6. **Click Save.**

   The contact information is added to your address book.

Figure 4-3: Enter information into Contacts.

Follow these steps to add a contact to the address book from an e-mail message:

1. **Open the e-mail message.**
2. **Click the trackwheel to view the menu.**
3. **Select Add to Contacts.**

   The New Address screen appears with the e-mail address filled in.

4. **Add any other contact information you'd like.**
5. **Click the trackwheel to bring up the menu.**
6. **Select Save; the contact information is saved in your Contacts.**

Security help

If you're strolling through Boston's Logan International Airport and you look a little shady to Massachusetts State Police officers, a BlackBerry may be unholstered long before a gun is drawn. The state police are using the devices to perform background checks on suspicious individuals. The BlackBerry connects to a database called LocatePlus, which contains information from various sources about more than 200 million U.S. residents. The database, based on the data, assigns a security rating to everyone. All of this information is available via the BlackBerry.

Browsing the Web

Using a BlackBerry to access the Internet used to be like using a spoon to dredge the ocean. Most Internet sites are not designed for viewing on such a small screen, although the BlackBerry is a way to read Web content in a pinch. Fortunately, the newer Blackberry models have improved browser rendering, and more and more Web sites are developing mobile versions of their Web sites to facilitate surfing on these small, handheld devices.

There are several ways to open a Web page. Here are the steps for entering a Web address in the BlackBerry and visiting that Web site:

1. **From the Home screen, click the Browser icon.**

   The Browser Bookmarks screen appears.

2. **Click the trackwheel to view the menu.**

   The menu appears.

3. **Click Go To, which brings up the Go To dialog box.**

4. **Enter the Web address.**

   I already told you about the trick of pressing the Space key to insert a key. You also can press Shift + Space to insert a forward slash (/).

5. **Click OK.**

   BlackBerry's browser loads and, hopefully, the Web site you requested appears.

Special versions of two popular Web sites are designed for small Web browsers l: `www.google.com/wml` and `mobile.yahoo.com/home`. I discuss many of these Web services and others in Book V, Chapter 2.

Chapter 5: Finding Wi-Fi Hotspots

In This Chapter

- **Using Wi-Fi directories**
- **Dreaming about airports, hotels, and clouds**
- **Thinking about security**

Your laptop and your smartphone are set up for wireless networking, and you're restless to connect to the Internet somewhere outside your home or office. You've heard about hotspots, which are places with public Internet access. How can you find them?

Luckily, you can turn to several places for this information before venturing from home. In this chapter I talk about Wi-Fi directories, as well as some public projects that are trying to make wireless access available to everyone. Of course, with the preponderance of hot spots these days, it's really easy just to turn on your wireless device and see what's available! From restaurants, to hotels, to bookstores, more and more businesses are offering some sort of Wi-Fi coverage — some free, some paid.

Getting Thee to a Directory

How do you find Wi-Fi heat in the spots you plan to travel? The quickest way is to do some homework before you leave, searching one of several large databases on the Internet for hotspots. Table 5-1 describes some of the largest online directories. WAP is a security protocol that scrambles your wireless communications to keep them from prying eyes.

Table 5-1 Online Wi-Fi Directories

Site	*URL*	*Description*
JiWire	www.jiwire.com	This large online directory of worldwide hotspots lists more than 272,000 hotspots in 140 countries. You can search for a hot spot using several criteria. A search results page is shown in Figure 5-1. A group of mini directories separates free hotspots. Offline versions are available. You can download Windows, Macintosh, and Linux versions from www.jiwire.com/hotspot-locator-laptop.htm. A third version for Web-enabled mobile phones connects live with the JiWire directory.
Wi-FiHot SpotList.com	www.wi-fihotspotlist.com	Calls itself the definitive list of hotspots. Though some find it to be slow to return results, I've found it to be satisfactory.
The HotSpot Haven	www.hotspothaven.com	Counts 107,799 hotspots in its directory. The United States has the largest number of hotspots, but the European and Asian directories also return a decent number of hotspots.
Wi-Fi Marine	www.wifimarine.org	Do marinas float your boat? Then you might check out this site. It covers everything related to boaters and wireless Internet access.
Web In-Flight	www.webinflight.com	Has information about Wi-Fi service available on airlines.
NodeDB.com	www.nodedb.com	If you're heading overseas, NodeDB.com seems to be one of the largest directories that focuses on hotspots outside the United States.
WiFiMaps.com	www.wifimaps.com	This site was a little slow for me. But the site is a little different from the others in that it displays hotspots on interactive U.S. and world maps. You can search by station name, U.S. state, or by geographic region.

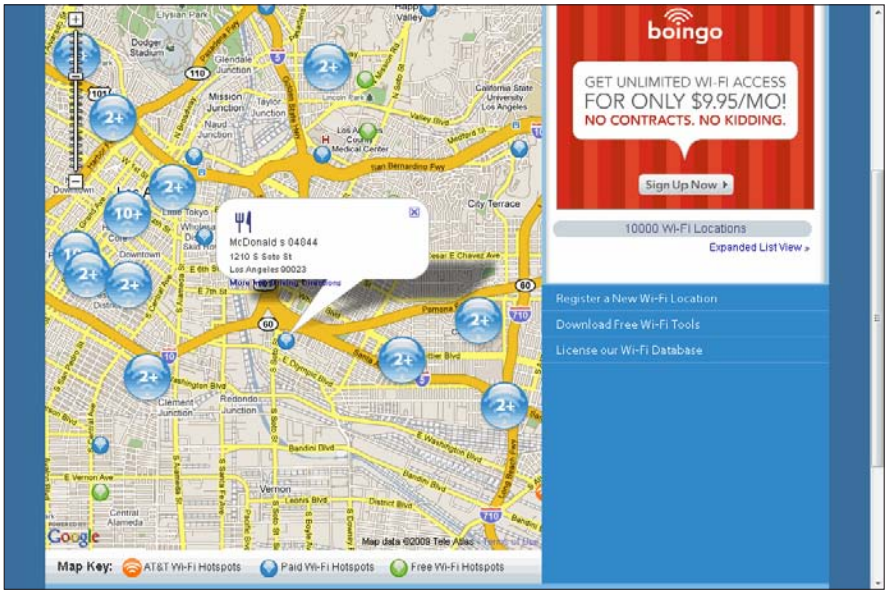


Figure 5-1: Search results for hotspots within 20 miles of a ZIP code.

Paying for the Goods: Commercial Providers

I wish everything were free (except this book!), but sometimes you need to turn to commercial Wi-Fi providers when you travel. I present you with a list of the major ones:

- **T-Mobile at** `www.t-mobile.com/hotspot/`. The nation's largest public hotspot provider sells Wi-Fi access at 45,000 locations worldwide, including Starbucks, FedEx Kinko's copy centers, and Borders bookstores. It also provides service in some major airports, as well as the frequent-flyer club lounges for Delta Air Lines, American Airlines, and United Airlines. As I write this, T-Mobile has three different ways to pay for access:
  - T-Mobile Unlimited national. The subscription includes unlimited minutes for $9.99 a month for qualifying T-Mobile voice customers.
  - Unlimited national. The subscription includes unlimited minutes for $29.99 a month if paid a year in advance or $39.99 a month if paid month to month.
  - DayPass. You can purchase this prepaid access for no minimum commitment. It costs $7.99 for 24 continuous hours.
  - Pay as you go. It costs $6 per login for the first hour with a minimum user session of 60 minutes, with additional minutes costing 10 cents each.

- **Boingo Wireless at** `www.boingo.com`**.** This large provider of hotspots boasts more than 100,000 locations. Boingo charges $9.95 a month for unlimited connection time in North America. For world travelers, there are more sophisticated (read: expensive plans) that run $59.00 per month.
- **Wayport at** `www.wayport.com`**.** Wayport is now AT&T Wireless, which offers a national plan for $19.99 per month. Plans for Europe are also available to national customers.

Paying for the Goods: Making a Commitment

If you're a road warrior, as I have been over the years, it's likely that you're going to want something a little more reliable than rolling the dice on a free Internet connections or an underperforming, yet expensive, option. Up until a few short years ago, hotspots were our best option. Of course, the problem was that arranging your schedule to only be in places that offered a Brand X hotspot was hardly convenient or practical.

Entering the 21st century, wireless providers took a new approach and stopped advertising their hotspot access and replaced it with a full-blown wireless broadband service. Rather than depending on your wireless device, these subscriptions were solely for laptop or netbook users and depended on a USB-device that you would use — along with an application — to connect to your provider's broadband network over a GSM, 3G, or 4G network. The download speeds for these connections are more than adequate for most business travelers; however, it's important to note that performance is still not as fast as at home over your wireless connection. Currently, most providers in the United States provide connection speeds of up to 1.4MB/1.5MB.

Searching made easier

T-Mobile used to offer a helpful tool called Connection Manager, which helped you find a nearby hotspot. It was replaced by Web Connect, which doesn't appear to offer this feature — rather, it's a plug in and go feature — but you can still download Connection Manager online if you're really interested in using it; just don't expect any support from T-Mobile.

Boingo Wireless has similar software available for Windows computers and Pocket PCs. You can download it from www.boingo.com/download-boingo.php, though a mobile version is also available for download. It also helps you connect to Boingo's virtual private network (VPN) service, which means you make a secure connection to the company's network so that all of your Internet traffic is encrypted (read: jumbled and hence safer). It's a virtual loincloth for public hotspots.

A handy feature that both utilities share: They detect all nearby Wi-Fi signals, whether or not they're part of the companies' network. You can easily connect to any of these detected hotspots.

There are five major mobile broadband providers in the United States; you might recognize them because most of them also offer voice plans. They are

- **Verizon Wireless:** One of the major players on the mobile broadband scene, Verizon offers a variety of plans for mobile devices such as netbooks, laptops, and USB modems that range from a day pass ($15/session) to monthly plans ($39.95–$59.99) that offer 250MB and 5GB monthly allowances, respectively. Verizon also offers a variety of plans for other mobile devices, including handsets or smartphones (www.verizonwireless.com/b2c/mobilebroadband/).
- **AT&T:** A solid network with a good coverage page; AT&T offers a number of data plans for handheld wireless devices, such as smartphones and BlackBerry devices. There is also a single data plan for mobile laptop broadband. This package offers up to 5GB traffic per month for $60. (www.wireless.att.com/cell-phone-service/cell-phone-plans/data-connect-plans.jsp).
- **Sprint:** Another one of the major players; it is now teamed up with Nextel to offer pretty impressive coverage. Sprint offers a variety of plans for mobile devices, including its Sprint wireless broadband cards, which let you connect to Sprint's national wireless broadband network. The mobile broadband connections range from $59.99 to $69.99 (if you're a voice customer) (http://nextelonline.nextel.com/NASApp/onlinestore/en/Action/DisplayPlans).
- **T-Mobile:** T-Mobile offers a pretty reliable network that always seemed to be around when I needed it. They offer not just standard data plans for wireless devices, but also BlackBerry and SideKick (a T-Mobile original) wireless data plans. These plans range from $39.98 to $59.99 per month (www.t-mobile.com/shop/plans/Cell-Phone-Plans.aspx?catgroup=Indvidual-cell-phone-plan&WT.mc_n=Individual_PlanFirstTile1&WT.mc_t=OnsiteAd).
- **U.S. Cellular:** This is probably the least robust option available in terms of coverage, but it does offer some good plans for the budget conscious. Data plans (not all high speed) range from $9.95 (bare bones service) to $49.95 (http://easyedge.uscc.com/easyedge/jsp/plans.jsp).

Going Public

The beauty of Wi-Fi networking is its mobility. It gives you the freedom to wander far from home and still have a solid connection to the Internet. You can find Wi-Fi hotspots around the globe, with the United States, Europe, and Asia leading the way as they add thousands of new access points every year.

In airports

Second to your hotel room, where do you spend most of your time during a business trip? It's probably not in the meeting or at the conference. More likely, it's the airports you pass through, especially with the increased security that forces you to arrive earlier and stay longer. Of course, layovers add to the fray.

That's why it's a good idea to know, before you leave on your trip, which airports offer what Wi-Fi services. Some may offer free access, a combination of limited free access and commercial access, or commercial access only.

Generally speaking, paid wireless access will run you about $9.95 for 24 hours or $49.95 per month for unlimited service. If you're stuck in one of these airports for several hours, ten bucks may seem like a bargain as you pull out your laptop to check your e-mail.

Here's a list of major airports and some of the wireless Internet services they offer:

- **Chicago O'Hare International.** Concourse and Boingo are the providers here, which cover terminals 1, 2, and 3. Unlike many other airports, these services don't come for free.
- **Los Angeles International Airport.** Boingo Wireless rules the roost here and covers no less than seven terminals.
- **Dallas-Ft. Worth International Airport.** Boingo and T-Mobile provide coverage in various areas throughout the airport, though Boingo is your cheaper option if you plan on surfing more than an hour.
- **Atlanta Hartsfield International.** A-town offers one of the most extensive airport wireless lists, offering Boingo, Concourse, Sprint PCS, Access, Opti-fi, and T-Mobile. I forgot to mention that none of them are free.
- **Denver International Airport.** Not surprisingly, Boingo is the mile-high Wi-Fi provider (are you sensing a trend?).

Obviously, any of these services can change in an Internet minute. However, these snapshots of Wi-Fi access available in the larger airports at least gives you an idea of what's out there. As with other hotspots, you can check availability on one of the hotspot directories listed in Table 5-1.

In hotels

Not so long ago, it was a pretty big deal when I found a hotel offering high-speed, wired Internet access. It beat a slow, dial-up connection, and I was able to work better in my hotel room.

Now it's almost expected, especially among mid- to high-end hotels, that you'll have wireless Internet access from your room and possibly the lobby, too. Note that wireless access outside the United States is generally not free and can cost upwards of $25 per day. For example, these large hotel chains offer some services (if you're in the U.S.):

- **Hyatt.** Most of the chain's more than 200 hotels have Wi-Fi access; currently there are 414 properties that offer wireless. The service is available in the lobby, other public areas, and some guest rooms. Hyatt charges a daily rate that varies by location.
- **Marriott.** More than 1,200 of Marriott's hotels have wireless Internet access. Hotels include Marriott Hotels & Resorts, Renaissance Hotels & Resorts, Courtyard, Residence Inn, TownePlace Suites, Fairfield Inn, and SpringHill Suites. Access is available in hotel lobbies, meeting rooms, and public spaces.
- **Hilton.** As one might expect, almost every Hilton property (including Hampton Inn and Hilton Garden Inn) offer wireless access. Generally speaking, the Hilton properties charge a daily fee for Internet access; however, its partners (notably the two mentioned here) offer complimentary wireless access.
- **Sheraton.** Owner Starwood Hotels & Resorts has Wi-Fi connectivity in more than 150 Sheraton, Westin, and W hotels in the United States. It also provides access to about 40 properties in 10 countries and regions across Asia Pacific.
- **Omni.** All U.S.-based Omni hotels offer high-speed wireless access. In some hotels, this is limited to certain rooms or public areas.
- **Best Western.** Yep, you read that right. Even the lower end of the hotel industry is embracing Wi-Fi. And how: Best Western plans to install wireless access in 2,300 properties throughout North America.

In the (city) clouds

A new movement is equipping many city centers with Wi-Fi access. The Wi-Fi service areas, called city clouds or hot zones, are a way for cities to differentiate themselves from other business and tourism centers. In many cases, the hot zones are dual use, with police and fire workers using it along with residents and visitors.

It is good PR: If you can check your e-mail on your Wi-Fi–enabled laptop or PDA while visiting a city's downtown, aren't you more likely to remember your visit and have good feelings about the hospitality? Covering several or more blocks beats isolated hotspots at coffee houses and other limited locations.

Hot cities and countries

Not surprisingly, the United States is the nation with the most hotspots. In fact, it has more hotspots than the next nine nations on the worldwide top ten list combined. The source of this list, JiWire (www.jiwire.com), counts over 273,000 hotspots worldwide.

- United States: 66,312
- China: 28,678
- United Kingdom: 27,458
- France: 25,573
- Russian Federation: 14,457
- Germany: 14,434
- South Korea: 12,813
- Japan: 11,607
- Sweden: 6,634
- Taiwan: 5,386

When it comes to U.S. cities with the most hotspots, New York City tops the list. Interestingly, half of these cities are in either California or Texas, as the map shows.

- New York City: 885
- San Francisco: 871
- Chicago: 788
- Seattle: 624
- Houston: 600
- Los Angeles: 499
- Atlanta: 451
- San Diego: 422
- San Antonio, TX: 416
- Austin, TX: 411

Here's a small selection of cities and states offering wireless access:

- **New York City.** In the Big Apple, thinking big is part of living. Officials are planning a Wi-Fi network for public safety employees. The price tag: a staggering $500 million to $1 billion. For the general public, you can find wireless access virtually anywhere just due to the sheer size of the city.
- **Washington, D.C.** You can get free Wi-Fi access from the front of the Supreme Court, the Library of Congress, and the Capitol visitors' site. The nonprofit group deploying the network has a hot zone stretch from Capitol Hill to the Washington Monument.
- **San Francisco.** The real San Francisco treat is the city's plan to install 360 solar-powered bus stops with Wi-Fi across the city over the next couple of years.
- **Seattle.** If you're sleepless in this city, sometime in the future you might be able to access what city officials hope will be border-to-border wireless Internet access. Of course, this city has what seems like a limitless number of coffee shops ready to provide you with Wi-Fi coverage in the meantime.

- **Spokane, Washington.** Its dual-use Wi-Fi network covers a 100-block area that is a mile long and a third of a mile wide.
- **Rio Rancho, New Mexico.** This is the first city to offer city-wide, free wireless access. It's also home to Intel's primary manufacturing center.
- **Austin, Texas.** A volunteer effort is under way here to keep Wi-Fi free.
- **St. Cloud, Florida.** The city is offering free Internet access, with its hot zone covering an area about 20 city blocks.
- **Paris.** For those of you traveling in Europe, there is an extensive public wireless access system in Paris. Many parks and other public spaces offer free wireless internet access. It's not uncommon to see people in parks with their laptops, working.

McWireless and others

What's left after the other locations? In many places, such as Seattle, Wi-Fi–equipped coffee shops are all the rage. (If you live in Seattle, check out the Caffeinated and Unstrung Web site at `www.seattle.wifimug.org`.) Wireless Internet access is also making inroads to fast-food restaurants and sports venues.

Retailers

Schlotzsky's Delis, Apple retail stores, Panera Bread, and Krystal Restaurants are among the national chains that have Wi-Fi in at least some of their locations. Not only can you buy goods and services from these places, you can go online:

- **Starbucks:** While this national coffee shop famously keeps its customers wired, it also offers Wi-Fi access. The company says that Wi-Fi users stay in its stores longer, with the average wireless session lasting about 45 minutes. Now it's safe to drink and (hard) drive.
- **McDonald's:** I'm not sure how many people take their laptops or PDAs to a McDonald's to get some work done, but 15,000 of the restaurants worldwide now offer wireless access. I'll have a salad, a large fry — and my e-mail, please.
- **FedEx Office:** It took T-Mobile six months to wire (unwire?) this copy center's 1,000 U.S. locations. They welcome your use of the stores as surrogate offices.
- **UPS Stores and Mailboxes Etc:** After starting with AT&T to offer high-speed access to customers, they were unceremoniously dropped, and I'm not quite sure what's on the menu anymore.

Stadiums and arenas

During baseball game broadcasts, I'm surprised how many people I see in the stands chatting on their cell phones. Maybe providing wireless Internet access is the next logical step? The San Francisco Giants is offering free Wi-Fi access to its baseball fans. Now you can attend a day game while checking your e-mail, making it appear you're working. You also can check on scores and stats — anything you can do at home is available. The Charlotte Bobcats basketball team offers a similar service. Other stadiums and arenas have toyed with the idea, too.

On the road

You can be between points A and B and still get online:

- **Airplanes:** German airline Lufthansa has on-board Wi-Fi access. With regards to the U.S. market, Delta and Virgin America are the most advanced so far. This service is provided by Gogo Inflight, which is available at `http://gogoinflight.com/`.
- **Truck stops:** Truck drivers need Wi-Fi access, too. There's family to e-mail and paperwork to file. Offering access differentiates one truck stop from the other, providing a competitive advantage.
- **Highway rest areas:** Texas, Iowa, and Maryland think they know how to encourage tired drivers to stop more often at highway rest stops: Offer them wireless Internet access from the comfort of their vehicles. It's especially a boon to truckers and RVers. With the security lines in airports being so long, the highways may become an important alternative to business travelers.
- **Campgrounds:** The state of Michigan installed Wi-Fi access in a state park campground. It plans to do this in other state parks, as well. I'm sure this is happening elsewhere, too. My idea of roughing it is watching TV on anything other than a big screen, so battling insects in a tent and foot fungus in the shower is not within my definition of reality. Yet I understand many folks like this return to precivilization days. Now they can swat the mosquitoes while surfing the Web. Progress!

Clenching Your Security Blanket

Most, if not all, of the public hotspots I discuss in this chapter provide unsecured wireless Internet access. That means you're out there naked, baby. The guy with the tall latte at the next table can easily access your laptop or PDA files if you're not careful. Use a firewall and buckle down your file access, as I discuss in Book IV, Chapter 1. If you're connecting to a corporate network, do so through a virtual private networking (VPN) connection, which I discuss in Book V, Chapter 6.

Don't send out personal information like credit card numbers unless you're connecting to a Web site that encrypts the data before sending it. You can tell if it's a secured site by the Web address, which usually begins with https, and a closed padlock icon appears in your browser.

T-Mobile, which operates hotspots in Starbucks locations, is very clear that you're on your own when it comes to security. "The T-Mobile HotSpot network is based on evolving wireless technology and is not inherently secure," it says in a security statement posted on Starbucks' Web site. "We therefore cannot guarantee the privacy of your data and communications while using the HotSpot service." The statement cautions that an unexplained loss or deterioration of your connection could mean that a nearby hacker has gained free access to the Internet using your HotSpot username and password. If you suspect that's the case, logging out knocks the freeloading hacker off the Internet. T-Mobile suggests you then call its customer service department.

While I cover many of these security issues elsewhere, they're worth mentioning here as you consider connecting to a public hotspot. There's no need to be paranoid (believe me, I know), but vigilance is diligence. T-Mobile makes these security recommendations:

- Don't leave your computer or device unattended. (Duh! The worst security is a stolen laptop.)
- Don't loan your computer or device to someone unfamiliar to you. (You might be a Dummy, but you're not an idiot.)
- Watch for over-the-shoulder viewing of your login, credit card number, or other personal information.
- Log out of Web sites by clicking Log Out instead of just closing your browser or typing in a new Internet address.
- Create passwords using a combination of letters and numbers, and they should be changed frequently. (This is always good advice.)
- Keep passwords and account numbers secure; don't store them on your computer or device or share them with anyone.
- Avoid using Web-based e-mail or instant messaging that uses clear, unencrypted text to send confidential information.
- Remove or disable your wireless card if you're working offline and you are not planning to connect to a hotspot.

Any way you sip it, it's worth letting this advice brew and considering it the next time you connect to the Internet through a public Wi-Fi hotspot.

Chapter 6: Setting Up a VPN Connection

In This Chapter

- **Creating a VPN connection**
- **Using VPN to connect to a far away computer**
- **Putting together an incoming VPN connection**

Wireless networking security is an evolving area. Though wireless networking has some built-in security features, you can't be as confident with it as you can with wired networking. What if you want to wirelessly move information from your PC to a computer located elsewhere? You're in an airport, using public Wi-Fi access, and you want to connect to an office computer — and don't want anyone to see the information you're sending. How can you pull this off? I'm glad you asked.

I show you how to create and use what's called a virtual private network (VPN) to move your data safely over a public network such as the Internet. When you create a VPN connection, you're creating a virtual tunnel. Everything moving through this tunnel is encrypted, or scrambled, so it's safe from prying eyes. Once the data reaches the computer on the other end, the information is decrypted so users can see what you sent.

Setting Up a VPN Connection

Follow along with these steps and you find it's pretty easy to set up a VPN connection (one of which is shown in Figure 6-1). If you have set up other network connections using Windows Vista's Network and Sharing Center, it is even easier for you.

Here's how you set up the VPN connection:

1. **Click the Start menu and select Control Panel.**

   The Control Panel opens.

2. **Click Network and Internet.**

   The Network and Internet dialog box appears.

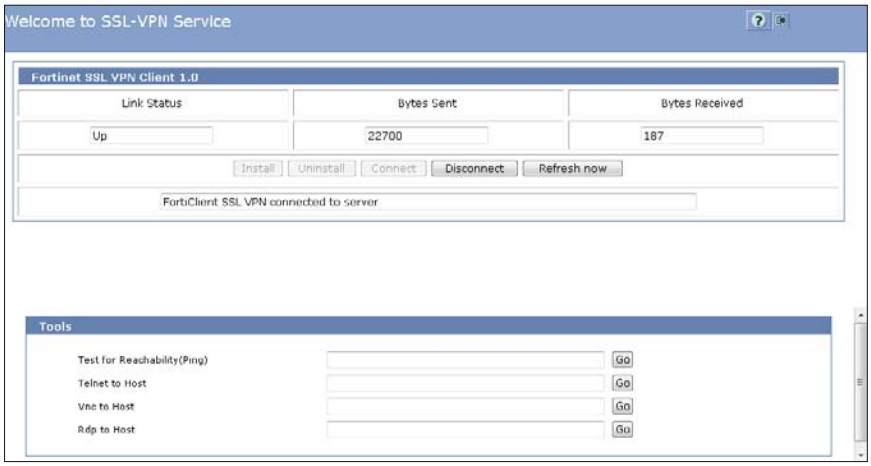


Figure 6-1: Data moving through a secure VPN tunnel.

3. **Click Network and Sharing Center.**

   The Network and Sharing Center appears.

4. **Under Tasks, click Set up a connection or network and then Connect to a workplace.**

   Figure 6-2 shows this being done. The Network Connection dialog box appears. Despite the menu selection's name, the VPN connection can be made anywhere, not just to a company network.

5. **Select whether to create a new connection or use an existing connection, as shown in Figure 6-3.**

   This procedure creates a new connection.

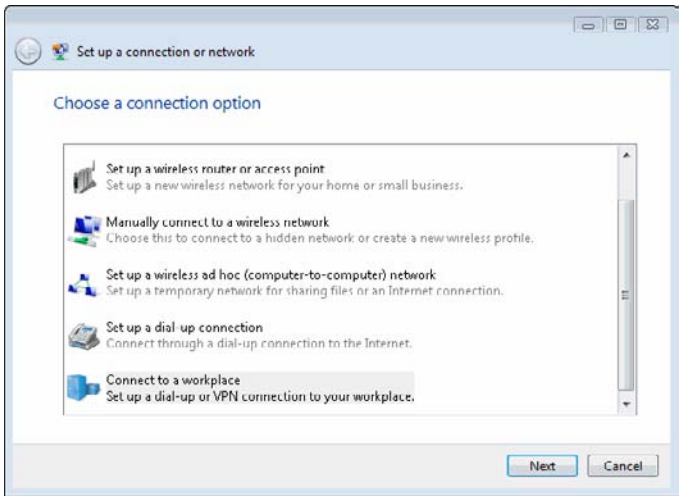


Figure 6-2: The first step in creating a VPN connection.

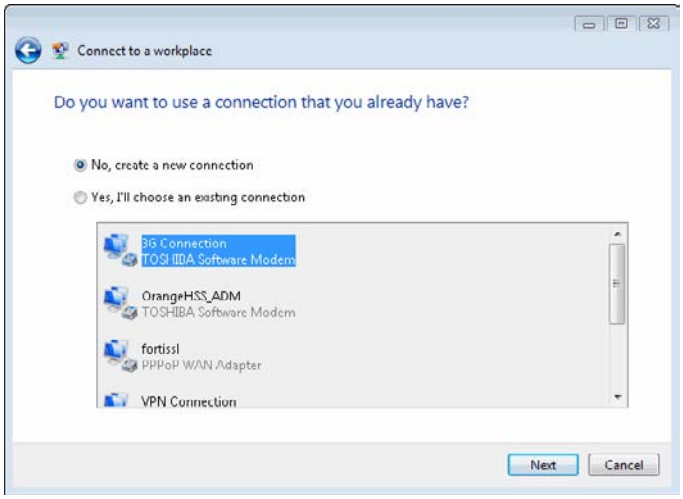


Figure 6-3: Selecting a VPN connection.

6. **Click Next.**

   The Connection dialog box appears and lets you choose how to connect, either using your Internet connection or dial-up.

7. **Select your Internet connection, as shown in Figure 6-4.**

8. **Enter the domain name or IP address of the computer to which you are connecting, as shown in Figure 6-5.**

   You can get this information from your network administrator.

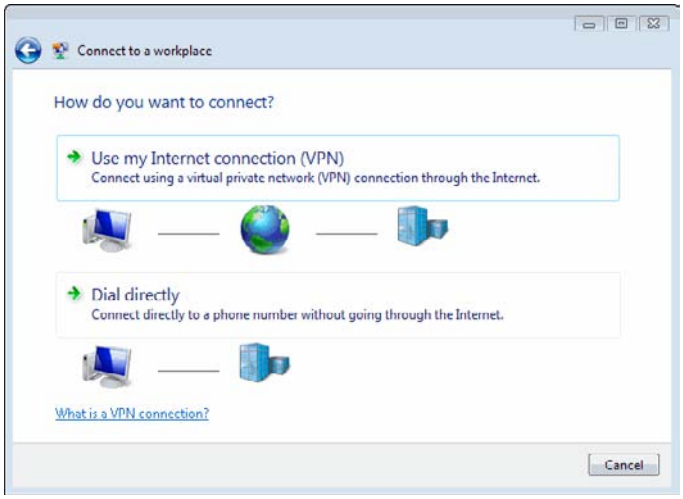


Figure 6-4: Entering a VPN connection name.

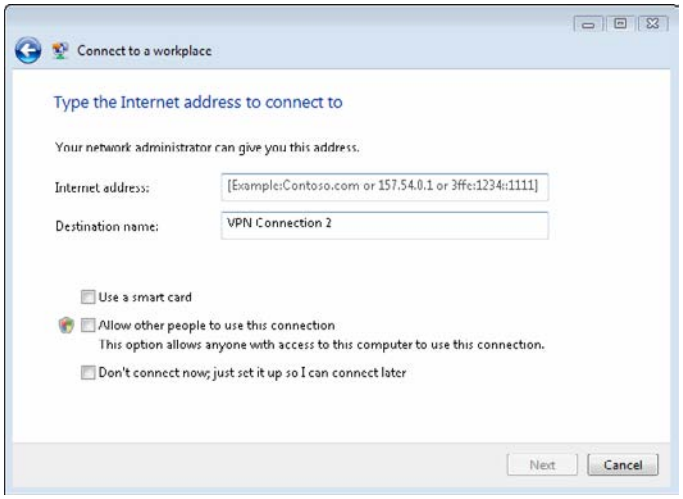


Figure 6-5: Entering a domain name or IP address.

9. **Click Next.**

   You can enter the login name and password for the VPN connection.

10. **Click Create.**

    Your new VPN connection appears in the Network Connections dialog box, as shown in Figure 6-6.

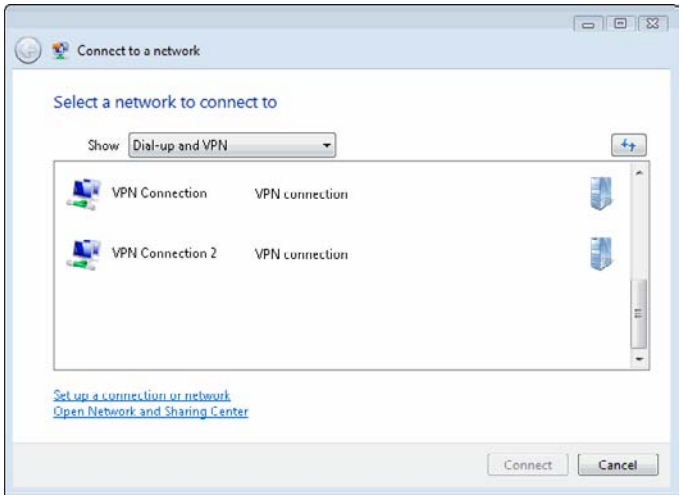


Figure 6-6: You created a VPN connection.

Connecting to a Remote Computer Using VPN

If you've set up a VPN connection on your computer, you can connect to a remote computer that accepts incoming VPN connections. Ask your network administrator whether a remote computer accepts VPN connections. (In the next section I show you how to create an incoming connection for a Windows Vista machine.)

Here's how you connect to a remote computer using VPN:

1. **From the Network Connections dialog box, double-click the VPN connection.**

   A connection dialog box appears.

2. **Enter the remote computer's username and password, as shown in Figure 6-7.**

   You can get this information from your network administrator.

   If you select Save This User Name and Password for the Following Users, everyone with access to your PC can connect to the remote computer. The username and password are saved on your computer, so users won't need to know that information to connect.

Figure 6-7: Entering a username and password.

3. **Click Connect.**

   You see the Connecting dialog box shown in Figure 6-8.

   If the connection is a success, your Virtual Private Network icon in the Network Connections dialog box says Connected.

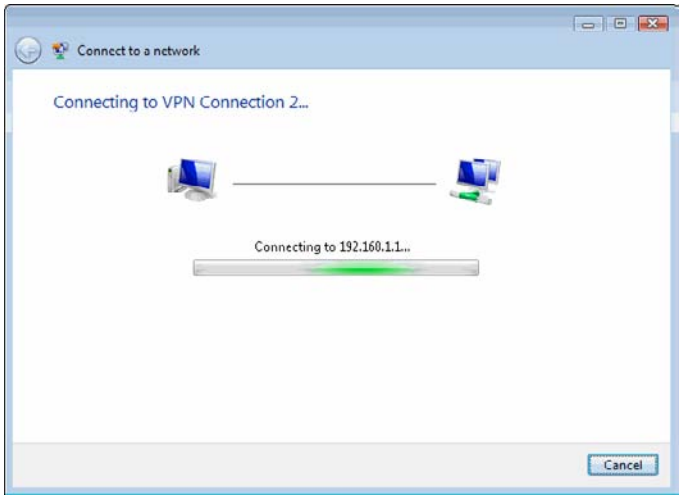


Figure 6-8: Connecting with a remote computer.

You can disconnect a VPN connection by right-clicking the VPN connection icon and selecting Disconnect. You can use the icon to reconnect whenever you want by clicking it.

Creating an Incoming VPN Connection

Windows Vista lets you create an incoming connection so that other users — maybe even yourself while on the road — can connect to your computer using a VPN connection.

The Home edition of Windows Vista can only accept one incoming VPN connection at a time. The Professional version allows multiple incoming connections.

These steps create an incoming connection:

1. **In the Network Connections dialog box, click File➪New Incoming Connection.**

   The following dialog box appears, once you get past the User Account Control, as shown in Figure 6-9.

2. **Select the user(s) with an account on the machine and click Next.**

   The network will accept incoming calls from these users. Once you click Next, the Allow connections to this computer dialog box appears.

3. **Select Through the Internet, as shown in Figure 6-10.**

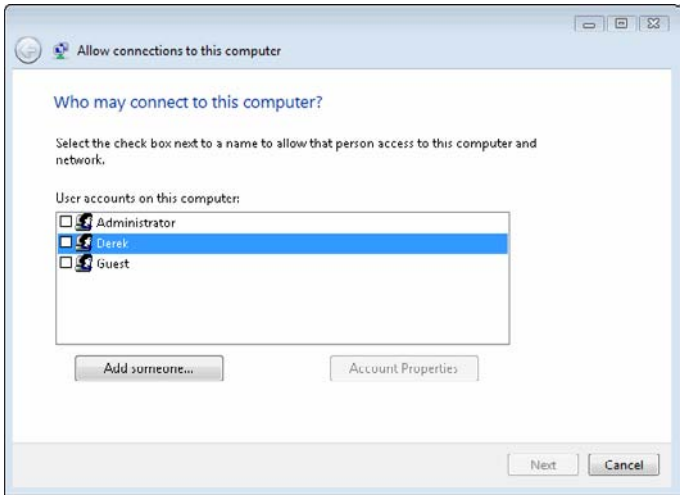


Figure 6-9: Allow incoming connections.

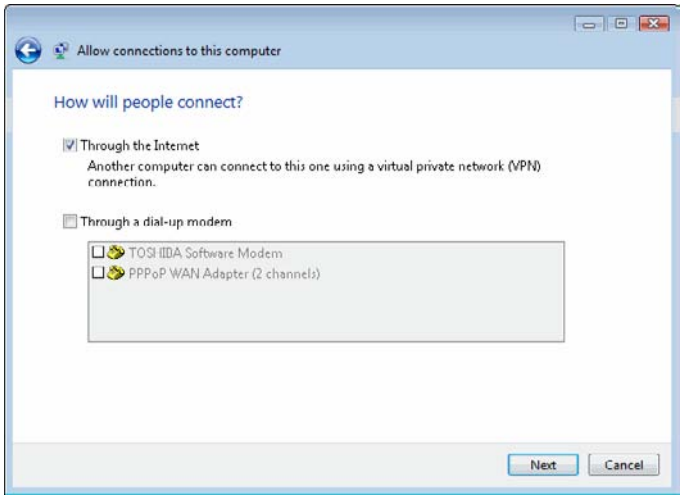


Figure 6-10: Internet or, um, dial-up. The choice is yours.

4. **Click Next.**

   The Network selection dialog box appears. Leave everything selected, as shown in Figure 6-11.

5. **Click Next.**

   The Devices for Incoming Connections dialog box appears. You can ignore this dialog box.

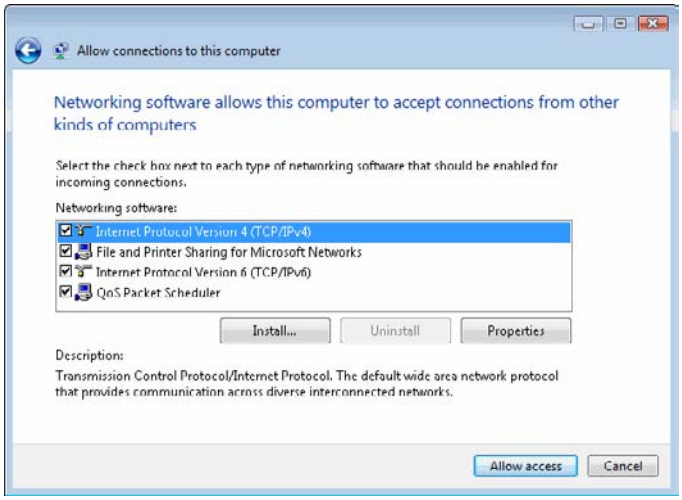


Figure 6-11: Accepting incoming connections using these protocols.

6. **Click Allow Access.**

   The procedure is completed, and your selected users can now access the network, as shown in Figure 6-12.

   Your new incoming connection shows up in the Network Connections dialog box like you see in Figure 6-13. That's it: You just set up an incoming VPN connection.

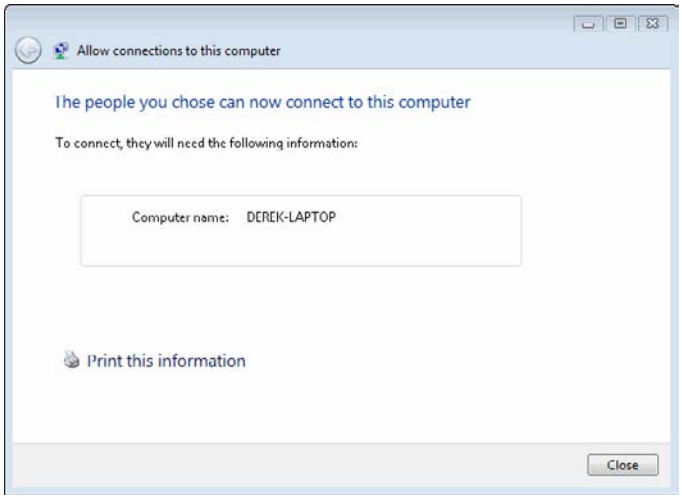


Figure 6-12: Be sure to note this information down!

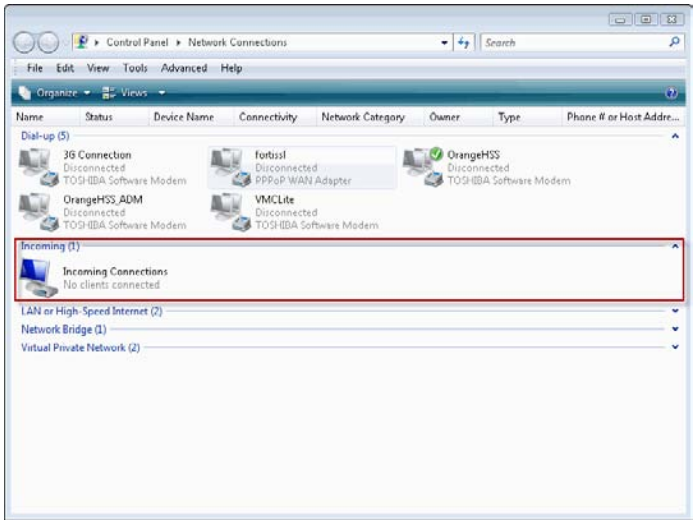


Figure 6-13: Success! The incoming connection is shown.

Chapter 7: Taking Home with You

In This Chapter

- **Watching TV around the world**
- **Taking off with Slingbox**
- **Making the most of the experience**

I know this sounds bad, but I love watching American television. Except for the abundance of commercials, it's like hunting through a junk shop. You've got loads of channels and only a handful of shows worth watching. One of the things I missed about home when I moved to Europe was all the shows that I would miss.

Thinking back a few years to my first stint living abroad in the late 1990s, technology was nowhere even remotely close to where it is today. Back in the day, phone calls back to America were outrageously priced, dial-up was the norm here, and streaming technology? Forget it.

Jumping ahead to 2009, times certainly have changed. For starters, my ISP has download speeds that I hadn't dreamt possible just a few short years ago. Thanks to VOIP technology, I am able to have a local number from the United States so family and friends can call me for the price of a local call. Finally, thanks to one great leap for mankind, I can watch my beloved sitcoms (and here's a special shout-out to DVR technology for surmounting the seven-hour time zone difference).

This chapter explores my latest toy, the Slingbox, from Sling Media, which allows me to watch television remotely with very little setup. Thanks to Slingbox, VOIP, and Web cams, I can feel like home even when I am thousands of miles away.

Watching TV around the World

The Slingbox, in my humble opinion, has to be one of the coolest, more practical gadgets for road warriors of the past 20 years. It's especially useful for those who travel out of the country frequently.

Once you take care of the hardest part (finding someone who will share their television with you), installation is easy, and you're on your way within minutes. Of course, there is some mild inconvenience for the host, as I discuss later in this chapter.

Using proprietary software, you can log on to your account, where you register your Slingbox, and then watch television live through your computer or wireless device. When you are connected to the Slingbox, you literally take over the television on the other end of the internet connection. This means that you control the sound, and more importantly, the channel!

The benefits are in spades, however, as you can enjoy the feeling of sitting on your favorite sofa back home watching your favorite shows. The only thing missing is a batch of mom's homemade chocolate chip cookies. There are no geographical limitations to using the Slingbox; you can live in the U.S., Germany, or Japan and log in to watch a Slingbox that is hosted in France, Brazil, or Canada. It's proven to be quite useful when out shopping with the kids; I can log on to the application on my smartphone and watch cartoons in the United States as we're shopping in Paris.

Taking Off with the Slingbox

There are a few items that you'll need to buy before you are up and running. Even though the installation process is pretty straightforward, you'll have to have some familiarity with wireless technology and a general level of patience for computers.

To get an idea of what you're going to need to get started, visit the Web site `www.slingmedia.com`. From a technical standpoint, you're going to want to make sure that you have a wireless network already configured in your home, or wherever you intend on installing the Slingbox itself. This means that the Slingbox is expecting to find a wireless router to which it can plug in.

After the network requirements are met, you can pick what kind of Slingbox you want to buy. The SOLO model allows you to broadcast your incoming satellite television transmission both over the local television and though authorized users over the Internet. The PRO-HD model lets you go one step farther — you can connect multiple devices, so that you can include DVRs, DVD players, satellite television, and so on in high-definition quality.

The Slingbox provides ample online documentation, but the following is a quick and dirty way to get started. Again, while it's not difficult to set up, it's like preparing a fancy recipe. The individual ingredients may be easy to prepare, but mixing them together at the right time may prove to be a more difficult maneuver to make. These instructions apply to the host — in other words, the person kind enough to share their television with you.

1. **Make sure that you have all the necessary equipment.**

   Locate the back of your satellite receiver, where input and output cables are plugged in.

2. **Plug the cables from the Slingbox to the back of your satellite receiver.**

   This allows the incoming satellite signal to be processed by the receiver (decoder) and then be sent as output to your Slingbox.

3. **Plug the Ethernet cable from the back of your Slingbox to an open port of your router.**

You may want to plug in the Slingbox to an electrical socket for good measure. Experience has taught me that a little bit of electricity also helps move things along. Once plugged in as described above, you should notice lights on in front of the Slingbox, which means that the Slingbox is receiving data and able to broadcast it.

If you have set up your home network in a way that your television/satellite television connection is not in the same room as your wireless router, do not fret. Slingmedia offers a dapper little device called a SlingLink that you can connect between your wireless router and your Slingbox to create a wireless connection between the devices when they are not in the same room.

Now that your host is ready to broadcast, it's now up to you to get things ready on your end. This is a simple process, but it does require a little bit of configuration on your end, so look sharp!

1. **Sign up for a free Sling account.**

   You can do this at `https://betasecure.sling.com/account/login`.

2. **Download the Slingbox software.**

   You can do this at `http://downloads.slingmedia.com/`. You'll want to first download SlingPlayer software for either Windows or Macintosh.

3. **Install the software.**

   This is a straightforward installation; double-click the installer that you downloaded in Step 2 and follow the instructions.

You're almost ready to go at this point! Click the icon that is installed on your desktop to launch the SlingPlayer software. The SlingPlayer appears as shown in Figure 7-1.

The first step is to click Log In, which is in the upper-right corner of the window. If you do not log on, you cannot configure the Slingbox now, nor will you be able to watch the SlingPlayer in the future. The Log In dialog box appears, as shown in Figure 7-2.

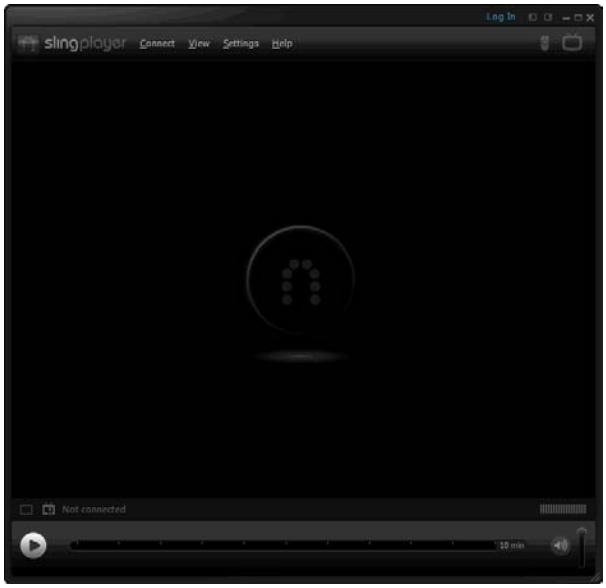


Figure 7-1: The SlingPlayer interface.

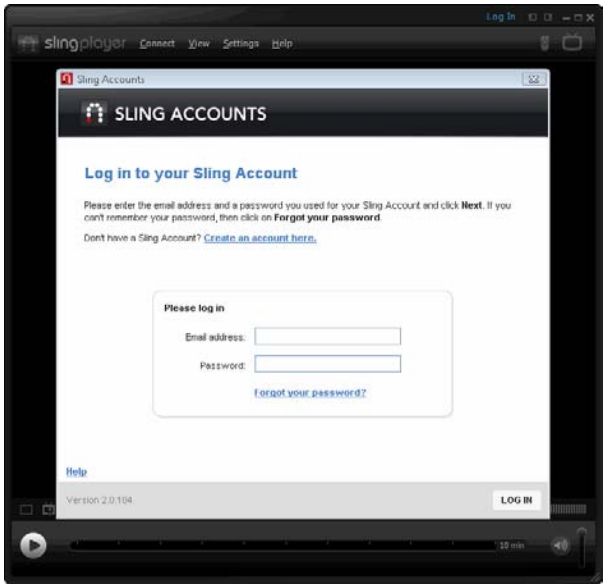


Figure 7-2: The SlingPlayer login window.

Once you are logged on to your Sling account, you will need to configure the Slingbox. This is something that you will likely only need to do once (unless you have to reinstall the software one day), and it will require some help from your Slingbox host.

1. **Choose Connect⇨Slingbox Directory.**
2. **Click Add.**

   The New Slingbox Entry Properties window appears, as shown in Figure 7-3.

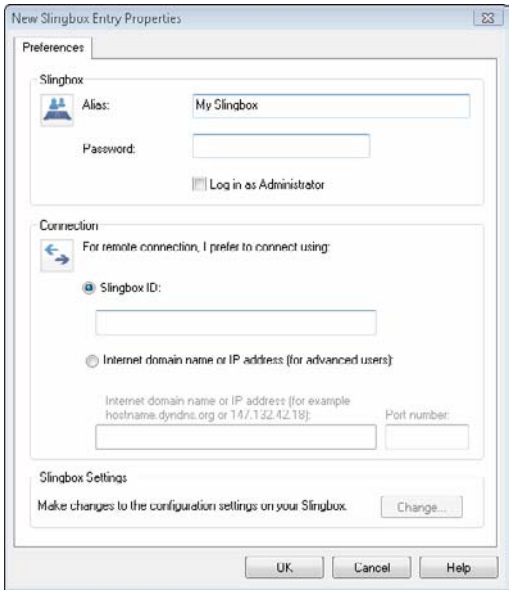


Figure 7-3: Add your Slingbox to your account.

3. **In the Connection section, add the Slingbox ID.**

   You guessed it; you need to get this number from the back of the Slingbox. Pick up the phone and call the person hosting your Slingbox for you, or go to the room with the Slingbox in it and jot that ridiculously long ID number down.

4. **You can add an administrator password if desired.**

   This is helpful if you want to watch the Slingbox and boot someone else off who is already watching it.

5. **Click OK.**

   The new Slingbox appears in the directory, as shown in Figure 7-4.

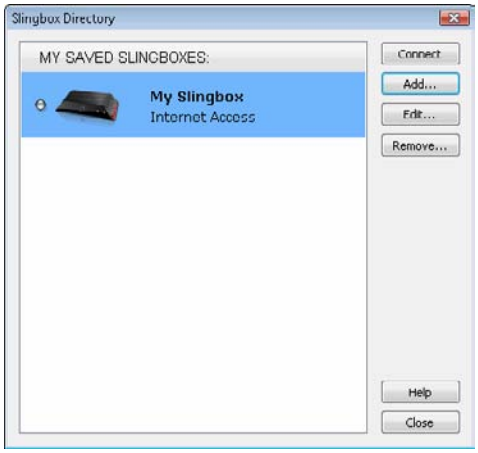


Figure 7-4: The Slingbox directory with new addition.

The Setup Assistant is available to help you set up your Slingbox connection; this is notably where you'll confirm the satellite connection/input device connection and make sure it is properly configured, as shown in Figure 7-5.

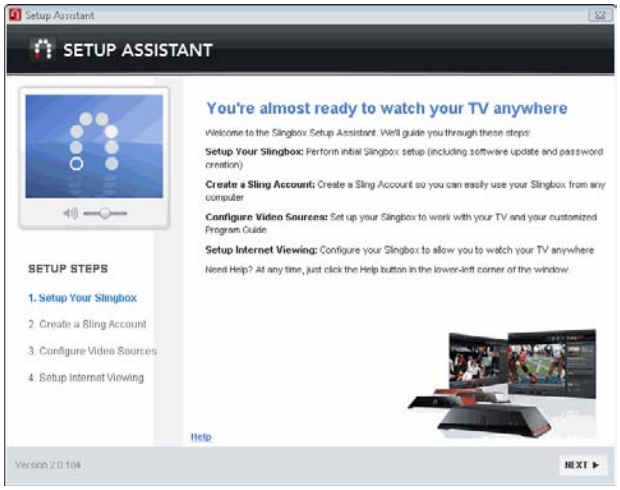


Figure 7-5: The Setup Assistant lets you make sure everything is properly set.

Once you are set, you can go back to the Connect menu and select the Connect to my Slingbox. Once it connects to the Slingbox next door or halfway around the world, it optimizes for the best possible.

Making the Most of the Experience

You're finally all set to watch your streaming television from anywhere around the world. What is strangest for me is watching shows in Europe and seeing the advertisements for stores or restaurants back home that do not exist here. More than once, I've said to myself, "grab your coat, kids, we're heading out! Wait a minute, doh!"

I should also point out that although the SlingPlayer software is free, you can purchase a version for mobile. If you have a wireless device that supports Internet access (a given, these days), you can buy a version of almost any mobile operating system, as well as iPhone. For more information on this version, check out `www.slingmedia.com/go/spm`.

As a frequent user of the mobile version, I still marvel at the fact that I can watch NBC from the comfort of the subway with amazing clarity. Given the advances in smartphone technology, I can watch on a rather generous-sized screen, without having to sacrifice sound quality.

The Slingbox itself can be somewhat pricey, admittedly. However, if you do enjoy watching television and are frequently on the road or not in the country, its money well spent.

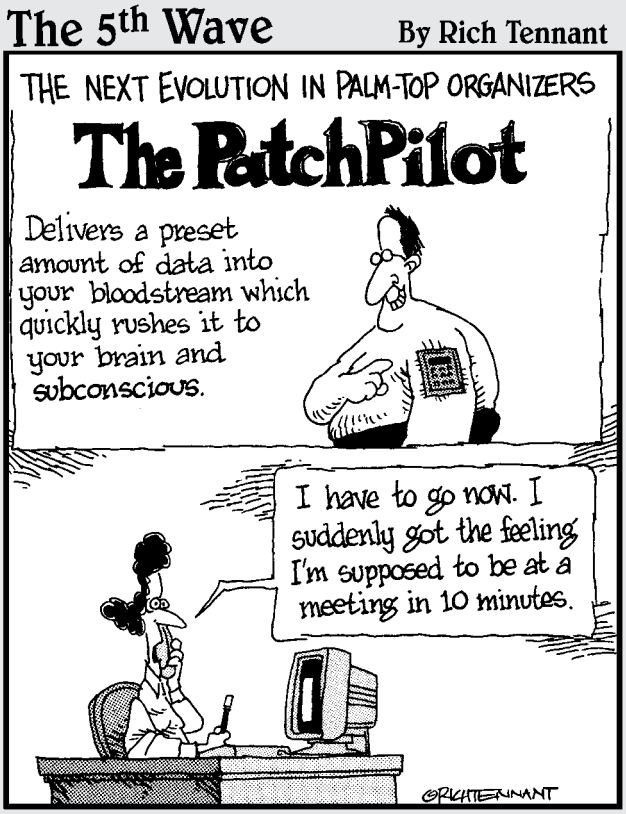
To truly make the most of the experience, I recommend watching on a computer with a proper screen size. I also hooked up some high-end speakers to my laptop so that I could enjoy the full cinema-like sound of what I was watching.

Depending on your computer's capabilities, it's also possible to hook up your PC/netbook/laptop to your television and to watch the SlingPlayer through your own television instead of a small PC screen.

As technology teaches us, where there's a will, there's a way. With Slingbox, I now have yet another piece of home closer to me, which really does prove that the world is indeed getting smaller.

Book VI

Other Networking Technologies



Contents at a Glance

Chapter 1: Choosing and Using Cordless Phones

In This Chapter

- **Distinguishing the difference between analog and digital**
- **Selecting your hertz: 900, 2.4, or 5.8**
- **Getting someone to speak up (or move things out of the way)**

It's bad enough that buying a cellular phone and wireless networking equipment is so complicated. Now, with new options for cordless phones, even that once straightforward purchase is forcing you to reach for the aspirin. Consider me the aspirin — and you don't even have to call me in the morning. In this chapter I discuss the different kinds of cordless phones, the advantages of one over the other, and a technology term or two.

You have choices when it comes to buying a cell phone and choices when installing wireless networking. Now, consider your standard telephone: when you decide to cut its cord and go wireless, you also have choices. Thankfully, cordless phones aren't nearly as complex as smartphones or Wi-Fi networks, but there are different types of cordless phones that use various technologies.

Cutting the Cords

If you're over 35, you probably remember the days when one of the only telephones in the house was a corded model mounted on the wall, possibly with a rotary dial. The only way to increase your distance from the phone was to purchase a longer cord. Although it might be possible, wrestling with a 300-foot cord so you can chat as you move from the kitchen to the garden to the garage is a bit impractical.

Around 1990, when the FCC assigned bandwidth in the 900 MHz frequency range, cordless phones first became a real alternative to corded telephones. While there were cordless phones before that (usually with big, metal, telescoping antennae), the newer frequencies were a big jump in clarity and range from the old 43–49 MHz band.

As manufacturers began making digital models, cordless phones grew even more practical; they were more secure (allowing for less eavesdropping) than analog versions. Also, more channels are available for use by the cordless phone to communicate between the base station and handset. A wider range of channels means interference is more easily thwarted. The breakdown is as follows:

- 10 to 25 channels for inexpensive 900 MHz phones.
- 20 to 60 channels for most 900 MHz phones.
- 50 to 100 channels for high-end 900 MHz phones and for 2.4 and 5.8 GHz phones.

Table 1-1 breaks down the megahertz and gigahertz by range.

Table 1-1: Cordless Phone Ranges

Frequency Band	*Range*
900 MHz	75 to 400 feet
900 MHz with DSS	200 to 1,500 feet
2.4 GHz with DSS	300 to 2,000 feet
5.8 GHz with DSS	300 to 2,000 feet

Analog phones

Analog cordless phones act like a plain, old AM/FM radio. They convert sounds waves into radio waves, transmitting them between the cordless phone and its base station. Anyone with a converter and a radio scanner can eavesdrop. (Selling police and fire radio scanners that pick up 900 MHz transmissions is illegal; 2.4 GHz and 5.8 GHz phones are out of range of most radio scanners.)

When you and an analog handset get too far from the base station, you hear static over the conversation until you can no longer communicate with the base station. These phones also are prone to static from interference. Figure 1-1 shows analog versus digital communications methods.

What is this DSS?

Many new cordless phones — and I recommend making sure this is true of the one you purchase next — use a technology called DSS, or digital spread spectrum. The digital part of DSS means your conversation is converted from analog sound waves to digital 1s and 0s. (You can buy a digital phone that does not use DSS, however.) The spread spectrum part is less clear, though it has something to do with the radio spectrum. This technical term is vague until you discover what it is, how it works, and why you want it.

First, why you want it: DSS-equipped phones are much more secure than analog and plain digital phones. In fact, it's nearly impossible to listen to a conversation taking place on a DSS phone because the listener only hears quick bursts of data that transmit very quickly across multiple frequencies. In other words, one data burst will be at frequency A, then next at B, and so on — and only the phone knows what frequency the next data burst will occur on. Everything happens so fast that it's impossible to follow conversations sent with DSS unless the eavesdropper has very expensive and sophisticated snooping equipment. You can feel pretty confident that the personal information you reveal during a telephone call (credit card numbers, social security numbers, and so on) on this phone is safe.

Second, phones using DSS suffer from less interference. Depending on different factors, they may also have a greater range than similar phones that don't use DSS technology. In addition to being more secure, DSS is a more efficient use of the radio spectrum.

A DSS phone may also be referred to by frequency hopping spread spectrum or FHSS.

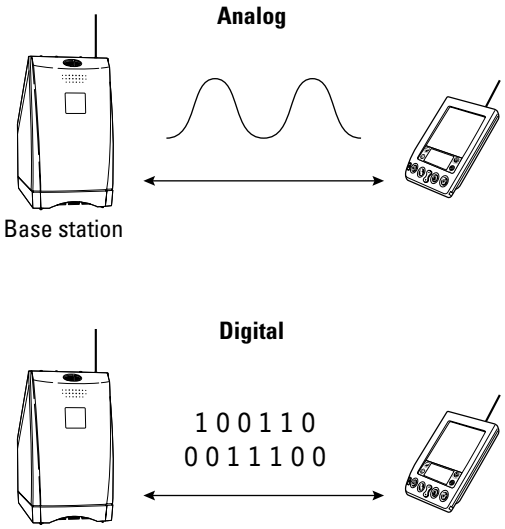


Figure 1-1: Analog and digital phones work differently.

Digital phones

Digital phones convert sound waves into digital signals, which consist of a lot of 1s and 0s. If you tune into a conversation transmitted digitally, you can't hear it without using equipment that converts the output into something humans can understand. When you go out of range with a digital phone, the conversation terminates suddenly with dead air. Digital phones offer no gray area between a good signal and a lousy signal. Their existence shows up on the time lines in Figure 1-2.

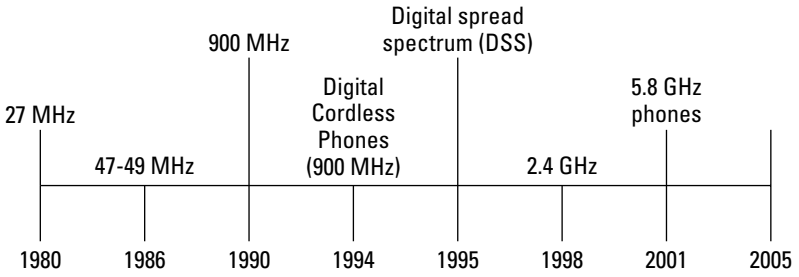


Figure 1-2: A time line of cordless phone frequency band use.

Some digital phones use something called digital spread spectrum (DSS). See the "What is this DSS?" sidebar in this chapter for further information. Not all digital phones have DSS, but all DSS phones are digital.

Choosing Your Frequency

Can you imagine if when purchasing a cell phone and a calling plan, you had to tell the company what technology you want to use? Of course, you have some choices when it comes to handsets and choosing a particular carrier for its network. You don't have to tell the cell phone provider at what frequency you want the phone to operate.

When you purchase a cell phone and calling plan, you make some technical decisions. These mainly concern the handset and its features, plus a carrier for the network. Cordless phone shoppers have their own set of technological decisions to make, above and beyond the features offered by the model.

When shopping for cordless phones, you choose the frequency and sometimes whether the radio signals are analog or digital. Shopping for the phones in a store does little to narrow your decision making, other than deciding on the look and feel of the phone. Table 1-2 can help you start your comparison shopping before you set foot in a store.

Table 1-2: Pros and Cons of Cordless Frequency Bands

Band	*Pros*	*Cons*
900 MHz	Cheap, won't interfere with Wi-Fi	Usually little or no security, limited range
2.4 GHz	Price is right, more secure than 900 MHz secure	Possible conflicts with Wi-Fi
5.8 GHz	Clear, likely more secure	More expensive

You have an array of choices when purchasing a cordless phone. The important option is the frequency band on which the phones operates. Cordless phones are available in 900 MHz, 2.4 GHz, and 5.8 GHz models. Generally, as the frequency goes higher, so does the maximum distance you can take the handset from the base station, and the clarity gets better. Watch out, however, for interference from other sources of radio waves, physical structures like walls, and the weather.

Here are what the three frequency bands offer.

900 MHz

You can buy one of these phones pretty cheaply, but many manufacturers are phasing them out, favoring instead the 2.4 GHz and 5.8 GHz models. If you're on a budget, you can buy one of these analog models for less than you paid for this book — but I wouldn't recommend it (the phone, not the book).

Why? The prices of 2.4 GHz phones are very reasonable and cover a larger area with less likelihood of interference. Also, higher frequency phones offer more conversation security: It's fairly simple to listen in to a 900 MHz analog signal with the right equipment.

2.4 GHz

Quality and price meet here. This is the sweet spot for cordless phones; most of them made today operate in this frequency range. They offer more clarity and range than you get with a 900 MHz phone.

Given the number of 2.4 GHz models, you can find them in a wide variety of configurations, choosing the features you want and not paying for ones you don't need. You can buy 2.4 GHz phones in analog and digital models. These phones are also available in multiple-handset models, which let you

add more handsets as you need them. Some models let you have as many as eight — seemingly enough for every room of your house. While the additional phones need a nearby AC outlet, they don't each need a phone jack.

You can find 2.4GHz phones in a huge variety of configurations with any number of features. Some contain digital answering machines. Some allow you to add up to eight handsets to the same base. Extra handsets usually come with a charging dock for which you need an AC connection, but you only need a phone jack for the base station itself.

Unfortunately, phones that operate in the 2.4 GHz range can interfere with some Wi-Fi wireless networks (802.11b and 802.11g, but not 802.11a or 802.11n).

5.8 GHz

These phones have an exceptionally notable advantage over the other two kinds of phones: The 5.8 GHz band is less populated, but that's changing quickly. Along with an increase in clarity and distance, cordless phones using this frequency are the perfect fit for a home that has a Wi-Fi network and other interference on the 2.4 GHz band.

The 5.8 GHz phones tend to be feature-packed affairs that get expensive quickly, although with the frequency growing in popularity it's only a matter of time before cheaper 5.8 GHz phones emerge.

Featuring Cordless Phones

If the confusion over frequencies isn't bad enough, you have to decide between a myriad of features when shopping for a cordless phone. From caller ID displays to multiple-handset models, you have much to discover before plopping down your greenbacks.

You find some of the features on cordless phones:

- **Caller ID.** If you subscribe to caller ID service through your local phone company, this feature is a must. If the phone's not enabled for caller ID, subscribing doesn't make any difference. When you get an incoming call, the caller's phone number and possibly the name (if you pay for this service) appears on the handset's display.
- **Call waiting ID.** Call waiting ID is a cool feature. While you're on the phone with someone else, you can see who is trying to reach you by glancing at the display on your phone. If you want to take the new call, you flash over to the other line. When you're done, if the first caller is still waiting, you can flash back to him or her.

- **Digital answering machine**. I thought everyone who needs to record calls signed up for voicemail through their phone company. I guess not. Long gone are the days of cassette tapes; the answering machines built into these phones are digital, which have far less recording capacity. One benefit is that long-winded callers have fewer seconds to leave their messages, sparing you some rambling. Sometimes you can even set the length of messages your answering machine will take before cutting off the caller.
- **Multiple handsets**. You can do several things with these phones:
  - Add up to eight handsets (depending on the model) for use throughout your home.
  - Answer a call using any one of the phones.
  - Transfer a call to and from a handset.
  - Page a handset, making the setup similar to an intercom system.
  - Plug each handset's cradle into a power outlet; they don't require separate phone jacks.
- **Two-line phones.** These models can handle multiple phone lines. If you have a second line in your home, consider this feature. My household uses a two-line phone — one for business and faxing and the other for personal calls.
- **Speakerphone.** This feature is always handy, especially when stuck on hold with a credit card company or other sadistic entity. You can push the appropriate button and leave the handset in its cradle, using the speakerphone located in the base station. Better still are handsets with speakerphone built-in; you can carry them around and have speakerphone conversations while you do other stuff.

Avoiding Interference

As I mentioned earlier, if you have a Wi-Fi network in your house, I don't recommend the purchase of a 2.4 GHz cordless phone. If your household is constantly using a baby monitor, that could be a problem, too. Even microwave ovens, which operate on the same frequency, can create problems. Never situate the base of your phone near a microwave, because if somebody decides to heat up last night's dinner while you're on the phone, you'll experience loud and annoying interference.

If your analog phone has interference, you hear it as static and hisses. A digital phone will probably fade in and out or have a shorter range, or even cough up sounds like buzzing or beeping (but not technically static).

The best way to eliminate or reduce these kinds of interference problems is to move the phone's base station around the house, seeing if a different location makes any difference. If you already have a Wi-Fi network and purchased a 2.4 GHz phone without reading my wise admonitions beforehand, you still have hope. Just turn off the network when you're using the phone and vice versa (as annoying as that can be). However, you may find the two coexist peacefully.

Chapter 2: Picking Peripherals

In This Chapter

- **Cleaning off your desk**
- **Choosing wireless peripherals**

You may be focusing on Wi-Fi and Bluetooth networks and forgetting some of the more "peripheral" uses of wireless technology. In this chapter, namely, I'm literally referring to peripherals — for your computers.

A peripheral is really anything that's not an internal, integral part of your desktop or laptop computer. Examples include keyboards, mice, trackballs, external hard drives, speakers, and game controllers. (It also includes printers, but they're covered in Book III, Chapter 4.) While these all once were tethered to your PC via wires, more and more of them are sold in cordless versions. In this chapter I highlight a few of the cordless peripherals you can buy.

Unplugging Your Desktop

Logitech, one of the largest manufacturers of cordless mice and keyboards, has shipped literally tens of millions of cordless peripherals worldwide, including keyboards, mice, and trackballs.

You may see peripherals called cordless or wireless. I guess I like wireless because this book isn't called Cordless All-in-One Desk Reference For Dummies. It's a good thing, too, as I picture a cordless phone disguised as a Dummies book. I'd love the look — I'll gladly take a black-and-yellow phone any day — but holding a book to my head for an hour could be tiring.

Of course, some cordless peripherals still come with cords. The base stations usually plug into a USB port (found on the back or front of your computer) on your computer and then sit somewhere on your desk — but probably out of the way and out of sight. Others simply require USB dongles to communicate with your computer — no wires at all.

Seems logical

Logitech introduced the first radio-frequency (RF) cordless mouse in 1991 and the first cordless keyboard-and-mouse combination in 1998. Logitech cites a study showing that eight out of ten U.S. consumers know about cordless peripherals.

It's a sizeable market, with Logitech estimating that retail sales of cordless mice and keyboards total $230 million a year. That's a growth rate of nearly 50 percent. It seems I'm not the only one cutting the cords and opting for a wireless desk.

One of the annoying things about corded, or wired, peripherals is when you attempt to move a mouse but the cord is hung up on something else on your desk. As you pull the mouse toward you to move the cursor down, the mouse stops, the cursor stops, but your eyes (and sometimes your hand) keep going. This little disruption can totally throw off your suspension of disbelief if it happens when you're in the middle of a game.

Switch to a cordless mouse, and you'll never experience that particular problem again. Of course, cordless mice have their own issues, but I'll get to them a bit later.

Using a Cordless Mouse

Microsoft and Logitech are two of the largest makers of cordless mice. Various other companies manufacture similar cordless peripherals, including game controllers, which are described later in this chapter.

Microsoft mouse

Microsoft has a massive line of cordless mice, including things like the Wireless Laser Mouse 7000, the Wireless Laser Mouse 8000, and the SideWinder X8 gaming mouse. It also has cordless notebook mice, which are more compact versions of standard mice, such as the Arc Mouse and the Mobile Memory Mouse 8000. Many of these operate in the 2.4 GHz range and allow for up to 30 feet of wireless range.

Bluetooth peripherals work similarly to the cordless mice and keyboards I mention in this chapter A Bluetooth base station can simultaneously interact with several devices, including appropriately equipped cell phones and handheld computers. I discuss mice and keyboards that use Bluetooth wireless technology in Book VI, Chapter 5.

SideWinder X8 Mouse

A dedicated gaming mouse, the SideWinder X8 Mouse is equipped with a 2.4GHz connection, a tilt scroll wheel, 12 buttons (7 of which are programmable), and something called Play and Charge. That's a charging cable that allows you to continue playing even if the built-in battery dies during a gaming session.

The grooviest thing about this mouse is that the thumb buttons, traditionally placed horizontally along the left side of the mouse, are, in this mouse's case, vertically placed for easier access. With programmable mice, gamers can program stuff they'd normally have to do with the keyboard to mouse buttons. This includes in-game actions like jumping, changing movement speeds (walk/run), ducking, and so on.

Wireless Laser Mouse 8000

This killer mouse goes beyond optical tracking. Like most high-end, modern mice, it doesn't use a ball or a visible LED for movement; it uses a laser. This makes for much more precise tracking over just about any kind of surface you can imagine. The Wireless Laser Mouse 8000 also includes 2.5 GHz Bluetooth technology, a rechargeable battery, and more.

Logitech mouse

Logitech also has a wide range of wireless mice. You can order them online at `www.logitech.com`.

This itty-bitty, portable mouse is the exact mouse I use with my notebook computer. It's small, yet features big technology. It's a laser mouse, it comes with a USB receiver the size of a nickel (literally), it's oddly palm-friendly for its size, and it runs on two AAA batteries.

I just leave the little receiver plugged into my notebook's USB port all the time. When the computer goes to sleep, I just wiggle the mouse and it wakes right up. The mouse has two main buttons, two buttons nestled to the left of the standard left mouse button, and a scroll wheel with tilt sensors. (See Figure 2-1.)

It really has just about everything a full-sized mouse might feature, but it's pocket-sized and easy to bring around the house, or even anywhere to which I may travel, and to use with my Wi-Fi enabled notebook for computing all over the place.

Figure 2-1: The Logitech VX Nano Cordless Laser Mouse

Trackballs

I'm no expert, but I'd say trackballs are a niche market. If you haven't seen one, it's basically a mouse with the ball on the top rather than the bottom. The unit stays in place as you move the ball (and hence, the onscreen pointer) with your fingers.

Trackballs are good for precision work (graphical work) and certain games. However, if you don't know if you need one, you probably don't. Logitech has two wireless trackballs. One is the Cordless TrackMan Optical and the other is the Cordless TrackMan Wheel. The TrackMan Optical is the fancier of the two and costs about $10 on the street. The TrackMan Wheel has a street price of about $50. Both models have lots of buttons. The TrackMan Wheel has its ball on the left side instead of on top. You use your thumb to operate the ball, rather than your fingers.

Finding the Home Row: Keyboards

You also can find keyboards that are wireless. Want to know more? Read on!

Microsoft wireless keyboards

Microsoft sells wireless keyboards and mice as a set. It offers about a dozen sets, some of which are Bluetooth enabled. The sets have different features, depending on the price tags. They range all over the place, from basic sets to elite sets.

Some of the keyboard sets come in ergonomic models, which I can't stand. If you don't know what ergonomic means, you probably have seen one of the keyboards, anyway: The keys are split into two groups, positioned at angles that more closely mimic the normal angles of your wrists. They cut down on injuries to your wrist but also typing precision. Bury me with my Logitech Wave keyboard (below).

Logitech wireless keyboards

Logitech also has a range of cordless keyboards and keyboard/mouse sets. The standout is called the Cordless Desktop Wave (See Figure 2-2). The Wave keyboard comes in a corded version; the Wave desktop has the same keyboard in a cordless form and a mouse to go with it. I prefer a different mouse, so I use the Wave keyboard without the mouse that came with it. Call me a rebel.

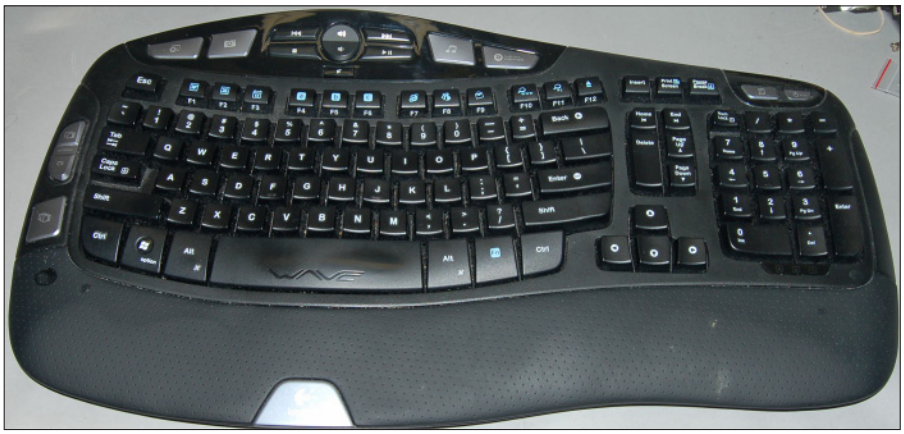


Figure 2-2: Cutting the cord with Logitech's Cordless Desktop Wave keyboard (it looks beat up, but it's actually well loved)

Book VII

Wireless Home Technology

"Good news! I found a place where the router works with the PC upstairs and the one in the basement."

Contents at a Glance

Chapter 1: Entertaining Yourself Wirelessly

In This Chapter:

- **Starting out with digital music**
- **Deciding between wireless and wired**
- **Finding out about digital media adapter basics**
- **Using other gadgets**

Your network is set up and ready to go. You're surfing the net wirelessly from your laptop. Maybe you've got music streaming from your desktop PC to your laptop.

One problem: the home theater is in your family room. You have content on your PC that you'd love to see on the big screen TV, but getting said content from one to the other seems like a major chore.

The real chore is not streaming the video or music to your home theater. Once you have your network set up to talk to your entertainment system, streaming is easy. What's hard, then?: asking the right questions.

In the next few chapters, I take a look at specific devices and show you how to set them up and connect to your wireless network. Think of these as examples; you may choose different gear, but the principles of installation and setup are the same.

In this chapter, I cover some basic knowledge, so you can understand exactly what I'm trying to do.

Entertaining the Wireless Way

The goal for a wireless entertainment experience falls somewhere between listening to audio on your $20 computer speakers and having a full-featured home media PC running a special version of Windows XP connected to your entertainment system. With the former, you get poor sound but few setup hassles. With the latter, you must invest much more money — at least

around $1,000 — to get a computer that directly feeds music, photos, and videos into your home entertainment center. (In fact, the home media PC becomes part of your home entertainment center.)

Instead, you want to take the content that already lives on your PC and deliver it to that home entertainment center. Most of the products I discuss are a compromise between those two extremes. You get the advantages of a dedicated device that does a few things very well with minimal hassle and that costs less than a full-fledged Media Center PC. Figure 1-1 shows a typical media player configuration on a wireless network.

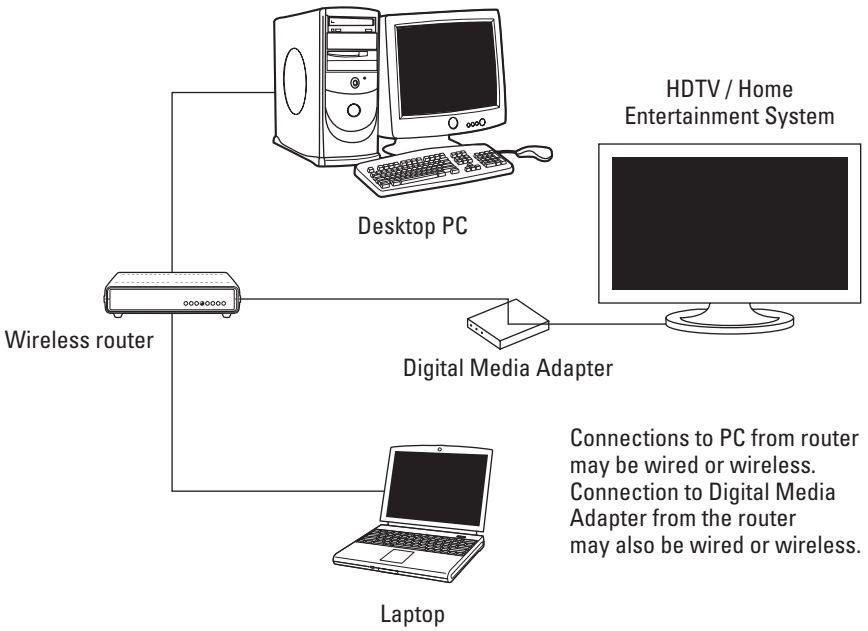


Figure 1-1: PCs connect to the digital media adapter over the home network.

Starting out with digital music

You choose your media adapter based on the type of content you want to play. If most of your music is bought or ripped from CDs using iTunes, you want a player capable of playing back music encoded with Apple's AAC format. If your music is in Windows Media Audio (WMA) format, make sure that your player can handle WMA playback.

A word on formats

CDs are easy: There's really only one type of audio CD, known as Red Book Audio CD, which is the actual color of the cover defining the CD audio standard. You buy a CD, and you can pretty much pop it into any CD player and feel confident that it will play.

The world of digital music is less well defined. When you rip a CD onto your computer, it may be stored an one of a number of different competing formats. Apple's iTunes, for example, uses AAC (Advanced Audio Coding) as its normal format. Windows Media Player and Microsoft's Zune software encode music in WMA (Windows Media Audio).

The reason for competing formats is so that the companies can protect the music from unauthorized copying — this is also called DRM (digital rights management).

The closest thing to a universal standard for compressed music files is MP3. MP3 is MPEG-1 Audio Layer 3 and was developed by the Moving Pictures Expert Group, a standards organization that has developed a number of audio and video standards over the years.

So if you want to buy hardware to play back the music you've stored on your PC, you'll need to understand what format is being used.

Note that all digital media players understand MP3, which is perhaps the most common format for storing digital music.

There are wrinkles and variations to even the most common formats. For example, WMA can rip music from CDs *losslessly*. Apple's iTunes also has a lossless ripping format available. Most music compression schemes throw away some data — usually not data that affects the actual sound. However, audio purists prefer formats that keep *all* the data. These lossless formats include Apple Lossless, WMA Pro Lossless, and FLAC (free lossless audio codec). Even players capable of playing WMA sometimes can't play back music files encoded in WMA Lossless format, so be aware of your digital music players' limitations.

Another potential sore spot is *digital rights management*, or DRM. DRM is a way of preventing unauthorized copies of digital content. Until recently, all music bought from the iTunes store was protected with a DRM scheme called FairPlay. Most digital media players that can play back AAC-encoded music can't play back music protected with FairPlay DRM.

Hardware support for playlists

In addition to the music itself, everyone makes playlists. You might be hosting a party and want to have a long playlist of catchy songs to set the mood. You might be working and want a background music playlist. There are three common playlist formats: M3U, PLS, and WPL. If you do make extensive use of playlists, you'll want your DMA to handle the format you use.

The good news is that Apple now offers most of the music you can buy from the iTunes store in unprotected AAC. Microsoft is a little behind the curve but is starting to add unprotected music. Note that Amazon.com's MP3 download service sells all its songs in MP3 format with no DRM added.

Every picture tells a story

You know that big box of photos you have somewhere that you plan to organize any day now? Well, that day has arrived. Now that you can view your photos on your TV screen, why not take the time to scan in your photos so they're available for use by these gizmos?

Both Windows and Mac have some fine software packages that help you organize your photos. You can scan them on a scanner, make some changes (like eliminating that dreadful red eye that happens when you use a flash), and organize them.

Adobe Photoshop Album (`www.adobe.com`; about $50) and Google's free Picasa (`www.picasa.com`) software are both excellent photo management applications. Your printer may have shipped with one as well. The popular formats for photos include the following:

- **JPEG:** JPEG is the most common compressed format for digital pictures and was developed by the Joint Photographic Experts Group. High levels of compression can reduce picture quality.
- **TIFF:** TIFF (Tagged Image File Format) is a picture format originally developed for scanners. TIFF supports file compression, but not at the cost of image quality.
- **BMP:** BMP stands for "bitmap" and was a picture standard developed for Microsoft Windows.
- **PNG:** PNG, or Portable Network Graphics, uses lossless compression to make picture files smaller but maintains a high level of image quality. It's not commonly used in cameras but is used often in Web design.
- **RAW:** This is the pure, unaltered digital sample recorded by the camera during exposure. Every camera company uses a different raw format. RAW format is used mostly in digital SLRs.

The good news is that most digital media adapters capable of showing pictures handle most of the common picture formats. The confusion and variations in standards that prevail in the digital music world aren't quite as common in the arena of digital photos.

Hollywood on a hard drive

Video and wireless networking are not quite like water and oil, but they're close. If you're going to move around video files on a wireless network, bandwidth on the wireless network becomes important. If you have enough bandwidth, your video playback is smooth and uninterrupted. If you don't, the video will become jerky, frames will be dropped, and the whole experience will be terrible.

Early wireless routers and access points supported a standard called 802.11b, which maxes out at 11 megabits per second (mbps). At first blush, 11 mbps sounds good enough, but it really isn't. The best DVD quality video pushes a maximum of over 9 mbps, and high-definition video can exceed 20 mbps.

When 802.11b was released, another standard known as 802.11a also became available. Although 802.11a supported bandwidth up to 54 mbps, it wasn't common in home networking products, since it was mainly targeted for corporate use.

Since 802.11b, two newer wireless networking (Wi-Fi) standards have emerged suitable for home wireless networks: 802.11g and 802.11n. 802.11g boosts bandwidth up to 54 mbps (double that for some products), while 802.11n supports throughput as high as 600 mbps, although most current products max out at around 256 mbps.

Book II, Chapter 2 talks about 802.11 options in depth.

The throughput differences between the technologies (b, g, and n) are striking, and you'll definitely see an improvement with 802.11g networking equipment, and even more with 802.11n. If you're streaming video in real time you almost certainly need 802.11g equipment or better.

What kind of video can you watch on media players? Just about anything your media player can read. You may want to watch some home movies you've converted into digital format, for instance. A number of online movie rental and streaming services now exist, including services from Amazon, Hulu, iTunes, Xbox 360, and Netflix.

More video services are sure to follow, especially given Hollywood's concern about content transferring illegally over peer-to-peer networks. As Apple's iTunes music store has shown, people will pay for content. They're willing to go the legal route as long as the options are there.

Some of the more popular video formats include the following:

- **MPEG (MPEG-1, MPEG-2):** Commonly used in Web video, DVDs, and other common commercial applications.
- **MPEG4:** AVCHD high-definition standard, plus portable media players, including the iPod and Sony PSP.
- **WMV (Windows Media Video):** Used by Microsoft's Windows Media Player.
- **ASF (Advanced Systems Format):** Another Microsoft standard for digital containers for streaming video.
- **AVI:** Audio/video interleave is an earlier format for Windows video file.
- **Xvid / DiVX:** These are based on MPEG-4, but with proprietary extensions. They support high levels of compression with good quality.

There are more wireless media players that play only music than that play both music and video. That's partly because manufacturers — at least until recently with the growing popularity of 802.11g — probably felt they couldn't meet the expectations of non-geeky consumers. After all, video takes substantial bandwidth, which wired Ethernet and, in most cases, 802.11g can deliver.

Ultimately, though, keep it simple. It may sound really cool to first rip a DVD onto your PC's hard drive and then stream that movie wirelessly to your home entertainment system. In practice, it's far easier to just pop the DVD into your home theater system's DVD player — and you have all those nifty extras, which is often the real reason to own the disc.

What's important is to create an environment that works seamlessly and without a lot of unnecessary tweaking. If you have video content that is only available by streaming, by all means, go for it. But if you have to turn on your PC every time you simply want to watch a movie, there may be easier solutions.

Chapter 2: Streaming Digital Music in Your Home

In This Chapter

- **Serving up your digital music**
- **Sharing over your network**
- **Exploring digital music hardware options**

Wouldn't it be great to walk from your kitchen to your bedroom, then down to your family room, and be hearing music throughout your house? What if you could be listening to Miles Davis in your home office while your daughter listens to her favorite music in her bedroom? You can have all of this, using your wireless network, your PC, and networked digital music players.

This chapter explores the ins and outs of listening to music stored on your PC, anywhere in your home. You've invested your time and money to buy and download music from iTunes, Microsoft's Zune service, Rhapsody, or other music services. Or maybe you've spent all that time ripping your massive CD collection onto your PC. Sure, you can listen to it in your portable music player, but why not listen to it on your home theater system, too?

Serving Up Your Digital Music

You've been busy ripping your entire CD collection using your favorite music player software. You've also bought digital music, perhaps from a variety of sources. That iPod or Zune player is an inseparable companion. But you can't help thinking that something is missing, as you pop one of your music CDs into your CD player in your home entertainment system.

Stop right there. Why are you still using CDs to play music on your large format audio speakers? You can have your entire digitally ripped music collection, with your customized playlists, playing on those superb-sounding home theater speakers that grace your living room. Banish your CD player forever, and replace it with a modern digital music player.

Dealing with DRM

One of the problems with iTunes and other paid music services was the issue of content protection, known as DRM (digital rights management.) A song bought from the iTunes store was almost always protected with Apple's own DRM scheme, known as FairPlay. Although you could play that music on Apple players — iPods and iPhones — you couldn't play protected music on networked devices.

Note that both WMA and AAC can have DRM assigned to specific music files. Networked digital music players usually cannot play DRMed content, so I suggest either paying a little extra money to buy DRM-free music, ripping your music from CD or burning an audio CD, then re-ripping that CD into a DRM-free format.

Recently, though, Apple has removed content protection from most iTunes music. There's still a lot of music out there on players that still have FairPlay DRM, however, so unless all those users re-buy their music, FairPlay will be with us for some time.

The choice of the best digital music player depends on what digital format you've been using for your music, which I discussed in Chapter 1 of this minibook. The other piece of the puzzle is how music is delivered from your PC (or another source, such as network attached storage) to your home entertainment system. That also depends on the digital music format you use and what software.

Using music software

More people use iTunes than any other digital music application. It's available on both Macintosh- and Windows-based PCs. iTunes is tightly linked to the iTunes Store, where content can be purchased for instant download. But you can also use iTunes to rip your CD collection.

iTunes uses two different formats, depending on how you rip the music from your CD. One is known as Advanced Audio Coding (AAC), the other is Apple Lossless. Apple Lossless offers better sound quality, because its compression doesn't throw away data. AAC, like MP3, discards what it thinks is redundant data. Usually, the result can sound pretty good, but I'd suggest using the highest possible bit rate for the best results.

Microsoft's Windows Media Player and the Zune player both use Windows Media Audio (WMA) audio format. Windows Media also offers a lossless compression option for the best possible sound quality.

One other option for lossless compression is known as FLAC (free lossless audio codec). FLAC is, as the acronym hints, free. It's widely supported by many digital media players, but you need either a plug-in for Windows Media Player or some standalone application to rip your collection into FLAC format.

You can use a number of ways to get your music from your PC to your home entertainment center; all do require additional hardware. I look at two examples of how you can do this: Logitech's Squeezebox and the Sonos Music System.

The Logitech Squeezebox

The original Squeezebox was developed by a company called Slim Devices prior to being acquired by peripheral manufacturer Logitech. The philosophy behind the Squeezebox was to make it simple to play your digital music anywhere in the house and to make the options flexible.

Currently, a number of Squeezebox products exist: Squeezebox Classic, Squeezebox Duet, Squeezebox Touch, Squeezebox Radio, the Squeezebox Boom, and the Squeezebox Transporter. In this section, I cover how to set up the Squeezebox Duet, a compact, two-piece unit with a remote control that behaves much like a portable digital music player, shown in Figures 2-1 and 2-2.

The Duet's receiver fits easily into small spaces and connects up to either an A/V receiver or to powered speakers. In our hookup, the Squeezebox duet is connected to an A/V receiver equipped with a pair of stereo speakers.

Figure 2-1: The Squeezebox Duet consist of the receiver box and a remote with iPod-like controls and a small LCD screen.

Figure 2-2: Squeezebox connections.

The Squeezebox can be connected via Wi-Fi but also has a built-in wired Ethernet connection. Audio output is either through a pair of analog stereo RCA connectors (for powered speakers) or your choice of digital coax or digital optical cables (for connecting to an A/V receiver).

That's the Squeezebox Duet hardware. I show you how to use the hardware shortly. But first, you have to set up the software that enables music playback on the Squeezebox, which is called *SqueezeCenter*. (You may see references online to *Slimserver*, which is the old name for SqueezeCenter.)

Setting up SqueezeCenter

You can install SqueezeCenter from the CD that ships with the Squeezebox or download the latest version from the Logitech Web site (`www.logitech.com`).

The installer is a standard Windows installer, so after launching the installation, just click next and pick the default locations. At the end of the installation process, SqueezeCenter will launch. SqueezeCenter is actually a Web-based application, so don't be surprised if your favorite Web browser fires up at this point.

Now you have to make a decision: Where is your music?

Most people have their digital music stored in whatever default location used by their digital music software. For iTunes running in Windows Vista,

that's usually Users➪<your user name>➪Music➪iTunes➪iTunes Music. For Zune, it's Users➪<your user name>➪Music➪Zune.

Alternatively, you may choose to have your music live on a home server or network-attached storage device (NAS.) That's my choice for storing music. It's convenient, safer than my desktop PC, since the NAS unit offers redundant storage, and accessible even when my PC is turned off. However, SqueezeCenter does require your PC to be running.

To use a network storage location, you first need to set up your network location as if it were a hard drive on your local PC; this is known as *mapping a network drive.* Simply open up your network location as you usually do, then right-click on the network folder and choose Map Network Drive, as shown in Figure 2-3.

Windows Vista calls user directories simply "music" or documents. Windows XP called its user folder "My Documents" or "My Music." Windows 7 returns to this naming convention. So the iTunes music folder above would be Users➪<your user name>➪My Music➪iTunes➪iTunes Music.

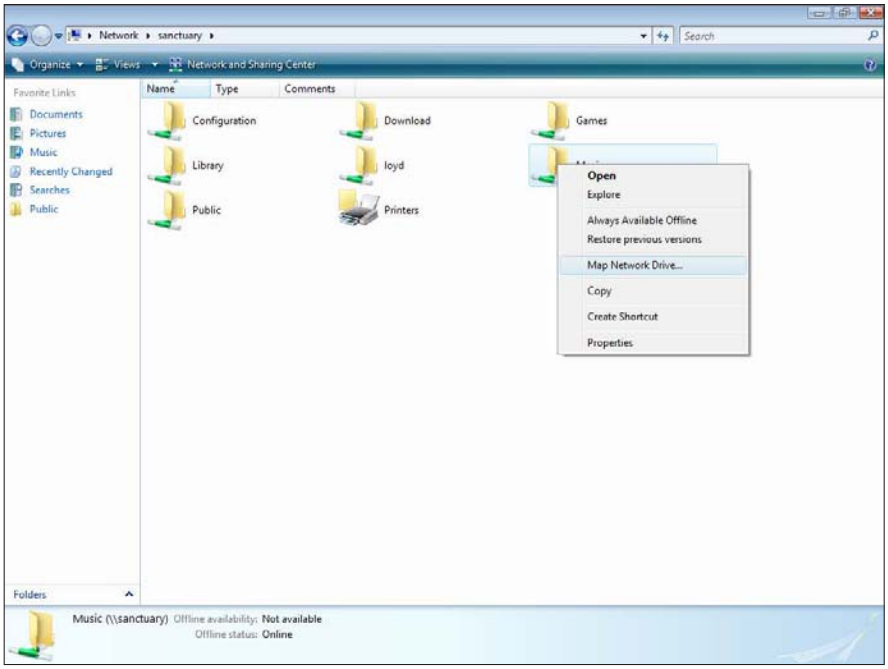


Figure 2-3: Mapping a network drive to a drive letter

For the purpose here, I assigned drive letter G: to the music folder on the network. Any drive letter will do.

Now that a drive letter is assigned, let's set up SqueezeCenter. If the application hasn't already launched, go ahead and run it from the icon on your desktop or the start menu. I'm skip the Internet access bits for the time being and get to what that means in Book VII, Chapter 4. Right now, you just want to play the music you've stored on our local system or home network.

1. **Because my own music is ripped in Windows Media Lossless format, I click the first check box. If you're an iTunes user, click the second box, which allows SqueezeCenter to use iTunes. (See Figure 2-4.)**
2. **The next two steps look identical: Choose a folder for your music location and then repeat the step for your playlist location.**

   In most cases, your music and playlists are in the same root folder. If you've stored your playlists in a different location than your music, you need to specify this in the second window, Local Playlist Folder shown in Figure 2-5.

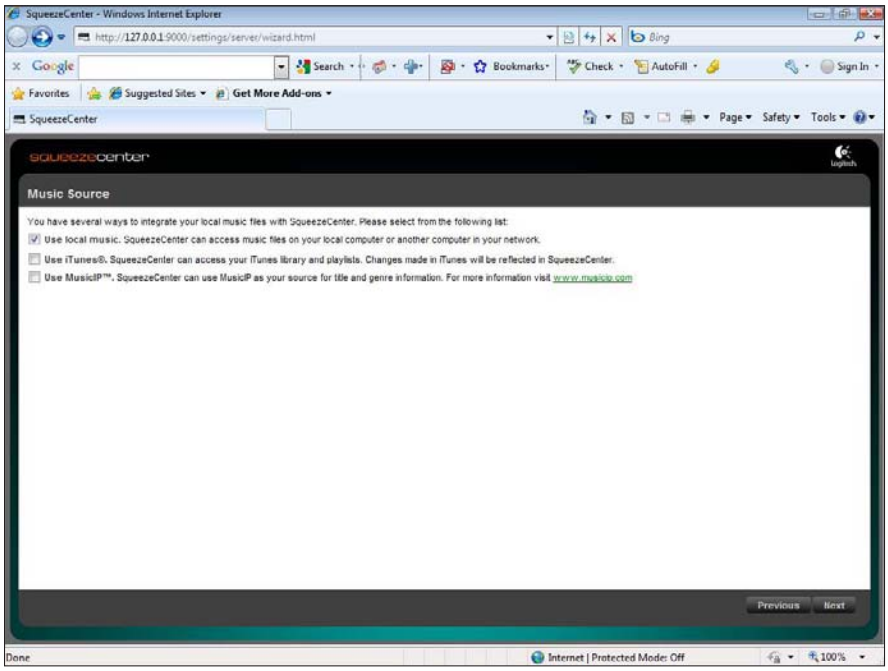


Figure 2-4: SqueezeCenter setup: choosing your media type

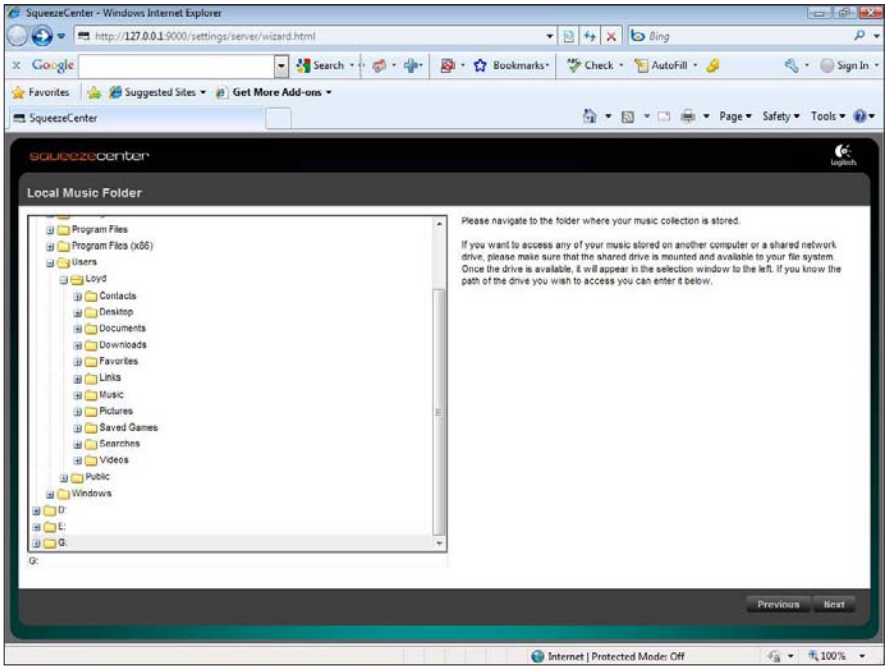


Figure 2-5: SqueezeCenter setup: choosing your music and playlist folder location.

When you click next after choosing your music folder, the screen will look the same, but the screen title changes to Choose Playlist Folder.

3. **Now you can just click through.**

   SqueezeCenter scans your music folders, which can take a few minutes or over an hour, depending on how much music you have. Eventually, you'll see the main SqueezeCenter screen populated with album art (if you click on "Albums"). (See Figure 2-6.)

SqueezeCenter for network storage

Customized versions of the SqueezeCenter exist for non-Windows PCs and other digital appliances. For example, a version exists for NETGEAR's ReadyNAS line of network-attached storage devices, which have a version of SqueezeCenter running directly on the ReadyNAS hardware. If you have such a supported device, then your Squeezebox can play music directly from the NAS device, and you don't need to have your PC running. Check the Logitech support site for more information. Note that the number of devices supported is limited, so if you like this idea, make sure the NAS box you're considering supports SqueezeCenter.

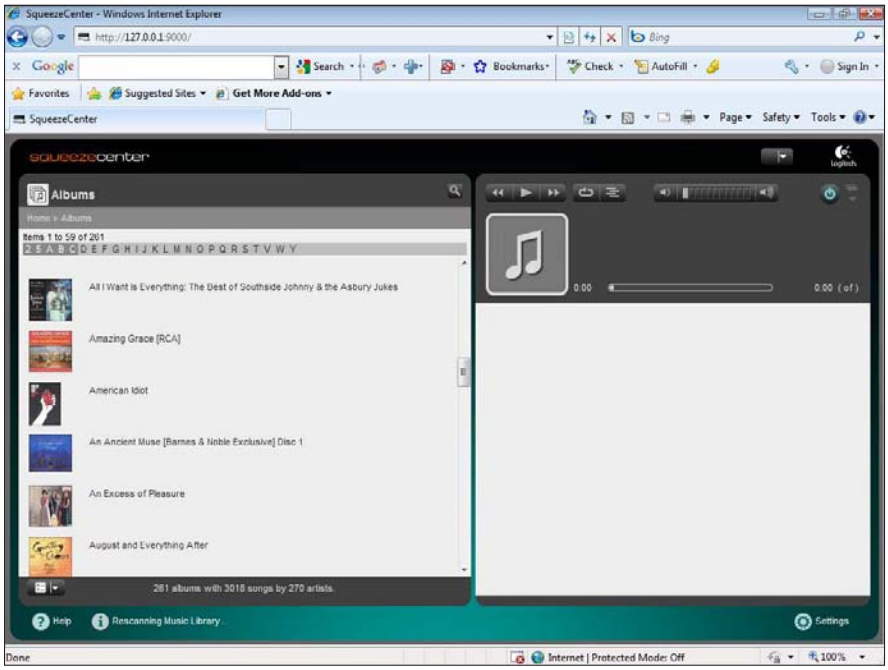


Figure 2-6: SqueezeCenter running

Setting up your Squeezebox Duet

Connecting up the Squeezebox hardware is simple:

Attach the analog stereo RCA cable or the correct digital cable to the input on the powered speaker or receiver. For example, on my system, I have the Squeezebox connected via a copper RCA digital coax cable to an input on my Onkyo A/V receiver — one that's set up normally for a CD player.

If you've just unpacked the Squeezebox Duet, plug in the charging stand and charge the remote control for a few hours. The unit ships with two small power bricks — one for the remote charging cradle and the other for the Duet receiver. While the receiver needs to be near your home audio system, the charging stand for the cradle can be located anywhere in your home.

While the physical connections are easy, connecting to your wireless network is a little more work. The Duet Remote has a small color LCD display and controls that allow you to navigate through the setup process. Stepping through the setup is pretty straightforward, but you have to know three things to connect the Squeezebox:

- **Your SSID.** The SSID is the name that your router assigns to the wireless network. It may be something as simple as your router's model name (such as D-Link DGL-4500) or some name you entered when you first set up the router.
- **Your security code.** If you're using WEB or WPA security, to prevent outside intruders from gaining access to your router, you'll need to enter the WEP or WPA key.
- **The system name or IP address of the system that's hosting the SqueezeCenter software.** Note that the Squeezebox remote will try to find this, but you may need to manually enter it.

All this assumes your router is set up to automatically assign IP addresses to new devices on the network — most routers do.

After your Squeezebox is connected to the network, you can use the scroll wheel and buttons to easily navigate to albums, artists, or playlists and begin listening to your digital music collection on your home audio system. Now you can enjoy your audio collection using the full range of your best speakers.

Using the Sonos Music System

The Squeezebox is a cool standalone digital music player, but what if you want to have your digital music play back in multiple locations throughout your home? One solution is the Sonos Music System (`www.sonos.com`.)

The Sonos Music System can be wired or wireless but works very well in a wireless environment. Each Sonos unit can find other Sonos devices on the network, creating what's known as a *mesh network*. If you have a large house that may have spotty Wi-Fi coverage, each Sonos box can relay the signal to the next one, filling in those Wi-Fi holes in your network coverage.

Why would you want a Sonos system? Simple: It's easy to control multiple ZonePlayers using a single remote control. You can have different ZonePlayers play different songs or playlists in different rooms. If you like, you can add additional remotes, so your spouse can have his or her own. But one remote can control multiple players, wirelessly (see Figure 2-7). And the remote is not an IR remote, but uses a radio signal, so you don't need line of sight.

Figure 2-7: The Sonos remote control.

The basic Sonos bundle consists of a ZonePlayer 120, a ZonePlayer 90 (Figure 2-8), and a controller. The ZP120 actually has a built-in digital amplifier, so you can connect them to bookshelf speakers anywhere in the house. The ZP90 is designed to connect to either powered speakers or a home audio system with an A/V receiver.

Figure 2-8: The Sonos ZP90 does require either amplified speakers or connection to an A/V system.

Setting up a Sonos system is even simpler than setting up a Squeezebox. First, plug in the remote control cradle into wall power and charge the control unit. While that's charging, set up the ZonePlayers. In my house, I used a pair of ZP90s attached to two different rooms. One was attached to my home

theater system, with a large A/V receiver and a 7.1 surround sound system. The other was attached to a smaller powered receiver that only had stereo speakers.

In both cases, the ZP90s were connected to the receivers via digital audio connections.

Once the remote is charged and the ZonePlayers connected, you pop the Sonos installation CD into your PC and run the setup application. Follow the prompts — they're very simple.

During setup, the Sonos software will locate all the ZonePlayers and configure them. You may need to verify a player's existence by walking up to it and pressing a button on the front during setup. (See Figure 2-9.)

As with SqueezeCenter, you need to tell the Sonos software the location of all your digital music files, which can be on the local PC or on a network storage device.

Figure 2-9: The Sonos software interface. You can set up playlists and manage music on your PC.

Unlike the SqueezeCenter, the Sonos natively recognizes file systems on network-attached storage devices. So if your music is on an NAS device, you don't need to have your PC running.

Sonos now offers an iPhone/iPod Touch application to control ZonePlayers, so you don't even need to use the bulkier Sonos control unit, though the Sonos remote is a little easier to use than the iPhone app.

At first, spending $999 or more on a Sonos bundle seems pricey. After you get whole-house audio running, controlled by a single remote control, you'll wonder why it costs so little.

A Word on Audio Quality

The era of digital music began when most people connected to the Internet via 56kb per second (or slower) modems. At that time, a 40GB hard drive was considered huge. So it was natural that the first digital music formats available on the Internet were highly compressed files.

When iTunes first started, the only format supported by the iTunes store was 128kbps AAC audio. On some music, you could actually hear artifacts in the music created when the compression software threw away what it thought was empty data.

Now, you have high-speed broadband connections and hard drives as large as 2TB. There's no need to squeeze your music so hard that it loses real data.

Today, several formats exist that compress audio *losslessly*. This means that any data that represents actual music is retained. However, music compressed with WMA Pro Lossless, Apple Lossless, or FLAC (free lossless audio codec) are considerably larger than the highly compressed music you buy from the iTunes or Zune stores.

If you like the idea of lossless compression, you can set iTunes, Windows Media Player, or the Zune Player to compress in the company's respective lossless format. One source for buying digital music is losslessly encoded, MusicGiants (`www.musicgiants.com`). The library at MusicGiants isn't as large as the iTunes or Zune stores, however.

After broadband becomes ubiquitous, maybe losslessly compressed options will become part of the mainstream stores as well. Your ears will thank you.

Chapter 3: Networking Your Television: From PC to HDTV

In This Chapter

- **Understanding PC video formats**
- **Maximizing your viewing experience**
- **Digital Media Adapters: Getting video from the PC to your HDTV**
- **Game consoles for watching PC video**

Streaming video over wireless networks is much more challenging than audio. Even full CD audio only pushes 176KB (that's kilobytes) per second — hardly enough to challenge even an old 802.11b network in home environments. Newer 802.11g or 802.11b networks can handle multiple users and multiple CD-quality audio streams.

Video is another beast entirely. DVD-quality video, which is already compressed with the lossy MPEG-2 codec, can consume as much as 9.8MB, or over 1.2MB. If you're thinking about streaming high-definition video, you're looking at bit rates that can approach 20 Mbps. Some pristine, well-mastered Blu-ray discs approach 40 Mbps.

Then there's the issue of quality of service. Quality of service, or QoS, is a nebulous term that tries to capture the idea that your video should look good. If you've ever watched a video streamed from the Internet, and noticed lots of interruptions or breakups in the picture, that's poor quality of service. All the bandwidth in the world isn't useful if your video stream keeps getting interrupted. Modern wireless routers and streaming applications are built to try to maintain a high level of QoS.

In this chapter, I show you how to maximize your viewing enjoyment while streaming video captured on your PC to your living room over your network. You find out about video formats, how to enhance your PC to maximize throughput, and examine a couple of sample scenarios using existing hardware.

Understanding PC Video Formats

As with audio, video is captured and stored on your PC in multiple different formats. My goal is not to exhaustively cover all possible formats, but to

explain the basic concepts in the context of getting that video from your PC to your home entertainment center.

In the old, pre-digital TV days, television was broadcast in purely analog formats. If you wanted to record and store an analog TV signal on your PC, it needed to be digitized. A number of different encoding methods emerged to convert the analog TV signal to digital format.

The key commonality is that all of these formats used some form of compression — usually lossy compression, which meant some of the data was actually discarded. Techniques such as MPEG-1, MPEG-2, WMV, and H.264 can predict what the pixel will look like five frames after the current one is displayed, so don't try to save the pixels in the four intervening frames.

What this actually means is that lossy compression can help reduce the bandwidth needed to stream video. Unfortunately, HDTV streams are *already* heavily compressed. A typical over-the-air high-definition broadcast can hit 20 Mbps. A cable or satellite HD stream ranges from 5 to 13 Mbps.

Windows Media Center in Windows Vista and Windows 7 can capture high-definition broadcasts using PC capable tuners. If you want to capture digital cable TV shows, you need a tuner capable of ClearQAM capture. Those shows need to be unencrypted.

There are PC models built with Windows Vista that can use CableCard to capture premium shows which are encrypted by the cable TV provider. But you have to buy those PCs as a unit — you can't add CableCard support to an existing PC.

Of course, you won't want to simply watch TV shows streamed from your PC. While the PC can work perfectly well as a DVR (digital video recorder), it's more interesting to use the PC to store and show videos you, your family, and friends have shot using digital and high-definition camcorders.

However you get the video into your PC, the tricky part is streaming it from your PC to your family room.

Using a PC to Maximize Your Viewing Experience

Before diving into how to display the video streamed from the PC to the home entertainment system, I need to talk about the PC that will be delivering the video.

People often just take whatever PC is handy — the home office PC, their laptop — and try to stream video to the TV from a general purpose PC. The result is often choppy video with strange compression artifacts. Now, you don't need a dedicated video server. Your home office PC might be good enough, but you'll need to tweak it a bit for best delivery of video content.

Here's a brief rundown on common digital video formats:

- **MPEG (including MPEG-1, MPEG-2, and MPEG-4):** Developed by the Motion Pictures Expert Group, the various MPEG formats are perhaps the most common encoding scheme. DVDs use MPEG-2; some Blu-ray discs are encoded in MPEG-4. Satellite and cable TV often deliver their video in MPEG-4 format.
- **WMV (Windows Media Video):** Microsoft's proprietary video compression format.
- **H.264:** This is a variant of MPEG-4, used in some Blu-ray movies and online video.
- **AVCHD:** This format is common to high-definition camcorders and is actually one form of H.264/MPEG-4.
- **DiVX:** This compression format is most commonly used on the Web, so if you download videos from the Web to your PC, they may be DiVX encoded.
- **Flash and Silverlight:** These are almost exclusively used for streaming video over the Web, and it's unlikely you'll be doing much downloading of Flash or Silverlight video. Flash is a proprietary video format owned by Adobe, while Silverlight is a Microsoft product.
- **AVI, QuickTime, and Transport Streams:** These are container formats — that is, they are wrappers around a compressed video stream (like MPEG, WMV, or DiVX). If you've ever wondered why your system can play some AVI files but not others, it's probably because the codec (*compressor-decompressor*) needed to decode a particular format isn't on your system.

To properly decompress and view a video file, you'll need the right codec software. As noted above, just because you can play a container format like QuickTime doesn't mean that you have the correct codec. Modern operating systems, like Windows 7, have become much smarter about codec support, so it's worth running Windows 7 if only to avoid having to hunt and download the right codec to playback your video.

CPUs versus GPUs

You may have heard that graphics processors — the chip that powers the graphics card in your system — are capable of handling those processor intensive transcoding chores. That's true, to an extent. A high-end graphics processor, such as an AMD Radeon 4890 or Nvidia 260 GTX Core 216, is actually a lot faster at most video transcoding than even fast quad-core CPU. However, only a few applications support the use of video cards for transcoding on the fly, and none of them are streaming applications — yet. But it's worth keeping an eye on this rapidly developing area.

Now that you have some understanding of video formats, you need to know what your eventual target device will be. For example, if you know that you're using a Windows Media Center extender, you know it will support Windows Media Video, MPEG-1, MPEG-2, and possibly MPEG-4. It may not directly support AVCHD, which is the format that high-definition camcorders use. For our purposes, this is really all you need to know about compression schemes.

If you are sure all formats you use are directly supported by the digital media adapter, then the PC just becomes responsible for streaming the data. That's a fairly straightforward process, and optimizing for sending out one or two video streams is fairly simple — I'll get to the specific shortly.

On the other hand, if your target device doesn't support the format directly, you'll need software on the PC that will *transcode* the format on the PC to one that the display device will understand, then stream it to the device. What's more, the transcoding will typically happen in real time.

It works like this. As you request a video from your PC, the PC knows that it needs to transcode the file to a format the display hardware understands. The transcoding is performed on the fly and then streamed to the TV. Some software needs to do this every time the video is streamed. Other software will cache the transcoded files, so the next time you want to watch, it becomes an exercise in simply streaming the file.

All this sounds complicated, but the right combination of hardware, once properly set up, just works. All the transcoding, streaming, and other background tasks occur silently, without fuss, when you press the Select button on your remote control to play the video.

Maximizing streaming performance

You want the video stream to flow without interruptions. Ensuring your PC can send the video stream consistently, and without hiccups, is fairly straightforward. Here's what you need to do:

- **Set up a regular schedule to defragment the hard drive.** As video is recorded to the system's hard drive, then deleted, then re-recorded, parts of newly recorded videos can be spread out over large areas of the drive. This can result in poor streaming performance and choppy playback.
- **Use a big hard drive.** If you're capturing high-definition video streams, the bigger the hard drive, the better. Part of the problem is that a drive that's almost full (or more than three-quarters full) tends to fragment more easily.
- **Minimize background services.** This is particularly true if you have an older or lower performing processor. For example, a typical desktop PC really doesn't need to run SmartCard services, telephony services, remote desktop services, Tablet Input Services, and others. Shutting those down will save memory and CPU cycles.

Maximizing transcoding performance

If your needs require the system to transcode a file into a different format before streaming, then you'll need a beefy CPU and lots of memory. If you can swing a midrange quad-core processor or a high-end dual-core CPU, and 4GB of RAM, you'll be in good shape.

This is particularly true if you plan on transcoding and streaming high-definition formats. For that, you'll definitely want a quad-core CPU, with at least 4GB of RAM, running a 64-bit operating system.

Why a 64-bit OS? The streaming and transcoding apps, like those that ship with products like the Sage TV HD Media Extender, aren't really 64-bit apps yet. But a 64-bit operating system (such as Windows 7 Home Premium 64-bit) actually gives a little more memory to 32-bit applications. And it won't be long before media applications move to 64-bit.

Of course, you'll also want to apply the tips and tricks I mentioned earlier for purely streaming applications as well.

Now that you've taken a look at video formats and system tuning, let's look at three examples of hardware and software combinations for watching PC video on your HDTV.

Media Center Extenders

I'm using the term *media center extenders* generically, not just the Microsoft Windows Media Center variety. I show you two scenarios. One is based on a Windows Media Center Extender by D-Link. The other is the Sage HD Media

Extender. Then I'll look at the issue of using a game console to stream video from the PC to the HDTV. Figure 3-1 shows some example hardware.

Sage TV HD Media Extender

Sage TV has made something of a reputation for being an alternative to Microsoft's Windows Media Center. On the one hand, the user interface tends to be just a little less polished than Windows Media Center. On the other hand, it's more powerful and flexible, allowing for heavy customization and offering very granular settings.

While you can use the Sage TV software on our PC, our focus here is using it in conjunction with Sage TV HD Media Extender. Setup is somewhat convoluted. First, you need to install two pieces of software on the PC that serves up the content: Sage TV and Sage TV Placeshifter. Installed along with Sage TV is the Sage TV server. The server is somewhat inflexible in that all content must reside on the PC where Sage TV is running. So you can't use network-attached storage to store your video content.

What Sage TV offers is control over a vast array of features. The setup menu is one of the most complete I've ever seen (see Figure 3-2).

Figure 3-1: Streaming video hardware: from top to bottom, the Xbox 360, the Sage TV HD Media Extender, and the D-Link HSM-750 Windows Media Center Extender.

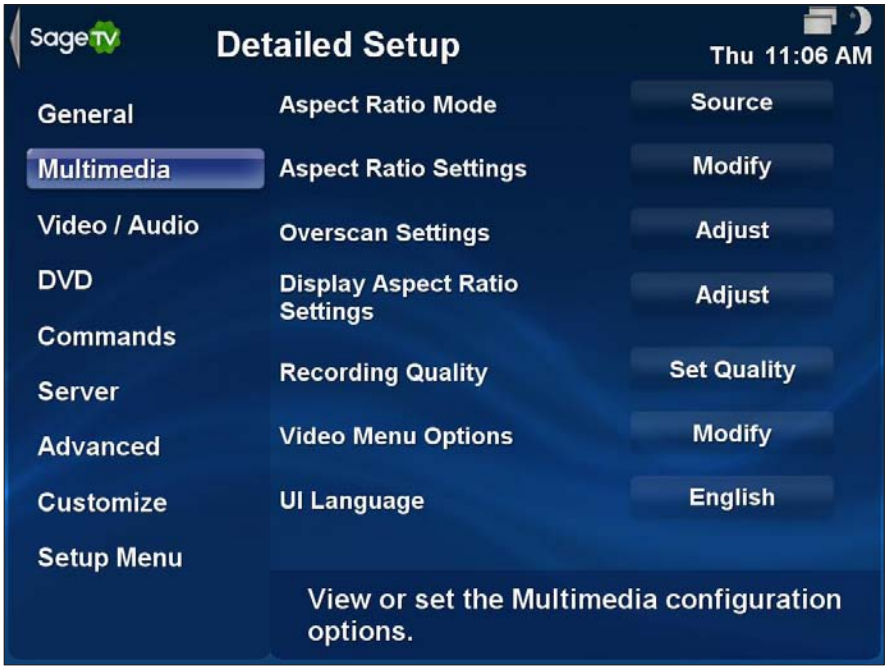


Figure 3-2: Sage TV's setup menu offers a wealth of detailed settings.

Each submenu within Sage TV breaks options down into very granular detail. You can adjust overscan settings (useful if the PC is attached directly to a TV), pick the DVD rendering method, and more (see Figure 3-3).

The real problem is trying to figure out which settings are actually important. It's best to leave things at their default settings when you first start, then adjust settings as needed. For the most part, though, you can leave the PC software at their defaults and make changes in the Sage TV HD Media Center setup screen.

Many of these settings exist because of the differences in PC hardware. The Sage TV HD Media Extender itself also has a rich set of options you can change, though it's somewhat simpler since the hardware is a known quantity. The menus themselves, however, look and operate in a similar way, but you'll use the remote control to configure settings, rather than a mouse and keyboard.

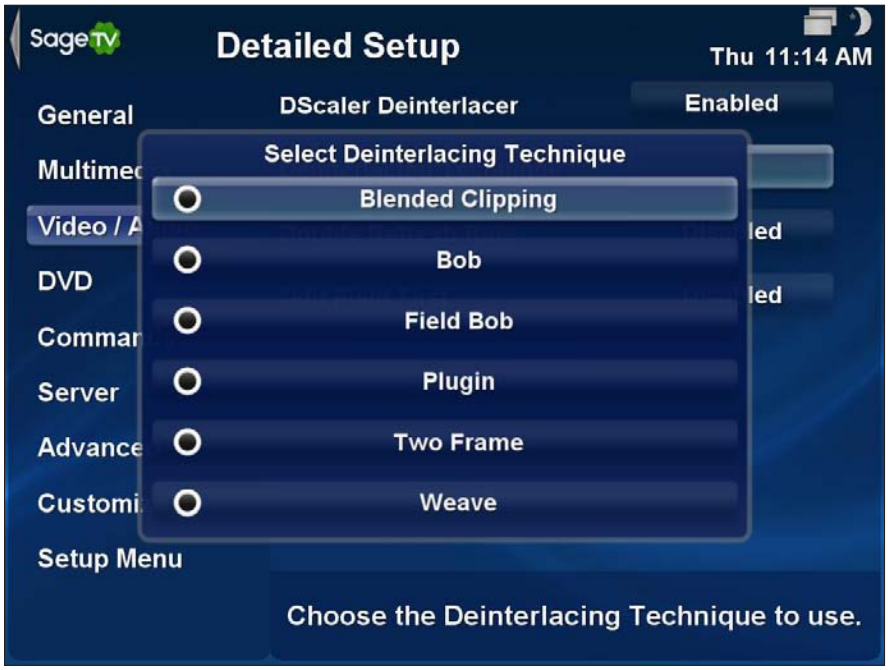


Figure 3-3: Digging deep with Sage TV — setting up deinter-lacing settings.

Installing the hardware itself is simple. You can use the included analog cables, but it's much better to attach the device to your system using an HDMI cable. An HDMI cable doesn't ship with the unit, so you'll need to obtain one separately.

Getting the unit running with the Sage TV software is an exercise in running back and forth between the computer and the location where the HD Media Center is installed. You need to enter a code in the Media Center Extender that's supplied by the Sage TV software, and that particular HD Media Center extender is locked to that specific PC.

After recording shows off the air, the Sage TV server software streams the media to the HD Media Extender. Note that the software doesn't transcode formats, so if you have a video or audio format that's not recognized by the HD Media Extender, the video won't play back.

Once the device is set up, using the extender is pretty straightforward. You use the remote to navigate the onscreen menus, playing back recorded content, as you would any digital video recorder.

D-Link Wireless N HD Media Center Extender

Most flavors of Windows Vista and Windows 7 used by consumers have built-in support for Microsoft Windows Media Center. Table 3-1 sorts out the different Windows versions.

Table 3-1: Windows Versions with Media Center

Windows XP	Windows Vista	Windows 7
Windows Media Center Edition	Home Premium	Home Premium
Windows Media Center 2005	Ultimate	Professional
		Ultimate

Windows Media Center Extenders are pretty much what they sound like — you're essentially running Windows Media Center remotely, on dedicated hardware.

The D-Link Wireless N HD Media Center, also known as the D-Link HSM-750, is one such gadget. It attaches to your HDTV or A/V receiver via either HDMI or analog video. Curiously, if you use HDMI for video, you still need to attach a digital audio cable (either optical or coax) to your TV or receiver for audio; the HSM-750 uses HDMI for video only.

When you plug in the HSM-750 to a power outlet and turn it on, a Windows Media Center–equipped PC will automatically discover the device through Windows Universal plug-and-play capability, if the device is plugged into a wired network. If you're planning on using the wireless option, you need to first configure the HSM-750 to connect to your wireless network, entering the SSID and security information (WEP or WPA key). After that's done, the Windows system can discover the Media Center extender. (See Figure 3-4.)

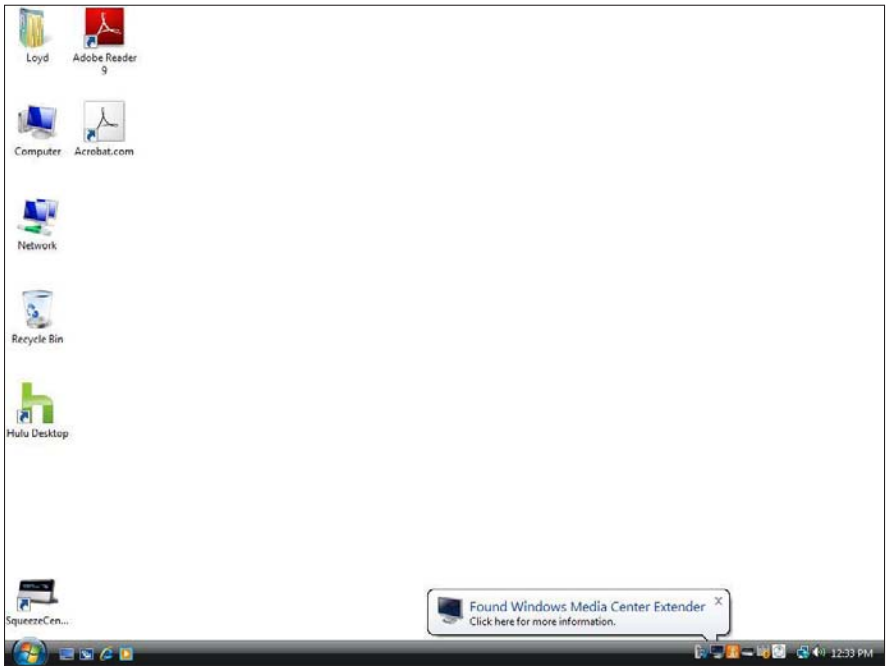


Figure 3-4: The bubble notifies you when a Windows Media Center discovery.

Follow these steps to finish the process:

1. **Click on the bubble to open a dialog box.**

   If you simply want to use the default settings, just click on the button labeled Allow, shown in Figure 3-5.

2. **The next step is to connect the Windows Center software with the Windows Media Center extender.**

   When you first start up the extender, one of the setup screens should walk you through this. If not, scroll through the user interface with the remote and select setup, then select the Windows Media Center icon and press the OK button. You are eventually presented with an eight-digit key, which you'll write down and enter on the PC. (See Figure 3-6.)

3. **After entering the eight-digit key, you can click Next several times to accept the defaults, shown in Figure 3-7.**

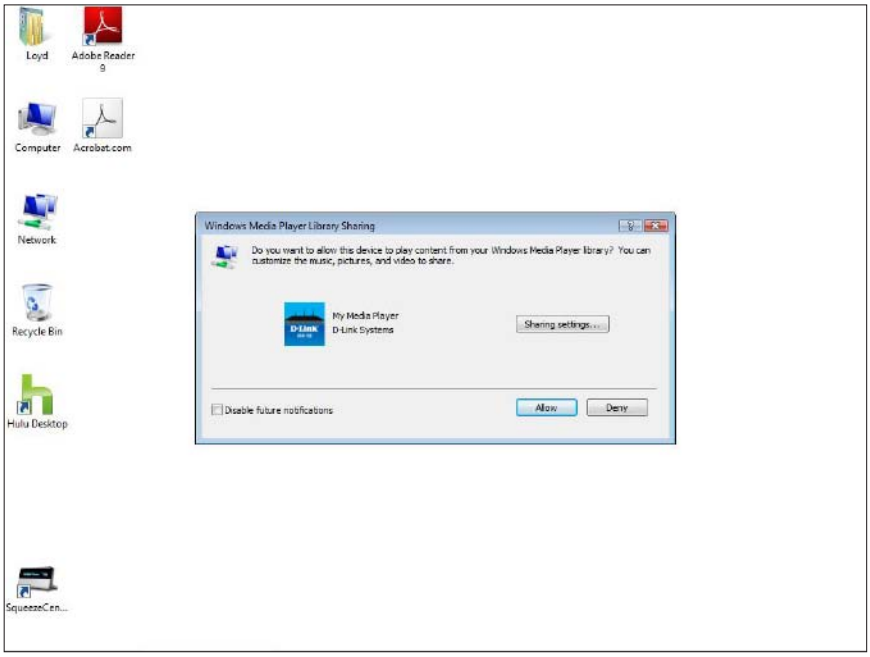


Figure 3-5: Just click on Allow.

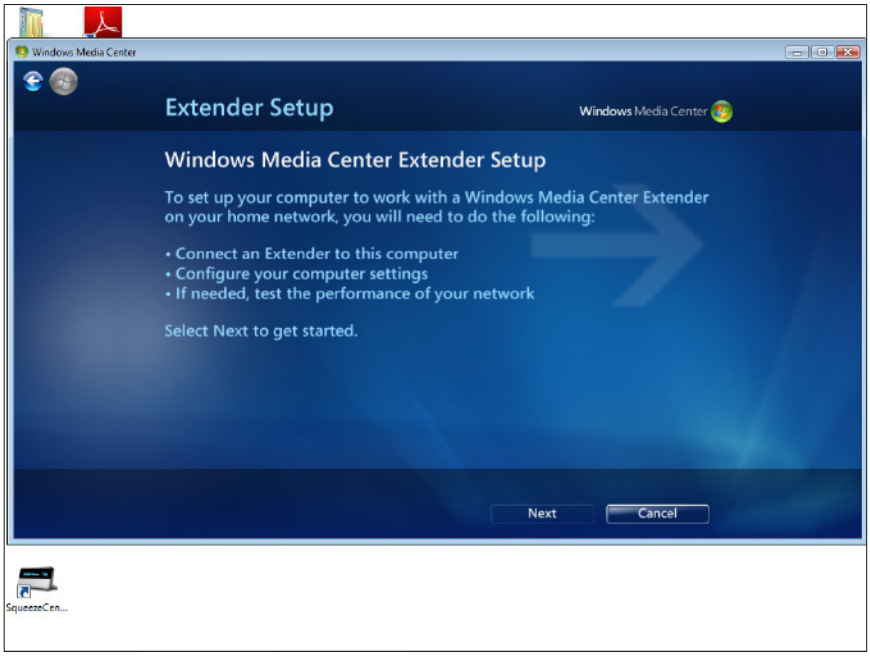


Figure 3-6: Just click next to start the process of connecting the extender to the PC.

Figure 3-7: Enter the eight-digit key supplied by the Windows Media Center extender.

4. **You also want to configure additional options on the extender, including aspect ratio (usually 16:9 for an HDTV).**

   Once connected, the HSM-750 behaves much like a Windows Media Center PC. The user interface behaves much the same. However, the HSM-750 may not support all the file and compression formats that the PC might support. For example, Microsoft's own Windows Media Lossless compression codec for audio isn't supported.

The HSM-750 can also act as a more general digital media adapter. If you're an iTunes user, you can navigate (outside of the Windows Media Center interface) to any PC running iTunes. You'll have to enable sharing in iTunes, but then you can play your ripped or non-DRM music. Network-attached storage with built-in iTunes or plug-and-play capability are also visible to the Media Center extender.

Finally, the HSM-750 connects to a number of different online streaming services, such as Youtube, so you can watch content directly streamed from the Internet, no PC needed.

Game Consoles as Digital Media Adapters

Game consoles can be used as general purpose digital media extenders. I'm not going to walk through the setup process for these consoles, but I will discuss each of the major consoles that support Media Center capabilities briefly.

Original Xbox

In its out-of-the-box form, Microsoft's first Xbox lacked any Media Center capability. However, since the system was essentially a cut-down PC, enterprising programmers developed XMBC (originally the Xbox Media Center). XBMC is an open source project that's free.

The XBMC team strongly suggests that the Xbox have a *mod chip* installed. This is an aftermarket chip that's installed in the Xbox to bypass some of the DRM and other restrictions imposed by Microsoft. Installing a mod chip voids the warranty, but since most Xboxes are out of warranty by now, that's not a big deal. You also can't call Microsoft for help.

Also, XBMC doesn't support high-definition playback unless the Xbox has been modified to upgrade the CPU.

For more on XBMC, check out http://xbmc.org.

Xbox 360

The Xbox 360 can connect as a Media Center extender in several ways. A Windows-based PC running Windows Media Connect (available with Windows Media Player 11 or later) can connect to an Xbox 360. Navigation is a little cumbersome, but it all works fairly well.

If the PC is a Windows Media Center capable PC, the Xbox 360 can also act as a Windows Media Center extender, similar to the D-Link HSM-750. Configuring the Xbox 360 Windows Media Extender is like any WMC extender hardware — generate an eight-digit code, enter it on the PC, and you're off and running.

You can extend the capabilities of Windows Media Center 11 by adding an application called TVersity (`www.tversity.com`) on your PC. TVersity will even transcode formats that the Xbox 360 doesn't natively understand into supported formats before streaming.

All in all, the Xbox 360 is a versatile media center extender, whose capabilities can be enhanced by third-party software.

Sony PlayStation 3

The PlayStation 3 is a DLNA (Digital Living Network Alliance) capable device. DLNA builds on the Universal plug-and-play standard to allow easy communication between disparate devices and PCs with media stored on them.

The PS3 is a capable media center extender, but lacks some of the tighter integration available with the Xbox 360. But if you have DLNA compliant media server software on the PC, or DLNA-enhanced network-attached storage, it's easy to navigate and playback media. As of Windows 7, Windows Media Connect is DLNA compliant, so you don't need third-party software if you're playing back supported formats.

Chapter 4: Listening to Music and Audio from the Web

In This Chapter

- **Finding good entertainment on the Web**
- **Watching on your PC**

The world of audio and video is changing. In the past 30 years, we saw the shift from broadcast TV to cable and satellite sources. Now, we're starting to see the shift to Internet-based channels for TV and music. It's even possible to forego paid services and get all your entertainment from the Web.

Alas, it's not easy. There are a huge variety of sources, from user-created content like YouTube to repackaging of commercial TV and movies on Hulu. Help is at hand, however, with software that can help you sort through the choices and stream the content you want to watch directly to your TV from the PC.

In addition, companies that make Blu-ray players and HDTVs are now building the capability into their sets to directly access some of the content streamed from the Internet.

The biggest problem is the walls that content providers put up. Want to watch NASCAR? You need to go to `www.ESPN.com`. Trying to find your favorite movies? Hulu is one place — but not all movies are on Hulu.

In this chapter, I show you how to find that content plus explore some sources for music and video. Then I take a look at the hardware you might need to get that Internet content from your PC to the TV. Finally, we'll take a look at some software packages that make life a little easier in getting your favorite audio or video to your home entertainment center.

Finding Content

The show you want to watch is almost certainly somewhere out there on the Internet. We're not talking about illegal downloads. Instead, there's a wealth of video and music legally available for your entertainment pleasure.

The problem is finding all that content. Sure, you can search on Google or Bing to find a particular show, but doing so is a tedious process.

This issue of locating your favorite shows exists because the content providers seriously guard their intellectual property. So they put up walls that make it difficult to get to what you want to watch from a single source.

Progress is slowly being made to aggregate all the balkanized world of copyrighted video, movies, and music. Some of these solutions require a particular piece of hardware, while others are software based. Finding the best solution for your viewing and listening pleasure is still something of a compromise, but instead of dozens of Web sites, all you need is a PC and the right hardware attached to your home theater system.

In the next section, I begin with solutions that exist on the PC for watching movies, TV, and listening to music available on the Web. Then I show you how you can get that from the PC to the living room.

Watching on Your PC

You've almost certainly watched hilarious or moving user-created videos on YouTube. If you want to watch commercially produced shows, however, you need to look elsewhere.

Two providers of streaming content that also rent or sell hard goods, such as DVDs, are Netflix (`www.netflix.com`) and Amazon (`www.amazon.com`). I take a closer look at the Netflix streaming service shortly.

Recently, Hulu, shown in Figure 4-1, has become increasingly popular. Hulu.com is a Web site that aggregates vast amounts of video — movies, TV shows, trailers, short subjects — into one easy-to-navigate site. Like broadcast television, Hulu pays for the shows by requiring you to watch advertisements. The good news is that Hulu ads are generally shorter and less intrusive than broadcast TV ads.

If you are a serious sports fan, or perhaps love watching NASCAR, the individual Web sites for the different leagues will often stream video. For example, if you want to subscribe to an entire season of baseball, you can head over to the Major League Baseball site, `www.MLB.com`. The sports sites, such as MLB.com, do a great job of integrating stats, video, and interactive features.

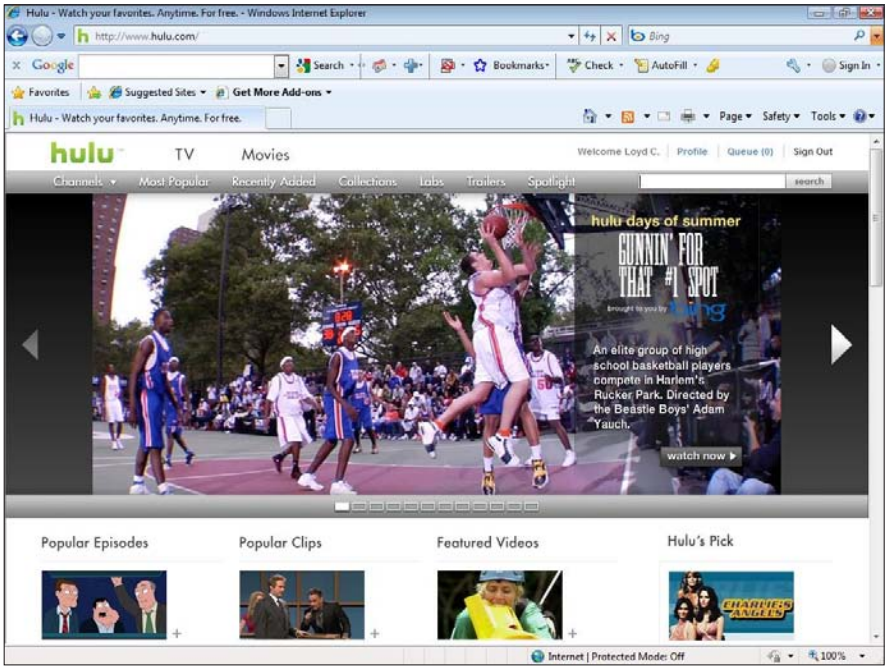


Figure 4-1: Hulu lets you watch a variety of movies and TV shows free, but with short ad breaks.

Sitting in front of your PC isn't the ultimate goal, however. You want to get that great streaming content onto your TV. There are ways of getting substantial amounts of entertainment to your living room with the right hardware — hardware that's easier to set up and use than a PC.

We're going to assume that you've got an HDTV and possibly an audio-video receiver and a surround sound speaker setup. It all looks and sounds great when watching broadcast shows or DVDs. I explain how to go further by streaming video in the next sections.

Using Xbox 360 for media

I touch on using the Xbox 360 as a Windows Media Center Extender (WMCE) in Chapter 3 of this minibook.

But the Xbox 360 offers additional streaming and downloadable video services. These include a variety of TV shows, music videos, independent videos, and movies. Some are somewhat obscure, some popular. Curiously lacking is sports content, which seems heavily weighted toward combat sports.

While some of the content is free, most of it is paid through Microsoft Points, Microsoft's attempt to manage pricing. If you can get the same content in different parts of the world, the point cost is the same — but the amount of money each point costs in real terms may differ. In the U.S. currently, 80 points is equivalent to one dollar.

Movies range in point costs from 200 points for older, obscure movies in standard definition to 480 points for newly released Hollywood movies. However, movies are rented — which means the movie is watchable for any number of viewings in the first 24 hours and expires after 14 days.

TV shows are another matter. Prices are widely divergent, ranging from free to a staggering 4400 points for the UFC Live show, one of a number of fighting shows on the 360. Unlike movies, TV shows don't expire, so you can keep them on the Xbox 360 hard drive as long as you want — as long as you have drive space available.

The issue of drive space is a crucial one. The original Xbox 360 Pro had a 20GB hard drive, barely large enough to hold a handful of high-definition TV shows. Watching a series — and keeping them on the system — was problematic. However, with TV shows, you can re-download a show to the same Xbox 360 if you've paid for it. The maximum amount of storage available is 120GB for the Xbox 360 Elite — better, but in the era of terabyte hard drives, hardly substantial.

Also available on the Xbox 360 is the Netflix Watch Instantly streaming service. You do have to have a Netflix subscription, and that subscription has to be a minimum $8.99 one, which leaves out those with a basic, two-disc per month plan.

You also need to set up the Watch Instantly queue on your PC using a Web browser. Although you can edit top lists in the Xbox 360 directly, it's a bit clumsy, so using the PC Web browser is still easier.

Standalone devices exist that can accept streaming media from the PC. These include Windows Media Center Extenders, such as D-Link's DSM-750, which supports 802.11n wireless connectivity. These devices generally layer some capability in addition to supporting WMC streaming from a PC. For example, the previously mentioned DSM-750 (Book VII Chapter 3) directly supports YouTube videos, provided your home has a broadband connection to the Internet.

Another interesting device is the SageTV HD Media Extender (www.sagetv.com). The SageTV HD Media Extender is a combination of the SageTV software running on the PC and the Media Extender hardware, which streams video captured by SageTV's software.

If all you want is Netflix Watch Instantly on your HDTV, Roku (`www.rokulabs.com`) offers a $99 box that supports Netflix Watch Instantly plus Amazon's own Amazon Video on Demand service.

DLNA hardware

DLNA is an acronym for Digital Living Network Alliance. DLNA is both an organization of technology companies and a standard developed by that organization for sharing media between the PC, HDTV, music players, cameras, and other consumer electronic devices.

Hundreds of DLNA-certified devices, including a number of network-ready HDTV units, are available. DLNA is a pretty basic standard and has suffered from implementation differences between hardware manufacturers. In addition, even though the PC was a key component of the DLNA standard, no Microsoft Media Player or (see Figure 4-2) Windows Media Center supported the standard.

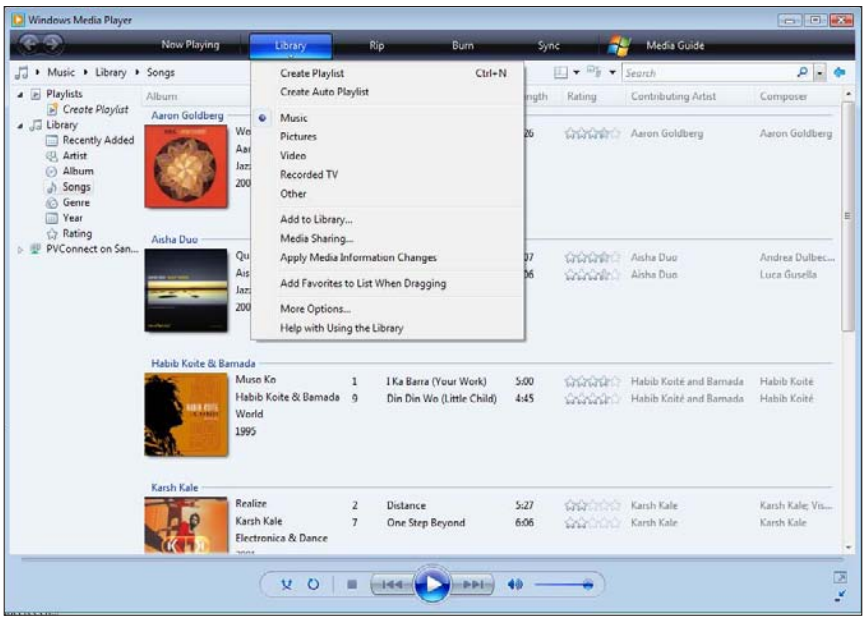


Figure 4-2: Windows Media Player 12 now supports DLNA 1.5 devices as part of its standard sharing protocol.

Having DLNA-compliant hardware means removing any intermediary devices. Although having a Windows Media Center Extender or game console has its own benefits, soon you'll be able to attach your HDTV, Blu-ray disc player, or set-top box to your network and stream content directly to your home entertainment system.

Some newer devices even have built-in services. For example, some LG HDTVs and Blu-ray players have the Netflix Watch Instantly service available on the unit.

Watching Internet TV in Your Living Room: PlayOn

Let's say you've got a Windows Media Center Extender (WMCE) or an Xbox 360 attached to your HDTV. Anything you can get on Windows Media Center on the PC is available in your console or WMCE device, right?

Not quite. As it turns out, services like Hulu and Netflix don't stream from Windows Media Center to an extender or console. However, software exists which takes those video streams, transcodes their formats into a format that your device can understand, and pipes it directly to your networked home theater.

The software is called PlayOn and is available from MediaMall Technologies (`www.themediamall.com`). PlayOn is a PnP (universal plug-and-play) media server that runs on the PC.

PlayOn supports a variety of streaming Internet services, including Hulu, YouTube, CBS, ESPN, CNN, and Netflix Watch Instantly. Setting up PlayOn is simple. You download the software from PlayOn's Web site and install it on your PC. (See Figure 4-3) Some services, such as Hulu, require login names and passwords, and you can enter these into the PlayOn configuration control panel. Others, like the CBS network, just stream directly from a virtual folder on the PC.

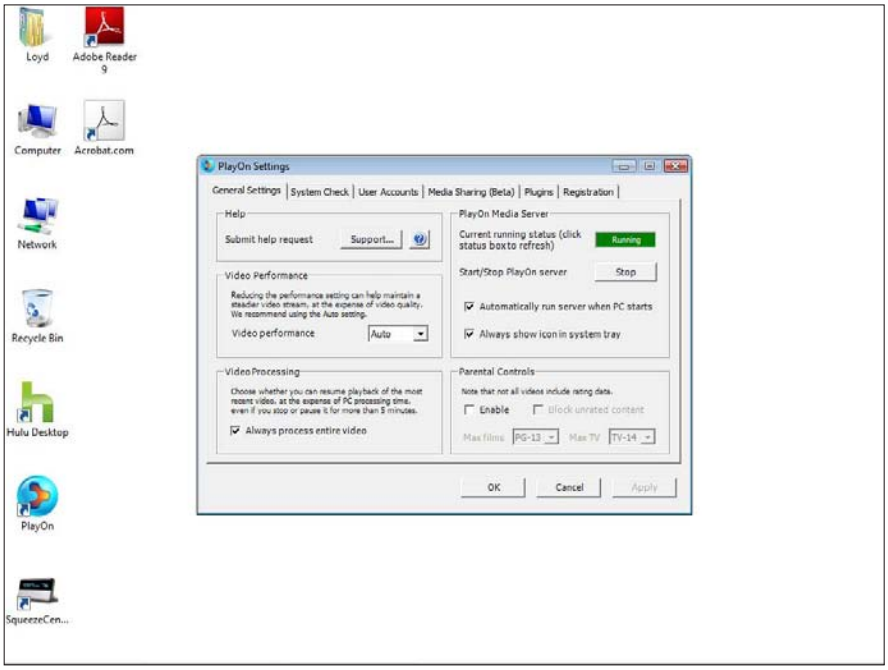


Figure 4-3: PlayOn Setup. There are relatively few settings you need to worry about; the defaults work well in almost all cases.

PlayOn has two issues that keep it from being more widely used: minimum PC requirements and limited hardware playback support.

PlayOn converts video formats on the fly as they stream from the source on the Web, to a format that the playback device can understand, a process known as *transcoding*. What this means is that you need a pretty beefy system. PlayOn recommends a dual-core CPU with 2GB of RAM at a minimum for standard definition transcoding. High-definition transcoding requires a high-performance dual-core or quad-core CPU.

PlayOn support for playback devices is limited. Currently, PlayOn officially supports the following hardware for playback:

- DirecTV HR21-100 HD DVR and HR20 receiver
- D-Link DSM-510, DSM-520, and DSM-750 media extenders
- Pioneer Elite Pro-1140 HDTV

- Popcom Hour A-100
- SageTV HD Theater
- VuNow VNHD100HD Hi-Def POD, VN100SD Std-Def POD
- XBMC (Xbox Media Center)
- Xbox 360
- PlayStation 3

Other devices are unofficially supported, and you can find discussions about additional devices in the PlayOn forums.

PlayOn costs about $40, although they occasionally offer half-price specials on the MediaMall Web site. It's really an elegant solution, slowly garnering wider support on a variety of networked playback devices due to its PnP and DLNA support.

Radio Internet: Web Radio in the Living Room

A wealth of radio-style programming exists on the Internet. These range from traditional radio stations simulcasting over the Web, to podcasts, to a range of other audio services, like the music recommendation service Last.fm.

In Chapter 2, we talked about devices like the Logitech Squeezebox and the Sonos Music Player. If you have one of these products, or something similar, you should be comfortable streaming music from your PC. What about all that Internet radio?

Now, take a look at the Squeezebox Duet as an example of something that can also act as an Internet radio player. First, you need to create an account on Logitech's SqueezeNetwork (`www.squeezenetwork.com`).

After your account is created, you set it up in SqueezeCenter on your PC. Follow these steps:

1. **Click on the Settings button on the lower right of the SqueezeCenter main window, shown in Figure 4-4; then click the SqueezeCenter tab.**
2. **Enter your SqueezeNetwork login information and click Apply and then Close. (See Figure 4-5.)**

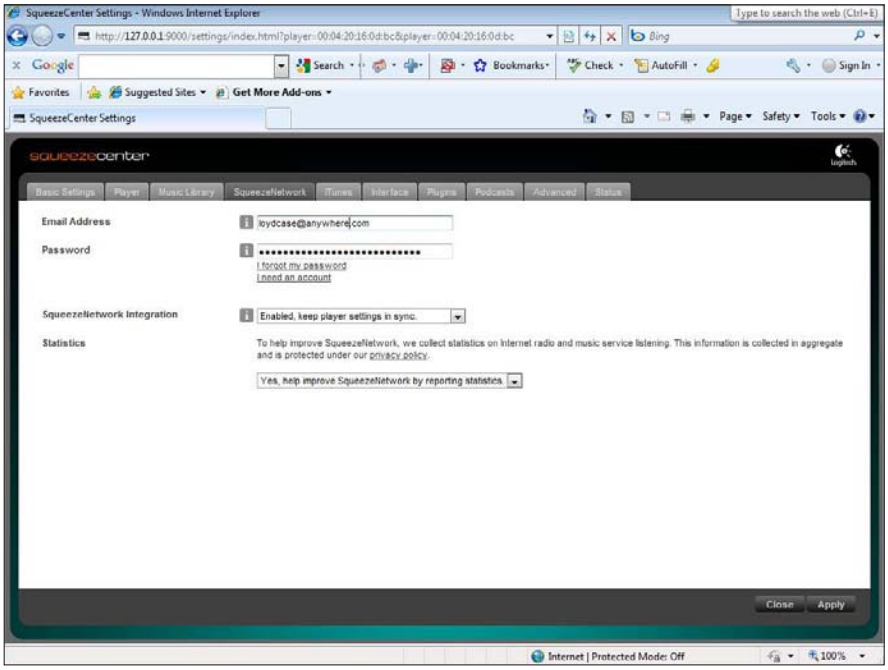


Figure 4-4: The Squeeze-Network login screen

3. **Now that your account information is entered, you can select SqueezeNetwork as one of the music sources.**

   You can do this in the SqueezeCenter browser or directly in the Squeezebox Duet.

Other devices, such as those from Sonos or Roku, also allow access to Internet radio in your living room or family room.

Internet radio and video have come a long way since the days of choppy, highly compressed content. Now you have access to a vast array of content, from traditional media sources to edgy, new media producers working out of their homes and garages. Grab that remote, plop yourself down, and take it all in.

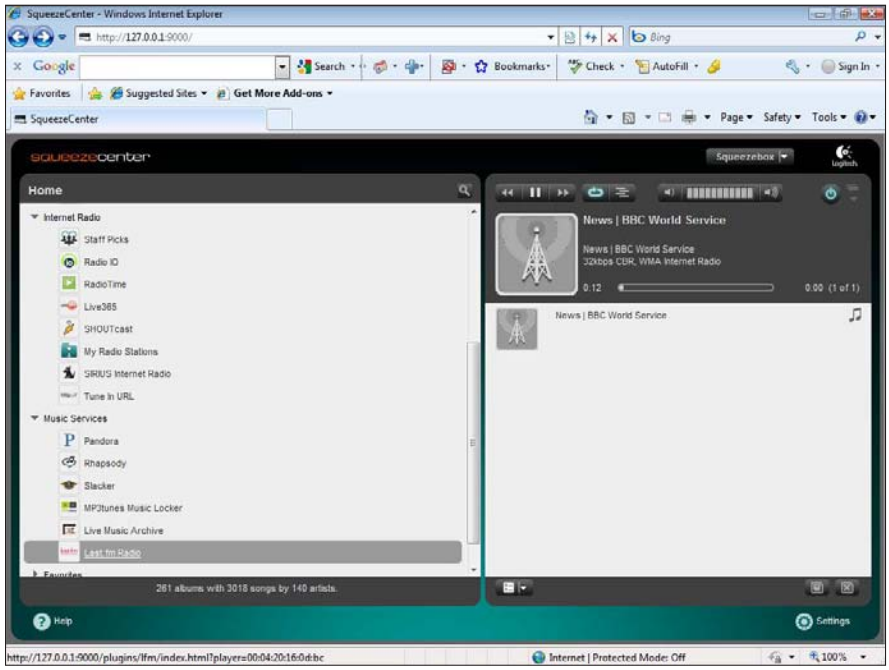


Figure 4-5: Internet Radio playback from Squeeze-Network.

Chapter 5: Exploring Digital TV and Satellite Radio

In This Chapter

- **Understanding digital TV**
- **Deciphering HDTV terms and jargon**
- **Listening to satellite radio**

On June 12, 2009, a remarkable thing happened in the United States: All analog television signals vanished. The digital television revolution, which began years before, has reached its climax. The federally mandated switch to digital television ended the more than half-century reign of analog TV. Not only were the old, bulky CRT TVs a thing of the past, but the very way TV signals were transmitted and processed inside the TV had changed.

A similar revolution was also occurring in radio. Over-the-air digital radio lagged behind satellite radio services such as Sirius XM, but both satellite radio and the emerging over-the-air HD radio bring radio firmly into the 21st century. I'll look at the various options for digital television and radio, so you can understand the choices and better enjoy the wealth of digital content available from a wide variety of providers.

Making HDTV Choices

Purchasing a television used to be so simple. All you needed to know was what size you wanted. All analog TVs were built pretty much the same.

Then home theater became popular, and TVs became more complicated — but only a little. The TVs were still pretty much the same, although some big screen TVs used three small CRTs (cathode ray tubes) to project the image onto a screen, rather than one large CRT as the main screen. More choices of connections also became available. In addition to the little, yellow plug — composite video — you also had S-Video and component video. Many users simply connected their antenna or cable box directly to the antenna input on the TV.

Then HDTV arrived, and the complexity of choices exploded by an order of magnitude. Several different display technologies arrived on the scene, the number of ways to connect to those displays exploded, and confusion reigned. On top of that, different methods of delivery have competed for viewers' attention, including cable, over-the-air, and satellite television.

The latest wrinkles include direct streaming of video over the Internet, and Blu-ray, the replacement for the highly popular DVD disc format.

Part of the mix also includes multichannel audio — 5.1 or 7.1 surround sound — once the purview of movie theaters. Now that you can buy TVs as big as 65 or more inches (diagonally measured), adding surround sound brings the theater into your family room.

The key thing to remember is that if you don't have a TV with an over-the-air tuner, whether it's built into the TV itself, an external DTV converter box, or part of a cable or satellite digital tuner, then you cannot receive over-the-air (OTA) DTV and high-definition broadcasts. Whatever else you buy, don't forget this simple rule.

Understanding All Those Terms

The list of features that are printed on the side of an HDTV box seems to consist of a mind-numbing array of acronyms, numbers, and indecipherable terms. Surprisingly, you can ignore a lot of those features if all you want is a straightforward high-definition television. Many of the terms you see have more to do with issues like image quality or overall visual fidelity, rather than the basic stuff you need. In the following sections, I cover the basic terminology.

Display technology

When HDTV first became popular, flat panel TVs — plasma and LCD TVs — were very expensive. So rear projection was popular for a time. A rear projection system consists of a big screen inside a large box that's mostly air. Inside the box is a small projector that projects the image through a series of lenses and prisms onto the large screen.

Rear projection HDTV

Because you need all that volume, rear projection TVs are bulky, even though the technology used in the projectors is small. There were two main types of rear projection TVs that were popular: DLP (Digital Light Processing), a technology developed by Texas Instruments, and LCoS (liquid

crystal on silicon). In actual practice the differences are minor, but LCoS TVs are pretty much extinct. DLP still exists, but mostly in very large screen HDTVs.

Rear projection TV is still a great bargain if you want a really big screen. You can typically buy a 65-inch or larger DLP RPTV for less than $2,000. Some other features, such as 3D movies (those movies that require you to use the special glasses) may serve to keep DLP alive for a time.

But the real action these days are flat panel TVs. Two different types of flat panel technologies coexist today: LCD and plasma. Plasma HDTVs have tiny cells, each of which behaves almost like a tiny CRT. LCD TVs are much like the flat panel screens used on personal computers, but much larger.

Flat panel TVs: Plasma versus LCD

Until recently, the differences in image quality between plasma and LCDs were substantial. LCD TVs were great in bright rooms but not so good for light-controlled environments — particularly a darkened room where you might be watching a high-definition movie with lots of low-light content. Plasmas were also much better for high-motion content, like sports.

Advances in LCD technologies have narrowed the gap considerably, though some differences still exist. Higher refresh rate — the speed at which frames are displayed on the screen — and new backlighting technologies, like LED backlighting, have made LCD TVs much more attractive. Today, the real difference is size: If you want something 50 inches and larger, plasmas are a better buy. On the other hand, 55-inch and smaller LCDs can be found at reasonable prices.

At that crossover size — 50 to 55 inches — the choice becomes a matter of taste. Better quality LCD TVs cost nearly as much as (sometimes more than) a good plasma.

One issue that dogged plasma TVs for years was the problem of *burn in*. If you left the TV on for a long time — say, on ESPN — that little ESPN "bug" at the lower right of the screen would eventually become a permanent ghost image that overlaid everything else. That problem no longer exists. Similarly, plasma TVs had a reputation of consuming more energy than LCD TVs, something that's a concern with green-aware consumers. But big LCD TVs use nearly as much juice as newer plasmas.

Both LCD TVs and plasma panels had issues with the overall life span, but today's models typically have life spans in excess of 50,000 hours to half-bright. That means a good eight years or more. The technology is evolving so rapidly, that you'll likely get a new TV before you notice any issues with fading images on plasma TVs.

Ultimately, which technology you want is really a matter of preference and budget. The best advice is to take the time to view lots of content on the TVs you're considering before buying.

Resolution

Display resolution as it applies to HDTV is simply a measure of the number of pixels on the screen and is typically shown as (number of horizontal pixels) x (number of vertical pixels). For example, many large-screen LCDs are 1920 x 1080.

Early HDTVs shipped in a variety of resolutions, including oddball pixel formats such as 1366 x 768, 1440 x 900, and even 1024 x 1024 (using nonsquare pixels.) A number of digital TVs also supported something called EDTV (extended-definition TV), which was 720 x 480 pixels, but progressively scanned (see below). Thankfully, this silly bit of confusion has all but disappeared.

Today, it's much simpler: You typically have 1920 x 1080 and 1280 x 720. These are often shortened to 1080p and 720p.

That *p* stands for *progressive,* as in progressive scanning. Progressive scanning simply means that the display is generated by displaying the entire image at once. This differs from interlaced scanning, which displays alternate images that are actually one-half the frame height. You'll see references to 1080i, in which two images of 1920 x 540 are rapidly displayed in succession; each interlaced frame actually comprises one complete image frame.

This idea of interlaced versus progressive scanning is actually a holdover from the old days of CRT displays, when an electron beam painted the image on the screen by rapidly scanning the beam over the inside of the screen. Modern digital TVs can now just display the entire image at once.

Interlacing works because the two half-frames are thrown up on the screen so fast, your eye is fooled into seeing it as a single frame. This idea of progressive versus interlaced is important because broadcasters transmit HDTV images in either 720p or 1080i; there are no HDTV broadcasts in the U.S. that are 1080p.

Why, then, do you see so many larger displays that describe themselves as 1080p? That's because circuitry built into the TV itself combines the two interlaced half-frames into a single image *before* they're displayed; this is known as *deinterlacing.* While home theater enthusiasts often argue about how well different HDTVs deinterlace signals, most current generation TVs do it well enough that the majority of viewers don't notice problems.

The new Blu-ray high-definition disc standard, on the other hand, does support 1080p, so Blu-ray content can take advantage of the full resolution of a 1080p display.

The bottom line: if you're getting a larger HDTV — above 32 inches — it's a good idea to opt for 1080p display.

Understanding standard definition

Standard definition TV is simply TV as it was shot and produced before the HDTV era. All your old favorites were shot in standard definition. SDTV, as it's sometimes called, had very low resolution — 480i — and was designed to be displayed on old CRT televisions with electron beams that scanned across the interior of the tube.

This very low resolution relative to true HDTV is challenging for HDTVs to display well, but a good quality HDTV can at least show a presentable SDTV signal. Similarly, DVDs were also 480i, but the production quality of DVDs is typically much higher, so the problems aren't as glaring when watching DVD movies.

Understanding aspect ratio

While the issue of available resolution of HDTVs has simplified a bit, understanding aspect ratios is still a confusing topic. Aspect ratio is simply the horizontal resolution divided by the vertical resolution, and is typically displayed as (some number):(some number).

For example, 1920 x 1080, which is the maximum HDTV resolution, is 1.78:1 (sometimes also referred to as 16:9); 1280 x 720 is also 1.78:1. This ratio of 1.78:1 is actually built into the industry standard for HDTV.

So if all available HDTVs are 1.78:1, what's the big deal?

There are two sources of confusion: movies and standard definition TV.

Movies are shot in a variety of aspect ratios. In fact, there are too many to really discuss here; if you're interested in the topic of movie aspect ratios, a good source is the Widescreen.org aspect ratio page: www.widescreen.org/aspect_ratios.shtml.

Standard definition TV was modeled on the original Academy movie aspect ratio, or 4:3. You'll also see 4:3 reduced to 1.33:1 — either format is correct and means the same thing. Worse, standard definition TV is effectively 480i, or 640 x 480 interlaced. So not only is the aspect ratio different, the effective resolution is much less. As Figure 5-1 shows, if the SDTV image is displayed on an 1920 x 1080 display, this is what you see.

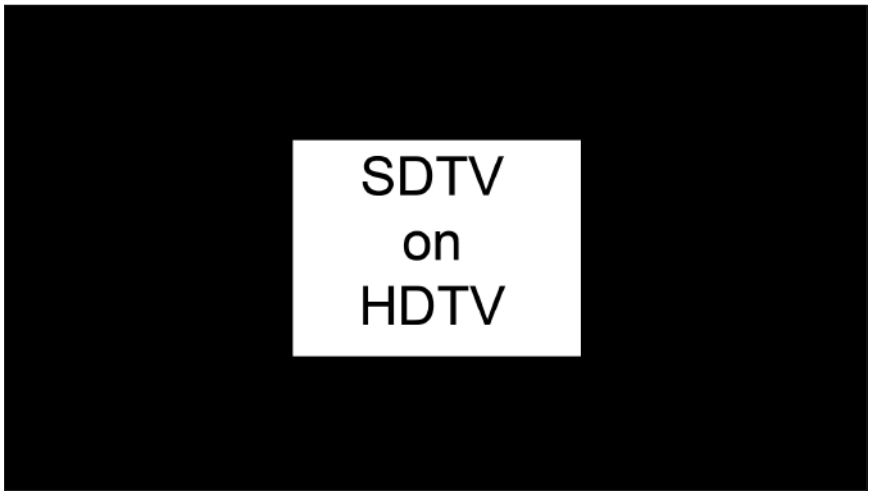


Figure 5-1: An SDTV image displayed on an HDTV would look very small.

You really want to avoid this, and most HDTVs will allow you to stretch the image but maintain the correct aspect ratio, as in Figure 5-2.

You'll still see black or gray bars on either side.

Many HDTVs try to intelligently scale the 4:3 image to fit the *entire* screen, but this can result in a distorted image. Many viewers don't seem to actually care, preferring not to fiddle with the HDTV settings. It's entirely personal preference, though image quality purists may cringe at this.

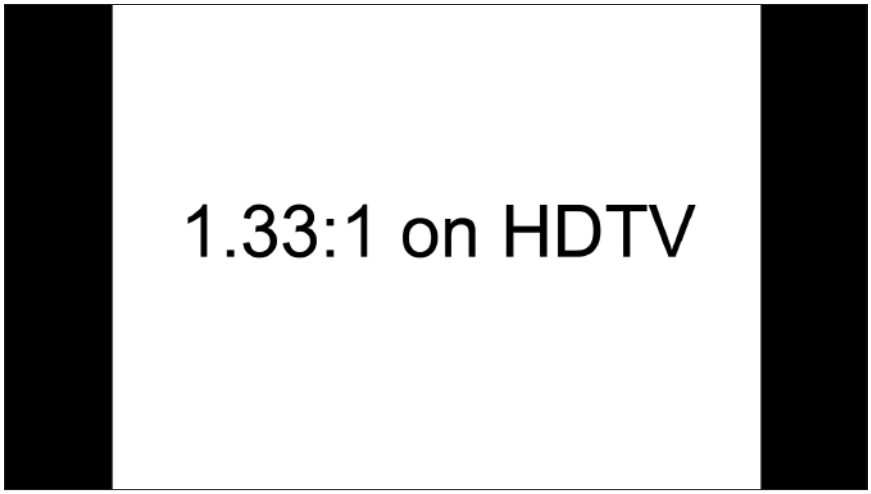


Figure 5-2: SDTV image scaled up to a larger image.

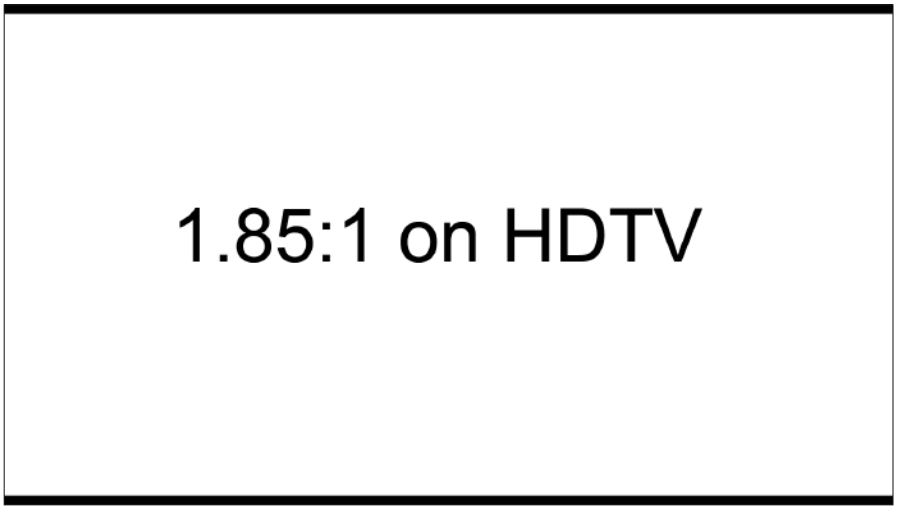


Figure 5-3: A 1.85:1 movie will show small black or gray bars at the top and bottom.

Wide-screen movies will show letterboxing at the top and bottom, rather than the left and right sides. Just briefly, this is what you'd see with the two most common wide-screen movie aspect ratios, 1.85: 1 and 2.35:1, shown in Figures 5-3 and 5-4.

Again, most current HDTVs try to scale the image to use the entire screen, with some distortion. Again, whether you do that or not entirely depends on how you value image quality.

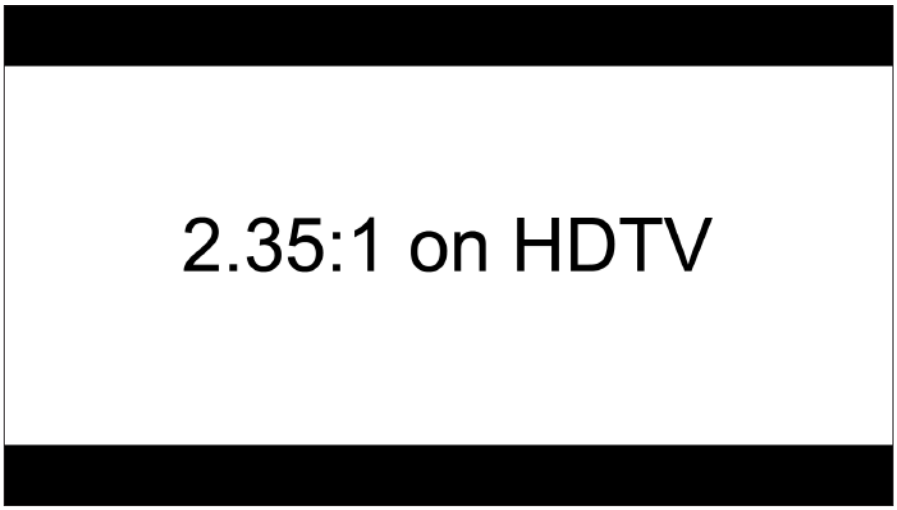


Figure 5-4: A 2.35:1 movie will show larger black or gray bars at the top and bottom.

That's resolution, interlacing, and aspect ratios in a nutshell. There are many more considerations when buying an HDTV. Mostly, though, take along some content (DVDs or Blu-ray movies) with you when buying an HDTV or at least insist on watching some content that you tend to view often. Then choose the TV based on what *you* see on the screen.

Shopping for an HDTV

Now that you have an understanding of several key technical terms, let's go shopping!

Consider the following items when shopping for an HDTV:

- **Budget:** How much money are you willing to spend? Your budget determines what feature set you can afford and also affects the ultimate screen size of the HDTV you purchase.
- **Physical size:** Have a huge living room and a small budget? Maybe a large format, DLP rear projection TV would work. On the other hand, if you have tight space constraints, perhaps because you have a particular piece of furniture that will house the HDTV, then that will dictate the maximum size of the unit.
- **Content Source:** What's the source of the HD content? If you want to use an over-the-air antenna exclusively, you'll need an HDTV with a built-in tuner or you'll have to make sure that an external tuner is part of the package. If you plan on watching exclusively through cable, then you may not need a built-in tuner.
- **Connections:** Finally, if all you want to connect is a cable or satellite box, you may not need many inputs. Similarly, if you're connecting multiple devices through an A/V receiver, one input on the HDTV will suffice. But if you want to have many devices connected directly to the HDTV, then you want to have multiple inputs — as many as you have devices to connect.

Prices of HDTVs have dropped considerably in the past several years, and it's not uncommon to find a 50-inch LCD for around $1,000 and a 50-inch plasma at nearly the same price — and those are the prices for 1080p. Above about 55 inches, prices increase much more rapidly, due to manufacturing constraints. Again, determine your budget and space constraints before going shopping.

A word about HDMI

I'm assuming your entire setup is fairly current. Whether your cable company is supplying you with a cable box or you're using a home theater A/V receiver, the best way to connect your HDTV today is HDMI (high-definition multimedia interface). HDMI carries both audio and video signals, so you only need one cable connecting a single source to the HDTV. It's far more convenient than component video cables with separate digital audio cables, for example. Plus, HDMI can carry all the newer high-definition audio standards, such as Dolby TrueHD and DTS-HD Master Audio.

As I noted earlier, make sure to watch some content on the HDTVs you're seriously considering buying. Even good quality HDTVs may handle color, brightness, and contrast a little differently, so personal preference often has a strong impact on what you buy. Note also that most HDTVs in showrooms typically have their controls set to be very bright, with very saturated colors, so that the images "pop" on the showroom floor.

One final word about buying: you should also make sure to buy your HDTV from a store with a solid return and exchange policy, in case the unit you buy simply won't work in your viewing environment.

Understanding Content Sources

Assuming you actually want to use your HDTV to view shows, you need a content source. The three primary sources of HDTV programming are over-the-air (OTA), cable TV, and satellite TV. A fourth source, streaming video from the Internet, is in its infancy but is rapidly becoming a popular alternative. Take a look at the options in the following sections.

Receiving TV over the air

Getting your programming over the air, using an antenna, has one key benefit: it's free. Depending on your location, you may have access to few or many channels of digital programming. Large urban areas can have access to 30 or more digital TV channels.

HDTV versus HDTV ready

Until recently, you could buy an HDTV without a built-in, over-the-air tuner. These were really just large monitors, not true TVs, and were often labeled "HDTV ready." You had to add your own content source. Most HDTVs today ship with an included OTA tuner, but you may still stumble across the occasional model that lacks a tuner. Be aware of what you're buying, since you need some source of HDTV content if you want to actually watch anything on your shiny new display.

All you need for OTA reception is a tuner and an antenna. Typically, you can buy a good antenna from the same source where you bought your HDTV. Note that some antennas are directional, while others can gather signals in all directions (omnidirectional.) Make sure to consult your dealer for the type of antenna best for your local area.

A good source of information on antennas and ways to help maximize your HDTV over the air reception is antennaweb.org, a Web site cosponsored by the Consumer Electronics Association (CEA) and the National Association of Broadcasters (NAB).

If you're lucky, you may only need an indoor antenna. Could the days of the rabbit ears be returning?

Even if you have cable or satellite TV, you may still want to have OTA reception. The reason is that over-the-air broadcasts actually offer better image quality, since satellite and cable providers often use heavy compression on their HD signals, reducing image quality. So if you have a choice of receiving a particular show through an OTA source, for from cable/satellite, get it from the local broadcast.

You also need an over-the-air tuner. OTA tuners are built into most modern HDTVs, but they're also often included in satellite or cable TV set-top boxes.

There is one difference between getting digital TV over the air and the old analog broadcasts. With DTV, you either get a picture or you don't. There's no fuzzy image because of poor reception. Poor reception means no picture at all, with DTV.

Premium services: Satellite and cable

Satellite and cable TV providers are pay services, usually requiring a monthly subscription fee. If you want to add HDTV and premium channels (such as HBO or Showtime), you may need to pay additional monthly fees. The advantage of premium services is the lack of commercial interruption.

Note that cable and satellite often offer similar mixes of HDTV programming, though there is some exclusive content on the different providers.

Receiving HDTV via satellite TV

Both local and cable channels broadcasting in HDTV are available from two satellite TV service providers, DirectTV and Dish Network. For an additional fee, you subscribe to local stations, receiving them via your satellite provider rather than over the air. However, the satellite set-top boxes also include OTA tuners, so you can hook up an antenna to them to get OTA HDTV from a single source.

Along with cable TV providers, satellite TV services are offering a package of HDTV content that goes beyond these local stations. They include new channels, such as ESPN HD, Discovery HD, HDnet (movies), HBO HD, and Showtime HD.

You usually need to purchase or rent a new set-top box that receives HDTV content. This investment is on top of the one you make for the high-definition TV. One popular option is the DVR (digital video recorder), which enables you to time-shift your viewing. A DVR contains a large capacity hard drive that stores shows for later viewing, much like people did in the analog era with VCRs.

Receiving HDTV over cable TV

Receiving HDTV programming over cable TV is similar to getting it from a satellite TV provider. In some cases, you could have trouble receiving all of the local HDTV channels directly on cable, if the local cable provider hasn't signed contracts with local TV stations to offer local content. However, you can still get those local channels through an OTA tuner.

As with satellite TV, local cable providers often offer DVR capability if you want to record shows for later viewing. A few cable companies are experimenting with virtual DVRs. A virtual DVR doesn't actually store the show in a local set-to box, but flags it back at the cable provider's server farm for later viewing.

To CableCard or not?

A new standard for connecting HDTVs to cable TV, known as CableCard, emerged several years back, but it wasn't widely adopted. CableCard theoretically allowed TV producers to embed a digital cable tuner in the HDTV itself that was independent of the cable provider. Once the TV was installed, you would call your local cable provider who would supply you with the proper CableCard for your area. The problem was that the first CableCard standard was one way, which meant that interactive services like video on demand still required a telephone connection. CableCard 2.0 attempts to address this key issue, but future adoption remains in doubt. For the moment, the better option is to buy an HDTV without a built-in digital cable tuner and go with the set-top box supplied by the local cable provider. If you want to use TiVO HD, though, you'll need to get two CableCards from your local provider, one for each of the cable tuners built into a TiVO high-definition DVR.

Some HDTV TV sets offer CableCard slots. With one of these cards, you can bypass the set-top box and plug the coaxial cable into your TV. You insert a card into a CableCard slot, which carries information about the services you are allowed to view, as well as any limitations on the programming you can record.

TV over the Internet

A generation of new streaming video services, some free, some fee based, is emerging. Free services like Hulu (`www.hulu.com`) are gaining in popularity. Like broadcast television, the Hulu service uses commercials to pay for the programming, though the commercial interruptions are typically briefer than broadcast television.

Companies such as Amazon and Netflix also offer streaming services. Amazon's streaming service is pay-per-view. Netflix, on the other hand, offers their Netflix Watch Instantly service free to any current Netflix subscriber who has more than the most basic subscription.

Image quality ranges from poor, if you have a slow, unreliable Internet connection, to high definition, if you have a high-speed broadband connection. However, not all shows or movies are available from any single service.

Getting streaming Internet services to your TV is something of a challenge. You can use your Wi-Fi network to deliver content streamed to your PC to the TV. Some services, like Netflix's Watch Instantly service, are available in a standalone set-top box which connects directly to your TV, or on the Xbox 360 game console.

The Xbox 360 itself offers downloadable TV shows and movies for a fee. Similarly, Apple TV uses Apple's own iTunes service to deliver video and music to your HDTV from the Apple TV box itself.

Emerging classes of HDTV and accessory products now have some of these services built into the unit itself. For example, some HDTV and Blu-ray players have Ethernet connections and can connect directly to the Internet, offering services like Watch Instantly directly on your TV — no PC needed.

Heavenly Radio

The era of driving in your car and listening to crackling and hissing radio stations interfering with each other is almost gone. The new era of digital radio, whether from satellite services like Sirius XM or the emerging generation of HD radio stations, will forever change the way we listen to radio.

Satellite radio

If you're looking for all the possible radio programming you could ever want, you need look no farther than Sirius XM, which provides satellite radio service nationwide. Most newer cars and many aftermarket automobile radio receivers offer Sirius XM. Of course, you do have to pay a monthly subscription fee of $12.95 per month. The service does offer a lifetime membership for around $500, but you can only switch receivers three times during that "lifetime."

HD radio

Digital radio is quietly, but rapidly, supplanting traditional AM/FM radio. It's quiet, because digital radio coexists alongside AM/FM, but you do need new hardware to receive the HD radio signals. Many newer cars and home audio receivers now have HD radio tuners built in. The audio quality of HD radio is substantially better than typical AM/FM radio and nearly as good as satellite radio.

Chapter 6: Exploring the Kindle

In This Chapter

- **Understanding eBooks**
- **Reading on the Kindle 2**
- **Reading blogs, newspapers, and more**
- **Reading eBooks for free**

Imagine being able to carry dozens of books around with you, without the weight and bulk of actual books. Now imagine you can buy those books anywhere, anytime, and have them delivered nearly instantaneously, whatever your location.

That's the promise of Amazon's Kindle. I get into more detail about what an eBook is, but for the moment, think of it as a thin, portable device for storing and reading anything that can be converted into electronic text. The Kindle revolutionized eBooks by adding the capability to buy books and have them automatically transferred wirelessly to the Kindle.

I explain how eBooks work in this chapter.

Understanding eBooks

When people first look at eBook readers and compare their prices to other devices, like Netbooks (small, Internet-connected laptops), the initial reaction is negative. After all, the second-generation Kindle 2 costs $299, the same price as many Netbooks. If you want the larger-screen Kindle DX, that costs a hefty $489.

Electronic book readers are built around a technology known as e-paper, or electronic ink. These are unlike the LCD displays in laptops in several ways:

- The image requires no refresh, which means the text or image is constant (no flickering). That makes it easier on the eyes and uses much less power than LCD displays.
- The surface of e-paper is reflective, rather than requiring a backlight (as a standard LCD) or emitting its own light (as with OLEDs).
- Current e-paper implementations are monochrome or shades of gray only, though color versions are working in research laboratories.

The extraordinarily low power draw, coupled with the reduced eyestrain relative to LCD displays, makes eBook readers compelling for actually reading. I've read very long books on the Kindle for hours at a time, with almost none of the eye fatigue associated with extended computer use.

A variety of eBook readers exist, from companies like Sony, iRex, Samsung, and others. Amazon launched the original Kindle in 2007. The Kindle offered a 6-inch screen and four shades of gray. The Kindle's key innovation was its built-in Whispernet capability, which uses Verizon's CDMA cell network to wirelessly transmit books bought on the Amazon.com store to the Kindle.

The Kindle was followed up with the notably thinner and slightly lighter Kindle 2. The Kindle 2 offers longer battery life, 16 shades of gray, and faster page turning. Like the original Kindle, it has a small keyboard and a 6-inch screen. The Kindle 2 also has built-in text-to-speech capability and an audio output jack, which can be used for headphones or speakers. So you can enjoy having books read to you, even if you're in the dark, or want to listen while driving.

Amazon also offers the Kindle DX, a larger, heavier version with a 9.4-inch display. Almost twice as heavy, at 18.9 ounces, and more expensive than the Kindle 2, the DX is targeted at students and others requiring more robust graphics support and native support for PDF files (the Kindle and Kindle 2 do not natively support PDF).

The Kindles uses a proprietary file format which includes DRM (digital rights management) capability to protect authors from having their works illegally distributed. The format is actually based on the open Mobipocket standard. The Kindle readers can also natively read Mobipocket formatted files. Many free eBooks are available as Mobipocket files.

Now that we understand a bit more about the various Kindles, keep reading to find out how to use them.

Reading on the Kindle 2

The Kindle 2 (Figure 6-1) is a compact device weighing just a shade over 10 ounces. The 6-inch screen seems small at first, but it's easy to read, and page turning is fairly quick.

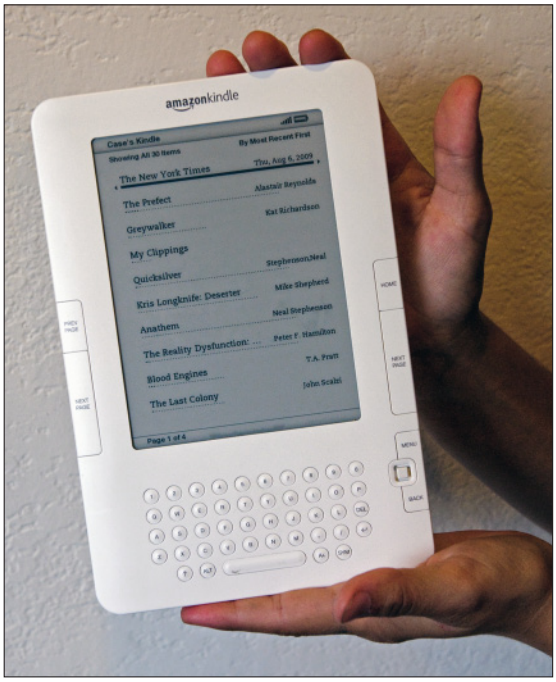


Figure 6-1: The Amazon Kindle 2 delivers books bought from the Amazon.com site wirelessly.

The power switch on the Kindle 2 has two purposes. If you quickly flick it, the Kindle 2 is put into a very low power sleep mode. The sleep mode still uses a little power, but the Kindle 2 can still remain in suspended animation for weeks without a recharge — provided you've also disabled Whispernet.

If you leave Whispernet on while the Kindle 2 is in sleep mode, Kindle books you buy from `www.Amazon.com` will still download automatically, but battery life will be reduced.

If you move the power switch, but hold it for several seconds, the device completely powers down. If you do this while the system is powered off, it powers up.

You buy Kindle books from Amazon's Web site. That's the only place to buy currently published work in Kindle format. However, other sources of free — as in zero cost — books are available in Kindle or other recognized formats. See "Reading free eBooks" later in the chapter.

The Kindle home page simply consists of a list of books, with the most recently read books at the top, as in Figure 6-2. One of the best features of a Kindle book is the automatic bookmarking. Whenever you exit a book, the reader will remember the last page read. When you return to that book, you can take up reading where you left off.

Navigating the book list is simple. A little nub in the lower right, between the MENU and BACK buttons, behaves like a tiny four-way joystick. You can navigate down the book list by moving the nub toward the bottom of the Kindle. Moving it right opens a book; moving it left asks you if you want to delete a book. You can also open the book by pressing the nub into the Kindle, like you would a mouse button. If you do delete a book, you can always re-download eBooks you own from Amazon at no charge.

If you have multiple pages of listings — something that's easy to do if you buy more than a few books — the Next Page button will take you to the next part of the book list. The Prev Page button takes you back.

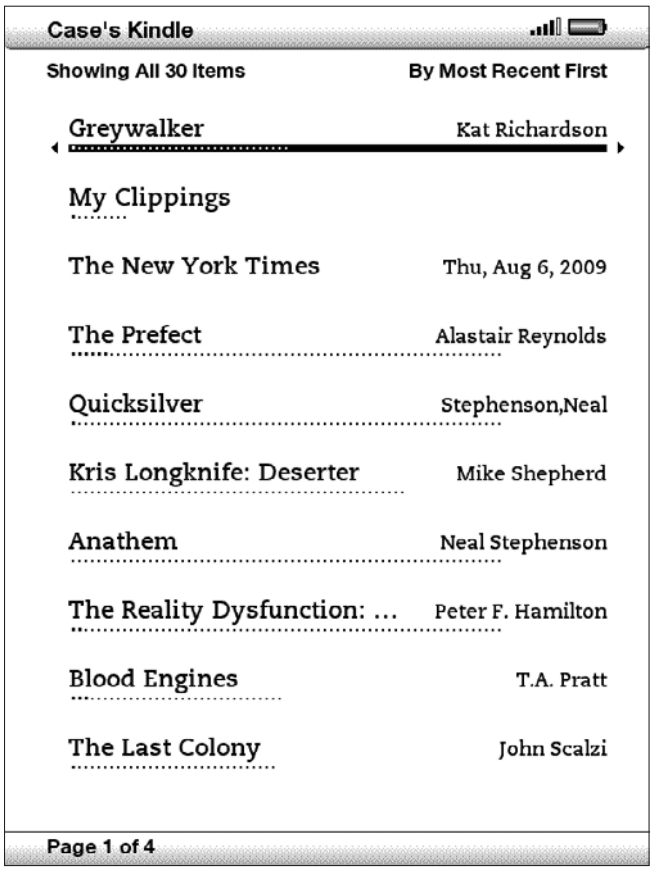


Figure 6-2: The Kindle book list.

The Menu button has two functions. When you're in the book list, you can search the Kindle, shop for books (shown in Figure 6-3), change settings, and peruse the Experimental section, which includes a crude Web browser, an MP3 player, and the text-to-speech function.

When you're reading a book, the menu shows alternative navigation possibilities, including creating custom bookmarks, looking at the table of contents, or even adding annotations to what you're reading. Each note is marked in the book with a footnote-like number. One very useful feature in the in-book menu is the ability to change the text size, making it easier to read in dimmer light or if your eyesight isn't as good as it used to be. See Figure 6-4.

You can also use the joystick nub to move a cursor through the text. Pausing over a word causes a brief definition of the nearest word at the bottom of the Kindle page. Pressing the return key takes you to the Kindle's built-in dictionary, if you want a more detailed definition.

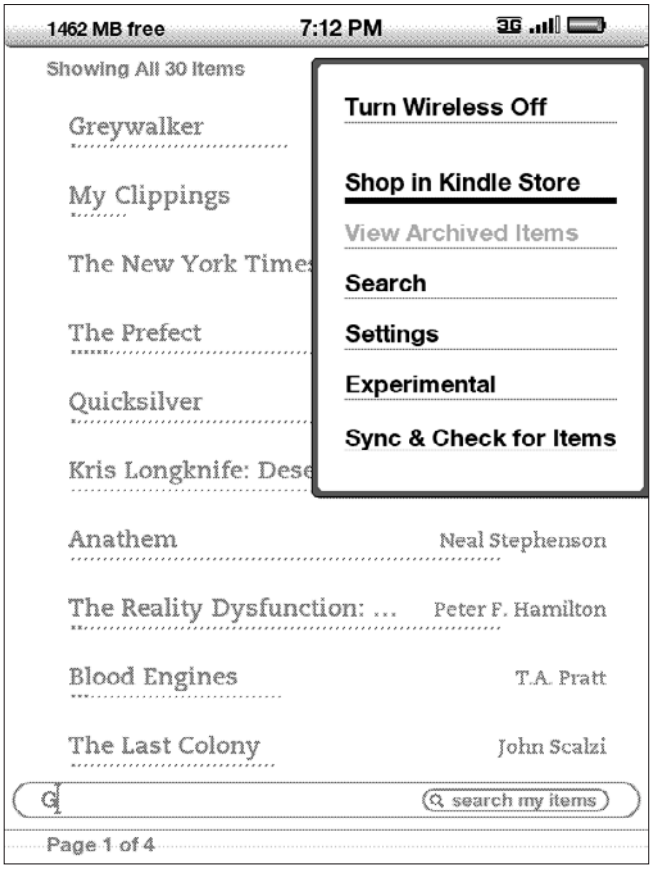


Figure 6-3: The Kindle menu on the main screen.

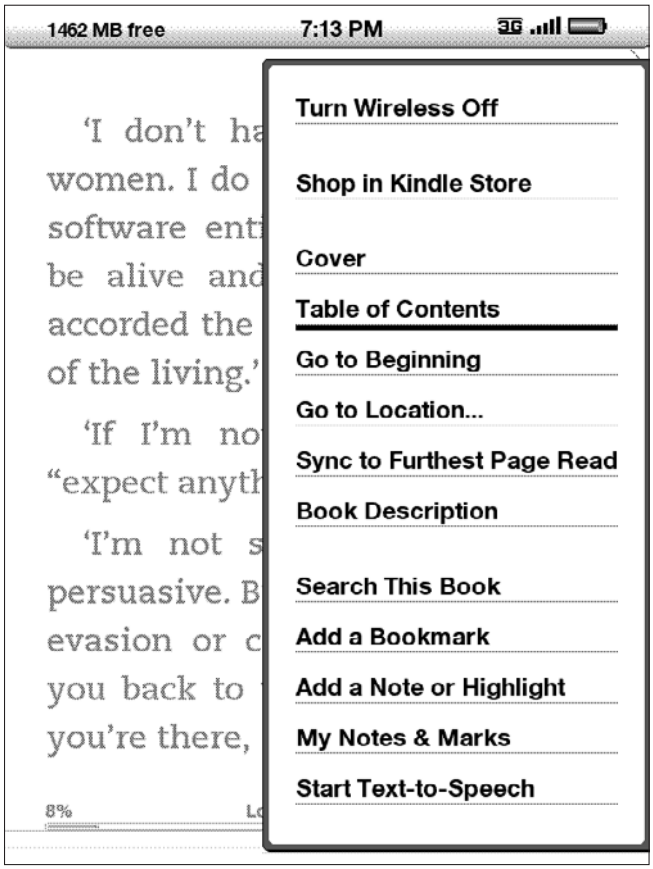


Figure 6-4: The Kindle menu when reading a book.

Every time you read a book, that book's title pops up to the top of the book list.

That's pretty much it. The Kindle 2 is an extremely simple device to use — another advantage of using a dedicated eBook reader rather than a small laptop.

Reading Blogs, Newspapers, and Magazines

In addition to books, other content is available for the Kindle 2, as shown in Figure 6-5. These include popular newspapers such as *The New York Times*, *Washington Post*, *Chicago Tribune*, *Le Monde* (if you can read French), and

many more. You pay a monthly subscription fee, which varies, depending on the publication. Color pictures are rendered in 16 shades of gray, so those don't look as good. But a newspaper supports most of the book-reading features, making reading easy and convenient.

Subscriptions to popular blogs, like boingboing.net, Slashdot, Gizmodo, and tons of other blogs, are also available. Unlike reading them for free on the Internet, you do pay a subscription fee, but it's typically only $1.99 for the more popular blogs and less for others.

If blogs and newspapers are available, what about magazines? In fact, a wide array of magazines are available. Text-heavy magazines, like those specializing in fiction, work best, while art heavy magazines are probably best avoided unless you have a Kindle DX.

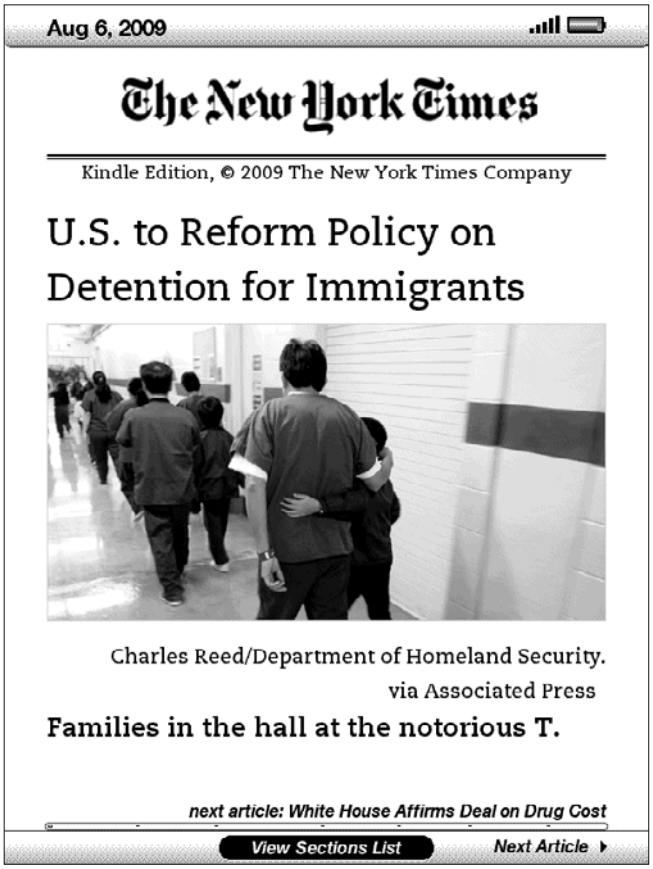


Figure 6-5: *The New York Times* on the Kindle 2.

Reading eBooks for Free!

So you have your Kindle 2. If you're like most first-time users, the ability to have hundreds of books in your backpack, purse, or messenger bag probably went to your head. You bought a bunch of books you're meaning to read.

Then your credit card bill arrives. Ouch.

Luckily, you don't need to spend hundreds of dollars on Kindle books. A vast array of books are available for free in either the Kindle's own format or the Mobipocket format, which the Kindle can natively display.

Amazon itself has a large number of free Kindle books. Most are in the public domain. For example, you can download most of William Shakespeare's plays for free (though only one at a time — the collected works cost a little money). Similarly, other classic authors, ranging from Charles Dickens to Alexander Dumas to Jules Verne, are downloadable for no charge.

Another source of free books in Kindle format is manybooks.net (`www.manybooks.net`.) There are many more sources, too numerous to mention, but you can find a unified list of free eBook sources for the Kindle at ireaderreview.com (`http://ireaderreview.com/2008/01/19/free-books-for-the-amazon-kindle/`).

Amazon also has a large assortment of titles that are not quite-free. Numerous classic titles from the golden age of science fiction (1930–1960) are available for 99 cents, for example.

So you don't need to bankrupt yourself in order to completely fill up your Kindle with more interesting books than you'll be able to read in a lifetime.

Converting PDF Files for the Kindle

If that's not enough, there are even more books available in Adobe Acrobat PDF format. Although the Kindle DX natively reads PDF format, the original Kindle and Kindle 2 do not. So how can you gain access to the staggering number of PDF books (and other PDF documents) for the Kindle?

Two utilities exist to convert PDF files. One is Mobipocket Creator, which can be downloaded for free personal use from the Mobipocket Web site (`www.mobipocket.com`). Mobipocket Creator doesn't actually convert to Kindle's .AZW format but converts to the open Mobipocket format, which the Kindle can read. Mobipocket is extremely flexible, allowing for substantial tweaking of the final output, but it is also a bit difficult to use because of all the options that must be manually set.

Another free tool is Stanza (`www.lexcycle.com/`). Stanza runs on the Mac, Windows PCs, and the iPhone. It's also a tool for reading and downloading eBooks. Converting files is very simple, but the formatting is sometimes odd.

With either Stanza or Creator, you need to connect your Kindle 2 to your PC or Mac. If it's a Creator Mobipocket file, you copy it manually to the Kindle 2 document folder. With Stanza, you export it to the correct folder.

By far the simplest way to convert PDF files to Kindle format is to use Amazon's own "experimental" service. When you buy a Kindle 2, you register an e-mail address: yourname@kindle.com. You don't have to worry about any settings, and the formatting usually looks correct.

If you take the PDF file (it must be a PDF file free of DRM protection) and e-mail it to yourname@kindle.com, you'll get back a file in Kindle format, delivered to your Kindle through Whispernet. Amazon charges 10 cents for each conversion.

If you're converting numerous, small files, 10 cents can add up pretty quickly. If you're willing to connect your Kindle to your PC and manually download the file, you can use the Amazon service for free by e-mailing the PDF to yourname@free.kindle.com. Amazon e-mails the converted file back to your Amazon contact e-mail (the one you use for your Amazon.com account). You'll have to manually download the file to your Kindle 2.

In the end, the Kindle line of eBook readers represents a new way of reading, coupling the benefits of a large, online book retailer with an eBook reader. That makes the process of buying and reading books substantially easier than previous readers. Much of that ease of use is due to the Kindle's built-in wireless service. So, what are you waiting for?

Book VIII

The Global Positioning System

Contents at a Glance

Chapter 1: Getting Uncle Sam to Ante Up

In This Chapter

- **Getting a handle on your position**
- **Knowing your options**
- **Making a connection with your PC**

Every once in a while, the U.S. federal government gives its citizens — and sometimes the entire world — a gift. When the government financed, launched, and began running the Global Positioning System (GPS), it did just that: gifted us.

GPS is a system for finding your place anywhere in the world. As long as you have a fairly clear view of the sky, where the two dozen (or so) satellites orbit the Earth, you have a pretty good chance of getting a GPS reading and finding your way to where you want to go.

Its uses are almost limitless:

- Navigate the roads, letting more advanced GPS receivers lead you along street by street. Some models even speak the directions so you can keep your eyes on the road and not on the receiver's display. You also know which direction you're traveling in and how fast you're driving.
- Find a remote fishing hole — and then find your way back to your car. You can even keep your favorite hot fishing spot a secret because with GPS you've no need to leave any sort of marker that might tip off other anglers.
- Hike in the woods without getting lost. Or at least if you do get lost, your GPS receiver helps you get un-lost. It's the modern version of Hansel and Gretel, but the bread crumbs in this case are virtual, displayed on your GPS receiver as waypoints.
- Find a lost child who is wearing a GPS receiver on his or her wrist.
- Run or jog and collect precise information about your workout.
- Make an emergency call with your new GPS-equipped cell phone and help the 911 dispatcher locate you even if you aren't sure of your precise location.

Knowing Where You Are

Where are you? I know you're there because you're reading this book. You have to be somewhere to do that. But where are you really? In precise terms.

I can tell you where I am in precise terms:

N 42.96506 W 085.92599 Elevation: 744 feet above sea level

That's with an accuracy of about 30 feet. Just enough to throw off a stalker or an angry editor. (I'm just kidding about the stalker part.) In the next chapter, I explain how to understand that reading, but for now I just want you to see how accurate GPS can be.

How'd I get this reading? By using a very inexpensive GPS receiver called the Garmin eTrex. It was a $79 Christmas gift. It doesn't talk to me and doesn't display any maps other than a very rudimentary one, but it's enough to get a basic reading from the GPS system. Figure 1-1 shows the eTrex. You can find out more about Garmin GPS receivers at `www.garmin.com`.

Figure 1-1: Garmin's eTrex GPS receiver is inexpensive.

Many other GPS receiver models do show quite detailed maps. For example, Sony (www.sony.com) sells a broad range of GPS receivers The Sony GPS

receivers and mapping programs not only tell you where you are, but they can tell you the best route from where you are to where you want to go. Figure 1-2 shows the Sony NV-U44 GPS receiver that not only shows your current position but can also keep a log of where you've been for later playback. Furthermore, it can hold a bunch of photographs on an SD card and use its screen to show off your family memories.

Figure 1-2: The Sony NV-U44, well-worn and loved.

Achieving Missile Precision — Almost

Do you have a chimney somewhere in the world at which you'd like the U.S. military to fire a long-distance missile? Using GPS, they can do it. Assuming all goes well, the missile will find the chimney, make a downward turn, and take a ride straight down. GPS is relatively new, although Santa Claus has been using a similar technique for years.

How the military uses GPS

How do you think the U.S. military makes those precision strikes during confrontations? Soldiers take a GPS reading of the target, transmit it to artillery and air forces, and get the heck out of the way. The GPS coordinates and very expensive ammunition do the rest — at least they do if no one in the area is using one of the GPS jammers available from Russia.

Being selective

On May 1, 2000, President Bill Clinton signed an order turning off the Selective Availability feature of the GPS system. Selective Availability was designed to degrade the GPS signal that was received by nonmilitary users so that the location information provided by civilian GPS units would be less precise than that of military GPS receivers. The U.S. military still has the ability to use a similar Selective Deniability feature in war zones or when there is a global terror alert, but this feature is targeted at specific areas rather than affecting all civilian users worldwide. See the article on GPS at wordiQ.com (`www.wordiq.com/definition/Global_Positioning_System`) for more information on GPS precision.

The military has an advantage over civilian GPS users: It uses some additional information to gain even more precision in GPS readings. The information is encrypted so that civilians — read: enemies — can't get the same precision. The U.S. military uses GPS in its missiles, its tanks, and other ground and air resources, and probably in ways that if I knew about they'd have to kill me.

Civilians can find their way, too

The precision the U.S. military achieves when using GPS for its guidance systems isn't quite as precise when a civilian uses the service. It's close enough for finding a fishing hole or navigating your way out of the woods, though.

The difference is so small, at least from a civilian perspective, that if I gave you the GPS coordinates for my front door, you might wind up at my back door — just enough precision to foil enemies without harming hapless hikers lost in the woods.

Actually, even civilian GPS receivers can have extremely precise measurements using a system known as Wide-Area Augmentation System (WAAS). This system relies upon ground-based transmitters whose position is very precisely known. These transmitters broadcast a signal that is matched with the satellite-transmitted GPS signal so that the normal positioning errors are reduced to such an insignificant degree that a WAAS-enabled system can be used to land an airplane in zero-visibility conditions. The WAAS system currently is only available in North America, but WAAS-enabled GPS receivers provide normal GPS accuracy even when they're used in areas where WAAS isn't available.

Most GPS receivers enable you to monitor the current signal to determine how accurately your position is being reported. Typically this information is reported using the following values:

- **PDOP (Position Dilution Of Precision):** A number representing the relationship between the error in user position and the error in satellite position using three coordinates. Smaller values are better.
- **HDOP (Horizontal Dilution of Precision):** A number similar to PDOP, but relating only to your horizontal position.
- **EHPE (Expected Horizontal Position Error):** The error in horizontal position, which you can assume under current conditions. For example, Figure 1-3 shows that the GPS receiver is probably accurate to within about 27 feet when I captured the image.

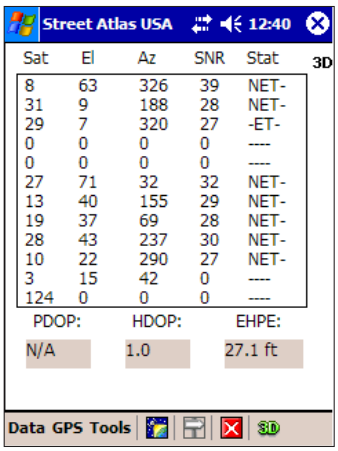


Figure 1-3: The GPS receiver has my position located within about 27 feet of my actual location.

Using GPS

What can you do with GPS and its receiver? As the list at the beginning of this chapter shows, the number of ways to take advantage of this free service are numerous. Here I go into detail on a few of the more popular uses.

Taking a hike

A GPS receiver is a must-have accessory for the outdoor types among you. It helps get you to where you want to go like a map cannot and prevents panic when all of those trees start looking alike.

Still, as my Garmin manual cautions, it's important to carry an old-fashioned compass and map with you whenever you hike in new territory. If your batteries die or the trees prevent you from getting a good lock on the satellite signals, your GPS receiver isn't much help. Also, if you're trekking into some back country or there's a possibility that the weather might turn sour, be sure to tell someone where you're planning on going so they know where to start looking for you if you don't return when you told them you'd be back.

If I was an outdoors person, and I'm not (although I do go outside to get the daily mail), I would buy one of the fancy, new two-way radios that combine a communications transceiver with a GPS receiver. I discuss these in Book VI, Chapter 3, which is about Family Radio Service and other two-way radios.

On the road again

I have a horrible time getting to new destinations. Actually, I have a horrid time finding places I've already visited, too. I don't know how many times I've driven to some strange city and found myself in the less glamorous parts of town rather than where I should be, safely in my friend's driveway.

GPS to the rescue!

Instead of relying on memory and getting all of those numbered highways mixed up in my head, I can rely on a GPS receiver to provide turn-by-turn directions. I tell the receiver where I'm going — it knows where I am, of course — and it tracks my direction and speed and lets me know when it's time to make a turn onto another highway or road.

If you're hungry on the way, some advanced models can tell you where the nearest restaurant is located. The DeLorme Street Atlas programs include information on literally thousands of points of interest including restaurants, gas stations, parks, campgrounds, and so on to make your trip far more enjoyable.

On a bike ride

It might not seem obvious at first, but a portable GPS receiver (or a PDA with a GPS accessory receiver) can be a wonderful addition for your bicycle. This is especially true if you set off on a road trip, but even mountain bikers can appreciate the way that a GPS receiver helps them find the trail in rugged back country.

If you do decide to bring along your GPS receiver on your bike, keep in mind that a bike presents something of a challenge to fragile electronic gear. Your local bike shop can probably supply a strong handlebar mount for the GPS receiver, but you may also want to shop carefully for a GPS receiver that's rated for rugged use.

It's a bird, no, it really is a plane

Private pilots travel in a world where the ordinary landmarks simply look a whole lot different than they do from ground level. It's awfully hard to read road signs from several thousand feet in the air, so getting a little extra help in determining exact position is really important to a pilot.

GPS technology has become a very important tool for pilots over the past several years. Products like Anywhere Map from Control Vision (`www.controlvision.com`) have simply revolutionized the general aviation

world because they've made it possible for virtually every flyer to realize the benefits of GPS mapping at a fraction of what it would have cost even a few years ago.

Just for fun

In the next chapter I talk about two other fun uses of GPS: finding goodies in a hobby called geocaching and finding your ancestors and their haunts in genealogy. I just mention them here briefly so you can decide whether you want to read more details in the next chapter.

Geocaching

By using your wits and a cheap GPS receiver, you can participate in something called geocaching. It's really a high-tech treasure hunt. The treasure, or cache, is usually inexpensive items, but the fun is in the chase. With coordinates in hand, you can drive to nearby locations, finding your way to the cache with GPS receiver in one hand and perhaps a can of bug spray in the other.

Genealogy

The use of GPS technology is just starting to catch on in the hobby of genealogy, which is the search for your family roots. With a GPS receiver, you can make the drive to old family homesteads easier and even find relatives' graves. Instead of requiring other researchers to retrace your steps on their own, you can provide precise GPS coordinates to make their hunt for family information and physical remnants easier.

Exploring Your Options

A wide variety of GPS receivers are available in all kinds of styles and with different levels of features. What you buy mostly depends on what its main use is, because a hiker's GPS receiver must be much smaller than one meant to rest on your vehicle dashboard.

Choosing a portable unit

When choosing a portable unit, these are some of your choices:

- Magellan at `www.magellangps.com/en/`
- Garmin at `www.garmin.com`
- Cobra at `www.cobra.com`

Each of these manufacturers offers an assortment of models aimed at different types of users. You probably want to look at several different GPS

receivers before choosing because the extra features that are included in the slightly more expensive models can greatly improve the convenience of using a portable unit.

If you intend to use your portable GPS receiver with your laptop PC, be sure to buy a unit that includes the necessary cables or adapters. These are typically not included with the least expensive models.

Driving around with a vehicle GPS unit

In the car, you have lots of options for using GPS, but don't pay it so much attention that it turns you into a reckless, dangerous, inattentive driver:

- You can buy a new car that has a fancy built-in navigation system. This is by far the most expensive option, of course, but it's the only one that's guaranteed to impress the neighbors (or make your boss start wondering if you're being paid too much). Built-in navigation systems often have a hidden cost your dealer may "forget" to mention, though. In most cases you need to buy expensive map add-ons if you want maps for the entire country.
- If you like the idea of a built-in GPS navigation system but aren't in the market for a new car, the manufacturers of portable GPS receivers offer aftermarket units that can be added to your existing car. While these might not have quite the panache of a factory-installed GPS navigation system, they're a lot more affordable, and you can move them to a new vehicle in the future.
- You can also use a Bluetooth or another GPS receiver with a laptop PC and carry it along in your car. This option is far less expensive than the other two vehicle options I mentioned, and it has one feature that trumps both of them in a big way — the laptop PC's screen is far bigger than that on any built-in vehicle GPS system. In addition, GPS mapping software for your laptop is far less expensive to update, so it's far easier on your wallet when you want to know about the newer roads.
- If you want the small size of a portable GPS receiver but you also want most of the advanced mapping options available with laptop PC GPS mapping software, you might want to consider pairing up a GPS receiver with a PDA. I talk about using a GPS receiver with a PDAPDA shortly, but this is an excellent choice in many cases.

No matter what type of GPS navigation system you use in a vehicle, it can be very dangerous to you and everyone else on the road if you don't take the time to get to know the unit before you begin driving. In fact, unless the GPS navigation system uses voice prompts to tell you when and where to turn, it's far safer to have a passenger handle the navigation duties than to try to watch the screen while you're driving.

Merging your laptop with GPS

I've already mentioned how you can use your laptop PC for navigation in your vehicle. This is a very popular option among RV owners because they usually have plenty of room for the laptop and at least one passenger who can handle the navigation while driving. In addition, GPS mapping software for laptops generally includes the locations of RV parks so you may not need a big, printed RV park directory.

Another way to use GPS with your laptop is to combine your search for Wi-Fi hotspots, which I discuss in another chapter, with GPS. Using your laptop, you can drive around, essentially mapping hotspot locations. To aid in this quest, you may want to download a trial version of WiNc from Cirond (www.cirond.com/winc.html). This extremely handy program quickly identifies all Wi-Fi connections within an area and helps you determine if you can connect to them. Cirond even offers a PDA version called pocketWiNc, shown in Figure 1-4.

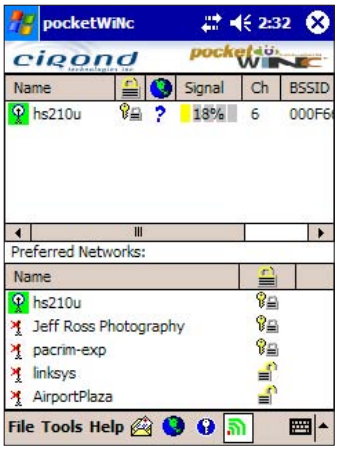


Figure 1-4: WiNc and pocketWiNc enable you to easily locate and connect to Wi-Fi hotspots.

Using GPS with a PDA

I've mentioned several times that a PDA and a GPS receiver make an excellent pairing. With the two, you have most of the size advantages of standalone portable GPS receivers and a whole raft of capabilities that you won't find in most portable GPS units. (You may want to pick up a copy of iPAQ For Dummies or PDA For Dummies — both written by Brian Underdahl and published by Wiley Publishing — to read more about what you can do with a PDA.)

Because different PDA models offer different expansion options, you'll find several types of GPS receivers that work with various PDAs. I recommend checking out the products that are available from the following:

- **DeLorme** at `www.delorme.com`
- **Sony** at `www.sony.com`
- **Teletype** at `www.teletype.com`
- **PocketMapStore** at `www.pocketmapstore.com`
- **ALK Technologies** at `www.alk.com`

In each case you should specify the type of PDA you own so you can get the proper GPS receiver.

GPS maps can eat up a lot of memory on a PDA. If you don't already have a PDA, try to get one with built-in Bluetooth, so you can use the expansion slot for a memory card to hold your maps.

Using a GPS-enabled cell phone or smartphone

Nextel has a service called TeleNav that provides audible driving directions, automatic notification when you've gone off course, and locations of nearby businesses like gas stations and restaurants. You can read more at `www.nextel.com/about/enterprise/wbs/gps/navigate.shtml`. Other carriers have similar services. Visit your carrier's Web site or call to see if they sell any GPS-enabled phones.

One very popular phone with a GPS integrated is, of course, the Apple iPhone. In fact, my doctor often brags to me while I'm lying on his table that he and his daughter went hiking in some backwater area of the United Kingdom, and when they got lost, she whipped out her iPhone and led them home. My doctor is an interesting fellow.

Saying Goodbye to AAA

Even though GPS devices rule so thoroughly, I recommend you don't take AAA or any other paper map out of the loop just yet, especially when you're using a GPS unit in the car. There's still the chance the map data you upload is not up to date, that your batteries will go dead, or that you'll have some other technical problem. Having a map gets you to the Grand Canyon long after your GPS receiver stops working. If you're hiking, a compass and a map are essential, even if you have the best GPS receiver available. In that case, your life is possibly at stake, and you don't want to rely on an electronic gizmo to get you out of the woods and back home.

GPS mapping programs for laptop PCs generally offer the option to print out both ordinary maps and those that show your selected route. These printed copies can serve as an excellent backup for your GPS unit and save you a trip to the auto club office.

Making a Connection with Your PC

There are quite a few reasons why I think you'll find that having a connection between your GPS receiver and your PC awfully handy. Examine a few of them.

Upgrading software and maps

As I mentioned in the previous section, once you move beyond the most basic portable GPS receivers, you quickly get into units that display maps rather than simply numbers to indicate your position. You may have noticed, however, that maps have a certain amount of obsolescence built in. For some reason people want to build new roads, change the course of old ones, or even just rename existing roads. That's one reason many GPS receivers offer the option to connect to your PC — so you can update the maps in the GPS receiver.

Downloading your life's movements

Virtually all GPS units can store some record of where they've been. By downloading this tracking information to your PC, you can map out the route you took in getting somewhere. Here are some possible uses for this type of information:

- Imagine how useful it would be to be able to print out maps of the trail to some hidden but beautiful picnic spot so that you could share those maps with your friends.
- If you have a consulting business where you must visit your client's locations, you could use your GPS track to justify the travel expenses you bill to the customers or that you claim on your tax returns.
- Because the GPS track also includes information about the speed of travel, you might try to beat an unwarranted speeding ticket by convincing a judge that the GPS track is an accurate representation of how you were driving. I don't think I'd bet on that working, but you're welcome to try. (Just don't blame me if the judge throws the book at you — remember, I'm not offering anything resembling legal advice here.)
- You could put your GPS receiver in your car before you let your teenager drive to the library and remind him or her that the unit tracks both speed and location. Who knows? It might just make your kid drive a bit more carefully.

Using your GPS with your laptop

Don't you just love it when you can get the best of both worlds out of a product? Well, when it comes to GPS, it's entirely possible for you to do so. There's no reason why you can't buy a small, portable GPS receiver that's perfect for taking on hikes and then connect that same GPS receiver to your laptop PC to use with the far more comprehensive PC-based GPS mapping software for trip navigation in your vehicle.

Sure, you probably have to buy a portable GPS receiver that's slightly above the bottom of the line, but virtually any of the portable units that include a PC connection cable as standard equipment can likely do the job. (You can check the PC-based GPS mapping software manufacturer's Web site to verify if a particular portable GPS unit is considered compatible.)

GPS receivers work the best in vehicles when the receiver has a clear view of the sky. The optimal location in most cars is at the front of the dashboard as close to the windshield as possible. A small piece of rubberized drawer liner (like you find in the housewares section at your local store) goes a long way toward preventing the GPS receiver from sliding around as you drive.

Chapter 2: Finding Your Way in the World

In This Chapter

- **Taking a quick mapping course**
- **Coordinating your coordinates**
- **Deciphering a GPS display**
- **Understanding waypoints**

In the preceding chapter, I give you an overview of the global positioning system (GPS). Hopefully, that chapter gives you a good understanding of what GPS is, how you can use it, and how to pick a GPS receiver. It also shows you a number of different options to fit different circumstances so you also realize that GPS isn't something just for a few dedicated hobbyists.

Now I'm going to take you to the next step, which is understanding how to read a GPS display. Most importantly, I give you a quick lesson in longitude, latitude, and related mapping terms so you know what your GPS receiver is telling you. You probably learned most of this in school, but if you're like me, you slept through most of it.

Still, while this information is interesting, it's more important to understand your GPS receiver so you can figure out how to get found when you've become lost. After all, it's unlikely a latitude and longitude reading will help much when you're lost in the middle of, say, the Adirondack National Park without any idea of how you got to wherever it is you are.

Giving Some Latitude to Your Longitude

Maybe you remember latitude and longitude from geography class, maybe you don't. It's an international way to indicate your location in the world. I don't think in international terms too much, though, so let's take a few minutes to review what latitude and longitude mean.

Figure 2-1 shows a world map divided by latitude and longitude lines. If you know the latitude and longitude values of any location on the planet, you can use those values to find that location on the map.

A GPS receiver does its magic by listening to signals from the GPS satellites and then tells you where you stand, also in the geographic sense, by determining

your precise latitude and longitude. In fact, that's how a GPS receiver is able to display your location on a map. It simply takes your latitude and longitude numbers and figures out where that position is on the map.

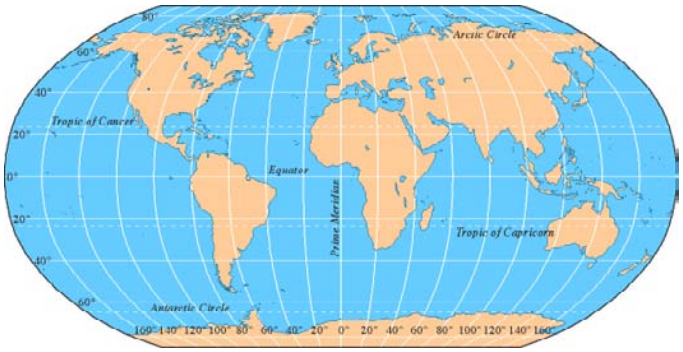


Figure 2-1: Latitude and longitude lines help you find your location on Earth.

A Quick Course on Mapping

This isn't a book on mapping or geography or even GPS, so this is a very short introduction to the three things you should know about: latitude, longitude, and elevation. Even so, this basic information should enable you to begin using your GPS receiver for simple navigation. It also helps you remember a few easily confusing facts.

A bit of simple geometry

Okay, you knew this was coming, didn't you? Yes, it's necessary to have just a brief review of geometry to make certain that we're all speaking the same language:

- When you divide a circle into degrees, there are 360 degrees in a complete circle.
- Both latitude and longitude are measured in degrees, which is often shown using the ° symbol.
- For the purposes of navigation, the Earth is considered to be essentially round. Flat Earth societies don't have a leg to stand on.
- Because latitude and longitude both indicate a position on a round planet, the total number of degrees around the Earth in either latitude or longitude is 360 (even though, as you discover shortly, the values are expressed a bit differently, they do add up to 360).
- Fractions of degrees are measured in minutes, with 60 minutes in 1 degree. The symbol for minutes is '. Don't get geometrical minutes mixed up with temporal minutes.

- Likewise, fractions of minutes are measured in seconds, with 60 seconds in a minute. The symbol for seconds is ". That's to further confuse people who use the clock on their GPS devices.
- Sometimes, though, fractions of degrees are expressed using decimal values rather than minutes and seconds. The results are the same, but just a bit of math is involved in converting between the two. For example, 39 degrees and 30 minutes could also be shown as 39.5 degrees (because 30 minutes is one-half of a degree). It could also be shown as 39° 30'.

That wasn't too bad, was it? Now that you've got the simple geometry out of the way, see how it applies to latitude and longitude.

Latitude

The lines of latitude run east and west around the globe. The equator is basically a line of latitude. Latitude is shown as degrees north in the Northern Hemisphere and as degrees south in the Southern Hemisphere. Starting at the equator, which is zero, when you go north, the north latitude rises to 90 degrees when you reach the North Pole. When you go south of the equator, the south latitude reaches 90 degrees when you hit the South Pole.

So, for example, Reno, Nevada, is located at approximately 39 degrees and 30 minutes north latitude, while Los Angeles, California, is at about 34 degrees north latitude. From these two values you can tell that Reno is farther north than Los Angeles — and that's without looking at a map.

Longitude

The imaginary lines of longitude run north and south. The zero-degrees longitude line runs through Greenwich, England, which is called the prime meridian. If you went west of the prime meridian and a friend went east, you'd eventually meet up at the International Date Line. You would go 180 degrees in both directions. (Remember how I told you the numbers would add up to 360?)

In the Eastern Hemisphere, the longitude is given as degrees east. In the Western Hemisphere, longitude is given as degrees west. You may also see west longitude expressed as a negative value. That is, W119° is the same as –119°.

Going back to the earlier example, you find that Reno is at about W119° 50' while Los Angeles is approximately W118° 15'. Hey, wait a minute! That puts Reno west of Los Angeles, doesn't it? Well, yes it does, and that's exactly why understanding a little bit of geometry is so important. (Go ahead, look on a map and you see that Reno actually is farther west than Los Angeles — you can win a bar bet with this one.)

Elevation

Elevation is basically the distance you're standing above the level of the world's oceans, called sea level. If you're on a high mountain, you're obviously at an elevation much higher than sea level.

When using a GPS, you must receive signals from a fourth satellite to measure your elevation. You only need three visible satellites if all you need is your two-dimensional position in the world. GPS receivers typically display 2D to indicate a two-dimensional fix and 3D to indicate a three-dimensional fix. A fix is simply the navigational term for knowing your precise location.

Coordinating Your Coordinates

Latitude lines are always parallel to the equator and to each other. Longitude lines, however, are not really parallel to each other because they meet at the north and south poles.

One important result regarding the difference between latitude and longitude lines is that a one-degree change of latitude is always equal to the same distance (ignoring elevation differences, of course), but a one-degree change of longitude varies. Look at how this can be:

- Going directly north or south changes your latitude but not your longitude. One degree of latitude change equals just about 70 miles. You could figure out the circumference of the Earth and divide that by 360 to verify this, but your number comes pretty close if you do.
- Going one degree east or west at the equator changes your longitude but not your latitude. Again, if you're at the equator, one degree of longitude change is also about 70 miles (because the Earth is round, so the circumference around the equator is virtually the same as it is on one of the longitude lines).
- Now, to blow your mind. Imagine that you are standing exactly at the north pole. Take one step south (that's any direction from where you are). That places you about 3 feet away from the north pole. If you stay the same distance out and walk all the way around the pole, you'll go about 20 feet. *But that 20 feet brought you all the way around the world so you traveled through 360 degrees of longitude!* A little math tells you that one degree of longitude change here is a bit less than an inch. How can this be? Well, the latitude lines are parallel (running east and west, remember), so the circles going entirely around the world are much shorter than they are at the equator. Because the longitude lines all meet at the poles, each of them is exactly the same length.

It's easy to see how this could be confusing, so aren't you glad that your GPS receiver does all of the math for you? And aren't you glad that I went to the north pole to do the measurements so you wouldn't have to?

Explaining How GPS Works

I'm not an engineer or anything close, but I think I can describe in simple terms how the GPS system works. It's not like it's — well, actually, in this case it really is — rocket science, but the general idea is fairly easy to understand.

Imagine for a moment that you have found three posts pounded into the ground in a triangular pattern somewhere in your yard. One day you're down at the library, and you come across some historical records that mention that the town recluse used to live on your property and that before he died he told someone that he had buried some treasure exactly 100 feet from the posts. Can you figure out where to dig without ruining all of the landscaping you've so carefully added to your yard?

Actually, that's a pretty simple problem because there's only one solution. If you tie a 100-foot string to each post and then see where the three ends meet, you've found the spot because there is no other place that's exactly 100 feet from all of the posts (as shown in Figure 2-2).

The GPS system works something like those three strings. Of course, it uses satellites instead of posts, but using several satellites, it can determine where you are, as you see in Figure 2-3. The rocket scientists figured out how to calculate the precise position of each GPS satellite, all of which are in geosynchronous orbit, at each point in time, and they know that radio signals travel at the speed of light, so throw in a little fancy math, and bingo!

Now, it takes not three, but four GPS satellites to fix your location. That's because you need one more measurement than the number of dimensions to rule out multiple positions in the remaining dimension. Get it?

In the example of using three strings to find the buried treasure in your yard, you assumed that where the three strings touched the ground was where the treasure was buried. If you held onto those three strings and raised them up above the ground, you would find that they would still meet, even if you held them above your head. The same thing happens with the GPS satellite signals, but once you add a fourth signal there's only one point that can be your location.

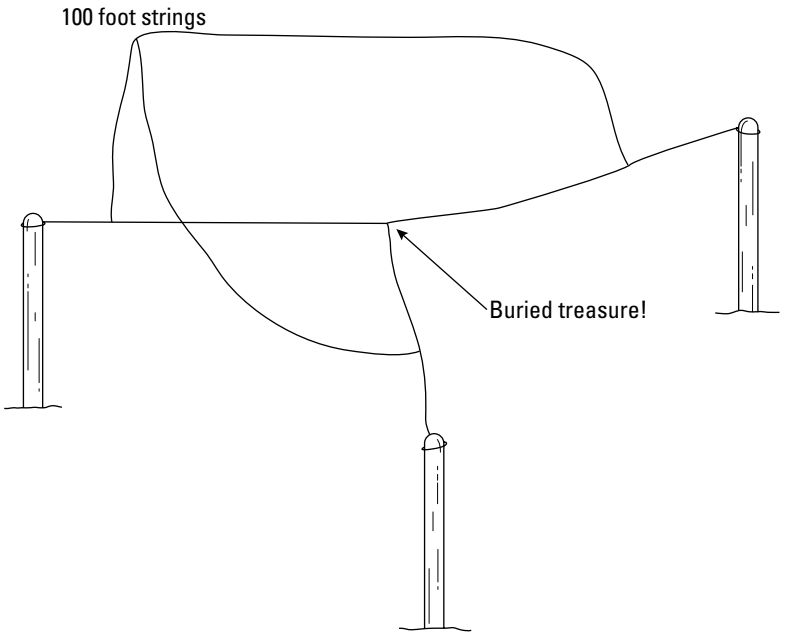


Figure 2-2: You can locate a point by carefully measuring the distance from known points.

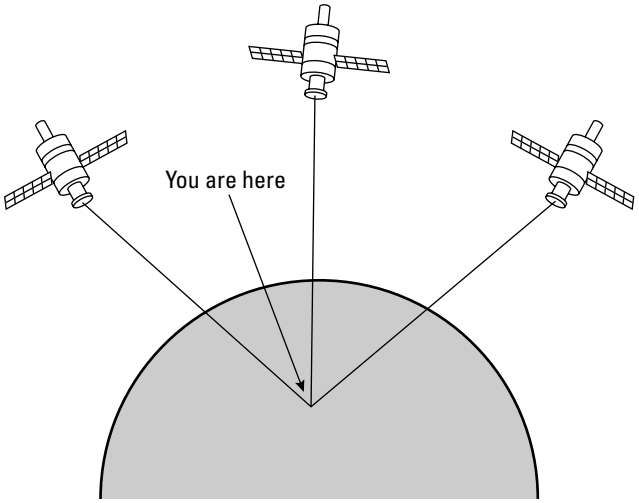


Figure 2-3: You can locate your position by carefully measuring the distance from the GPS satellites.

Figure 2-4 shows an example of how a GPS receiver shows a display of the satellites that are being tracked. In this case the display symbols indicate that four satellites are being used for navigation, and the 3D indicator near the upper right of the display tells you that the unit has a 3D fix. GPS receivers

often have more satellites in view than are being used for navigation simply because the data from some of the satellites might not be coming through reliably enough for navigation purposes.

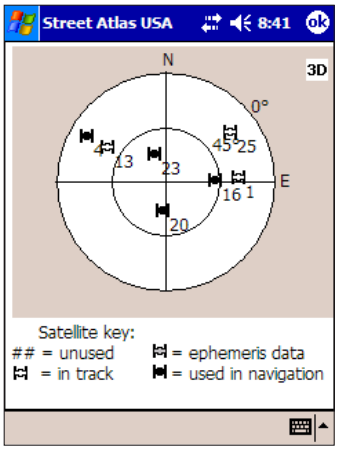


Figure 2-4: The GPS receiver is tracking seven GPS satellites and using four of them for navigation.

Reading a GPS Display

I own a Sony NV-U44 GPS device, but these examples are from my old Garmin eTrex GPS receiver. Like most modern GPS receivers, you can choose how to display your coordinates. That is, you can choose degrees, minutes, and seconds or you can opt for degrees and decimal fractions.

For example, my location in a digital format, according to the display on my GPS receiver, is this:

N 42.96506 W 085.92599

Using the degrees, minutes, and seconds display, the following represents the same location:

42° 57’ 54.4” N 85° 55’ 33.6” W

That means I’m in the Northern and Western hemispheres. To be exact, I’m in this location:

42 degrees, 57 minutes, and 54.4 seconds north of the equator

85 degrees, 55 minutes, and 33.6 seconds west of the prime meridian

That puts me in West Michigan. If you look at the digital equivalent of my location you can see how the 42 degrees, 57 minutes, and 54.4 seconds were simply converted to 42.96506:

N 42.96506 W 085.92599

The same was done with the second half of the coordinates. It's 57 minutes of one way and 0.96 of the other. In other words, they're the same coordinates, just expressed differently.

That's important to know because you may see coordinates expressed one way, but your GPS receiver may be set to display them another way. Usually, you can make a quick conversion to the coordinates of your choice by going into your receiver's setup menu and selecting Units or something similar.

Figure 2-5 shows how a GPS receiver display might look using the degrees and decimal degrees option, and Figure 2-6 shows the display when the degrees, minutes, and seconds option is selected. Note that these two readings do not show precisely the same location.

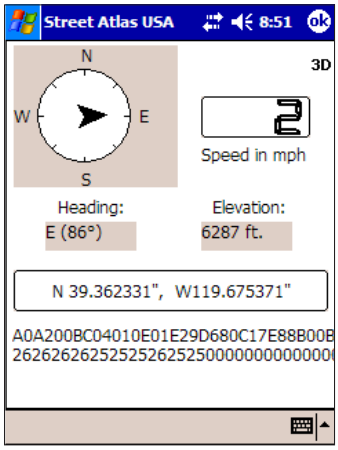


Figure 2-5: The GPS receiver is displaying coordinates using degrees and decimal degrees.

Due to rounding errors, you may not get precisely the same values when you try to convert between the two types of display. It's always best to pick one method and stick with it to avoid these types of errors.

Figure 2-7 shows one very good reason why you may prefer to use a GPS receiver that displays your position on a map rather than using latitude and longitude coordinates. I don't know about you, but it's a lot easier for me to determine my location by looking at the map display than by reading the coordinate display.

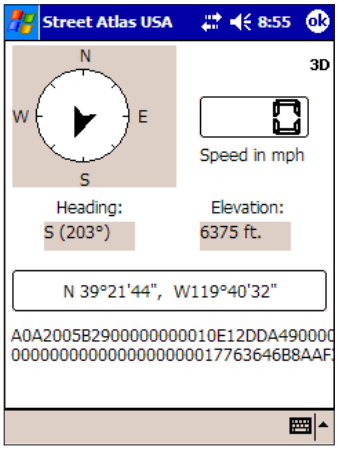


Figure 2-6: The GPS receiver is displaying coordinates using degrees, minutes, and seconds.

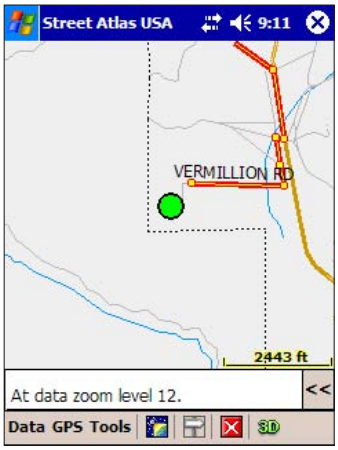


Figure 2-7: The GPS receiver is my current location using a map display.

Finding Your Waypoints

Waypoints are the essence of basic GPS navigation. At the simplest level waypoints are just the various points along the route between where you are and where you want to go. Even if you've never used a GPS receiver before, you've certainly used waypoints — you probably just didn't use that name for them.

Understanding how waypoints work

To understand how waypoints work, consider the following set of directions:

1. Take Highway 395 south to the junction of Highway 341.
2. Turn left on Highway 341.
3. Turn left at the intersection with Cartwright Road.

Those directions seem clear enough, don't they? Well, waypoints work pretty much the same way except that waypoints are often indicated using geographical coordinates in place of the names or numbers of roads or other physical objects. In fact, that same set of directions could be expressed using two waypoints (because the directions tell you to turn in two places) as in the following:

1. Go to N39° 24' 10.1", W119° 44' 46".
2. Go to N39° 21' 59.1", W119° 39' 59".
3. Turn left.

Although it's true that both sets of directions get you to the same place, the directions that use waypoints offer one distinct advantage over the directions that use highway names and numbers. Can you spot the important difference? The first set of directions is pretty useless without additional information — such as an assumed starting point. The sets of directions using waypoints need no other details because anyone with a GPS receiver can follow them, no matter where the trip began.

Even though this example only uses two waypoints, that doesn't mean that you necessarily want to set off on a cross-country hike directly between the two waypoints. You might find a number of obstacles in your path that prevent that sort of straight-line approach. If you use a GPS receiver that displays maps, you might want to choose the option to create a route that uses roads rather than to create a direct route. (The method for choosing this varies according to the type of GPS receiver you use.) But even if you choose the direct route option, your GPS receiver shows you the distance and direction to your next waypoint, just as you see in Figure 2-8. This means that if you have to navigate around a steep hill, a lake, or even a large building, your GPS receiver shows you how to reach the waypoint.

Creating waypoints

You can create your own waypoints a number of ways. The precise methods depend on your particular GPS receiver, of course, but generally you'll probably find that you have at least some of these options available:

- Enter waypoints manually by entering latitude and longitude coordinates before you set out with your GPS receiver. This method requires that you know the coordinates, of course, but it allows you to set very accurate waypoints.

- The manual process may also be as simple as clicking points on an on-screen map. This generally won't be quite as accurate as entering specific latitude and longitude values, but it's far more convenient.
- Most GPS receivers allow you to manually set waypoints at your current location. This method is very handy if you're out for a walk in a strange city and want to be sure that you can find the way back to your starting point.
- Many GPS receivers offer an automatic tracking option. Typically, this option creates waypoints at specific time intervals so you can later play back a record of your travels. If you use this option it's a good idea to learn how to set the recording interval. That way, you can set a value appropriate to your mode of travel — shorter intervals for vehicular travel and longer intervals when you're on foot.

Portable GPS receivers typically have a limited amount of available memory. If you set the recording interval too short you can lose your earlier recorded waypoints when the memory becomes full. As you can imagine, this could make it difficult for you to backtrack in unfamiliar terrain.

The popularity of GPS receivers has generated a whole new hobby — exchanging lists of useful and interesting waypoints. Web sites such as GPS Waypoint Registry (`www.waypoint.org`) are dedicated to collecting and sharing lists of these waypoints.

This chapter has helped you understand a bit more about how to use your GPS receiver. Although there wasn't room for an entire course on the finer points of GPS usage, I'm sure that you're far more comfortable about how you can use your GPS receiver to get from where you are to where you want to be.

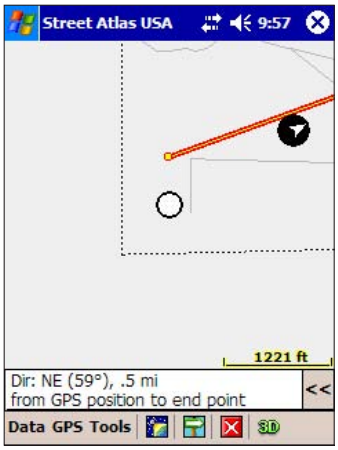


Figure 2-8: The next waypoint is a half-mile to the northeast from my current position.

Chapter 3: Exploring with the Rest of GPS

In This Chapter

- **Exploring geocaching**
- **Using GPS to find cemeteries**
- **Finding your ancestors' homesteads**

A popular hobby called geocaching uses your GPS receiver to track down plots of small prizes hidden around the globe. GPS stands for Global Positioning System, and it can be used for more than simply finding your way out of the forest.

The second use is a more practical one. You can use GPS coordinates in genealogy research, both for finding cemeteries (and even specific gravestones) and your ancestors' old homesteads, schools, churches, and other sites.

Seeking and Hiding with Geocaching

GPS is not only about using the technological equivalent of bread crumbs to find your way out of the forest. It also helps provide the basic navigational tools for geocaching, helping you pinpoint within feet the location of hidden caches that others have left for you to find.

When you've mastered the seeking, you may want to try the hiding part. You can create your own caches, maybe right in your backyard, that others can seek. There are even groups and Web sites dedicated to this hobby. Here are some popular geocaching Web sites:

- `www.geocaching.com`
- `www.navicache.com`
- `www.terracaching.com`
- `www.earthcache.com`

Check these out, lurk in their communities, and see which one is most exciting for you.

Playing it safe while playing

Having fun shouldn't lead to forgetting about good old common sense. Consider these things before heading off:

- Travel in pairs.
- Let someone know where you're going if you go out to look or hide a cache.
- Carry ID, water, and a flashlight if you're hiking.
- Make sure you get permissions to hide a cache on property if it's not yours.
- Make sure you know what the park rules are for hiding things.
- Follow your instincts, and don't do something if your gut is saying not to.

Nabbing the cache

Given the choice, you probably would rather nab cash. But geocaching leads to its own treasures, many of them you keep while others you take to the next cache location and exchange for something else. You can do this on and on, traveling across the United States and other countries (but mind the oceans, lest you find yourself with some wet cache).

For those who love technology, the outdoors, and a good quest, it's a perfect hobby. It's a little like a modern-day version of scouting, where you might have earned an orienteering badge for your skills with a map and compass. Now you're using your map, compass, and GPS navigational skills. You can do it with friends and family; you breathe the clean air of mostly remote areas and improve your navigational skills for the day you might need them. (On the other hand, staying inside is safer and dryer. But I'm assuming you like the outdoors.)

In most instances the hidden caches are tucked away in a hidden location in a public place. Don't expect to be digging for buried treasure in someone's yard — if you do, you're probably looking in the wrong place, and you're likely to get arrested, to boot.

You don't need an expensive GPS receiver for geocaching. An inexpensive model that's $75 or even less is enough to get you going. Later, if you want a better GPS receiver that allows you to carry pictures and music and stuff, you always can spend a little more money ($150 to $200) for an advanced model. See Book VIII, Chapter 1, for more information about your options in buying a GPS receiver.

You can find nearby caches by searching on the one of the Web sites listed above. At most such sites, you can search by ZIP code, state, country, and other variables. Once you find a cache you want to find, www.geocaching.com, for example, has some suggestions for hunting it down:

- Research the cache location. Buy a topographical map for remote cache locations. Use services like Google Maps (maps.google.com) or MapQuest (www.mapquest.com) to get driving directions for more easily accessible ones. Google Maps even has street level views of many locations, so you can familiarize yourself with the terrain in advance.
- If you're familiar with the area, navigate there using mostly the readings from your GPS unit. The site www.geocaching.com doesn't recommend this for first-time hunters. However, you may need to use a combination of all three strategies to find a cache. Bringing along a compass is a good idea, too.
- Drive as close to the cache location as you can. When you get within 300 feet, check your GPS receiver's margin of error. It could be between 25 and 200 feet. The smaller the error, the more you can rely on your receiver's reading. For the last 30 feet or so, circle the area to find the cache. For higher error rates, the circle is larger.
- When you find the cache, at least write your name in the enclosed log book. If you want to take an item from the cache and replace it with another, that's great, too. This is all done under the honor system, of course. You're not supposed to find the cache, take all the loot, and run off for an early retirement.
- **When you leave your car, mark a waypoint on your GPS receiver.** This way, you can find your way back to the car. Otherwise, you may need to wait for the next person who finds the cache, so they can lead you back to civilization. (For more information on waypoints, see Book VIII, Chapter 2.)

Hiding the bounty

Once you have mastered the art and science of geocaching, you may want to try your hand at hiding your very own cache.

As for goodies, you can put just about anything in your cache. Yes, even cash — which would make you a very popular person indeed on the geocaching circuit! Many caches contain inexpensive toys, CDs, and any other knickknacks you can imagine and that fit into the container used in the

cache. Some people even include one-time-use cameras, asking all the finders to take a photo of themselves (and, of course, then leave the camera for the cacher).

The site `www.geocaching.com` makes these recommendations for hiding your own cache:

- **Research the location.** Look for someplace that may require some hiking, rather than an easy-to-find place close to well-traveled areas where someone may discover the cache accidentally.
- **Prepare your cache.** Your best bet is a waterproof container. You can place the actual items inside sealable plastic bags like those you use for sandwiches. Include a log book (small spiral notebook) and pen or pencil so seekers can record their find. Consider including a goodie that finders can take with them, and asking them to leave something behind, via a note in the cache container.
- **Hide the goods.** This is where you use your GPS receiver. Get the cache's coordinates by taking a waypoint reading. For better accuracy, you should average the waypoints. If you're using a low-end GPS model, this may require taking a waypoint up to ten times — you take a waypoint and then walk away, returning to do another one — and then finding the average waypoint measurement. This average is what you write on your container and in the log book, keeping a copy for the next cache you find.
- **Leave a note**. Figure 3-1 shoes a typical geocache note.
- **Report the cache.** This involves filling out an online form on www.geocaching.com or another site. Information includes cache type, size, coordinates (of course!), overall difficulty and terrain ratings, a description, and optionally, hints.

Letterboxing: Geocaching sans batteries

What do you get if you take geocaching and substitute the GPS receiver with a compass? Letterboxing, a low-tech version of geocaching. And in this case, letterboxing has nothing to do with black bars on your TV set.

Instead of taking a trinket and leaving one, as you do in geocaching, letterboxing involves leaving your mark at every treasure location by stamping a log book with your own customized rubber stamp. You use another rubber stamp, stored in the cache box, to stamp your own book, like a passport.

If you wake up one Saturday morning and find your GPS receiver's batteries are dead, a similar hobby awaits you. That is, if you're handy with a compass.

You can read more about letterboxing at www.letterboxing.org.

GEOCACHE SITE - PLEASE READ

Congratulations, you've found it! Intentionally or not!

What is this hidden container sitting here for? What the heck is this thing doing here with all these things in it?

It is part of a worldwide game dedicated to GPS (Global Positioning System) users, called Geocaching. The game basically involves a GPS user hiding "treasure" (this container and its contents), and publishing the exact coordinates so other GPS users can come on a "treasure hunt" to find it. The only rules are: if you take something from the cache, you must leave something for the cache, and you must write about your visit in the logbook. Hopefully, the person that hid this container found a good spot that is not easily found by uninterested parties. Sometimes, a good spot turns out to be a bad spot, though.

IF YOU FOUND THIS CONTAINER BY ACCIDENT:

Great! You are welcome to join us! We ask only that you:

- Please do not move or vandalize the container. The real treasure is just finding the container and sharing your thoughts with everyone else who finds it.
- If you wish, go ahead and take something. But please also leave something of your own for others to find, and write it in the loghook.
- If possible, let us know that you found it, by visiting the web site listed below.

Geocaching is open to everyone with a GPS and a sense of adventure. There are similar sites all over the world. The organization has its home on the Internet. Visit our website if you want to learn more, or have any comments:

http://www.geocaching.com

If this container needs to be removed for any reason, please let us know. We apologize, and will be happy to move it.

Figure 3-1: A copy of a letter you can leave in your cache box.

Finding Your Ancestors

GPS receivers can help you find your way, plot your course, and always let you know where you stand in the world. One thing it can't do is help you find your soul. Believe me, if it could, I'd be in better shape.

Enough about lost souls. I have something pretty close to a soul, and that's discovering my past by tracking down where my ancestors have tread. Even if you know where deceased relatives lived, it's often difficult to find their old homesteads.

A very grave matter

Speaking of souls, you can use your GPS receiver to find burial sites. Some kind people have already logged the latitudinal and longitudinal positions of some cemeteries and share them with others on a Web site called The U.S. GeoGen Project (`www.geogen.org`).

In many cases, it's an even more difficult task to find old cemeteries, some of which aren't as preened and tended to as those where our closest relatives rest. They may be in heavily wooded areas. Or, worst of all, vandals or developers may have tipped over or removed headstones so that you're not even sure that what you're visiting is a cemetery. If you have a map that lists the cemetery, have jotted down its longitude and latitude coordinates, and are heading there with a GPS receiver, you have a much better chance of actually finding it, like the person shown in Figure 3-2.

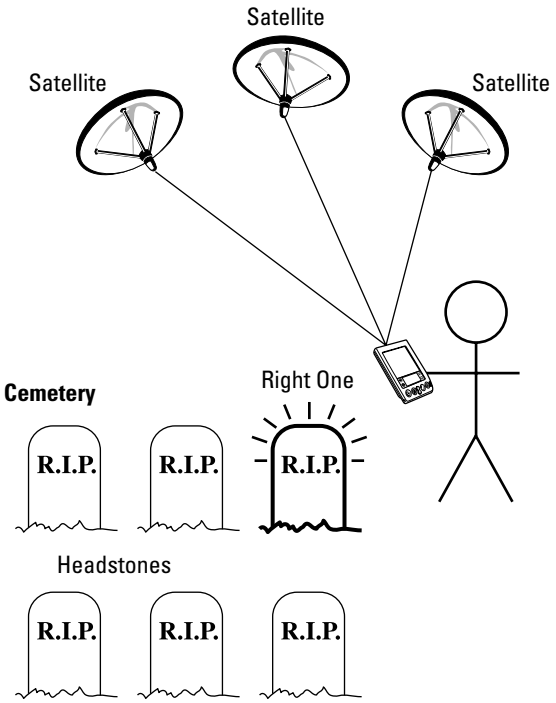


Figure 3-2: Your GPS receiver can help you find an ancestor's grave or homestead.

The original author of the first edition of this book enlisted his adventuresome mother in a quest for a great-grandfather's grave. They knew the cemetery, but not the location of the gravestone.

The author had the cemetery's name, so I bet you're thinking the rest was easy. Far from it. It was a large cemetery. There were thousands of gravestones, many of them flat against the ground so you could see them only after walking up to each and every one. And just finding the cemetery wasn't easy.

Now imagine you have the GPS coordinates for the cemetery and that, maybe from another genealogist's efforts, you even have the latitude and longitude of the actual grave. Now that's something! Imagine the time you'd save. Even with GPS readings that have a margin of error of 20 feet or so, you have narrowed down the search considerably.

This isn't a book on genealogy, and I'm assuming you can figure out how to narrow down your search of cemeteries where your ancestors may be buried. GPS technology isn't going to help you find these sites unless you know they are places to look for family headstones.

Once you have a good idea of which cemeteries are good bets, either because they are close to where ancestors lived or are located on the family land, you can use maps and other tools to find the coordinates. From there, it's a matter of using your GPS navigational skills to reach each one and check them out.

In addition to the U.S. GeoGen Project's Web site mentioned earlier, a good place to look for coordinates of cemeteries is the Geographic Names Information System (GNIS). The GNIS contains information about nearly 2 million U.S. physical and cultural geographic features. Many of these include associated latitudinal and longitudinal coordinates to enter into your GPS receiver to help you find them.

Here's how you do a quick search of the GNIS:

1. **Point your browser at http://geonames.usgs.gov/.**

   The GNIS home page appears.

2. **On the top, click Search Domestic Names (if you are looking for U.S. landmarks).**

   A query form appears.

3. **You can search many different ways. To search for a specific cemetery, as shown in Figure 3-3, do the following:**

   1. Type in the name of the cemetery.
   2. To narrow it down a bit, type in the county name and choose the proper state.
   3. Select Cemetery under Feature Type.
   4. Click Send Query.

   The site can sometimes take a painfully long time to search, but eventually it displays a list of search results, as shown in Figure 3-4.

Where is (old) home sweet home?

As I do a bit of genealogical research to find the source of my genes, I sometimes come across confusing maps showing where this or that ancestor made his home. I can't go to the grocery store without getting lost, so you can imagine my confusion when reading these homestead maps, let alone actually traveling to an old homestead.

Wouldn't it be easier if I knew the longitude and latitude of places I want to visit and then use my GPS receiver to find them? Why, yes, it would be easier.

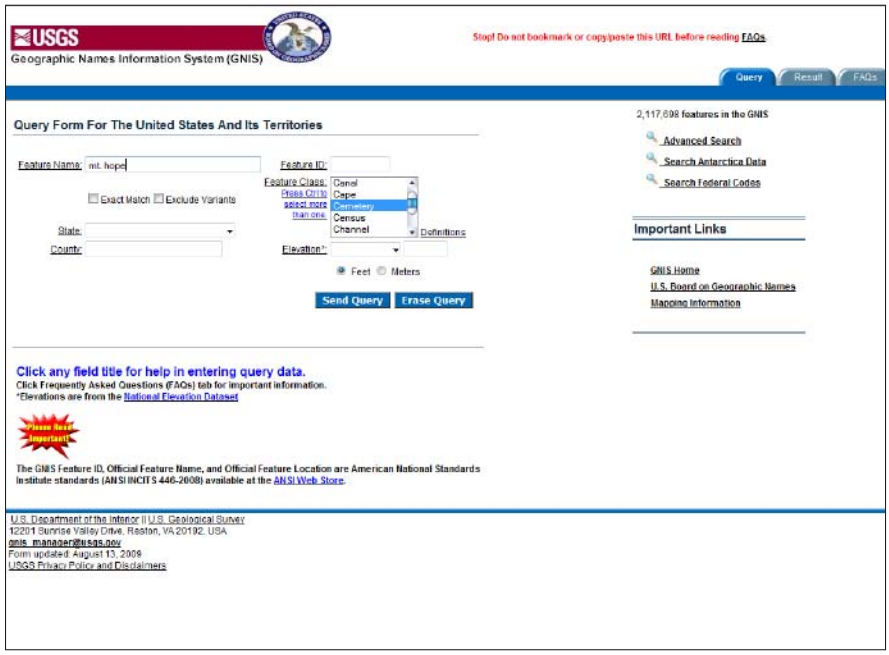


Figure 3-3: Searching for a particular cemetery

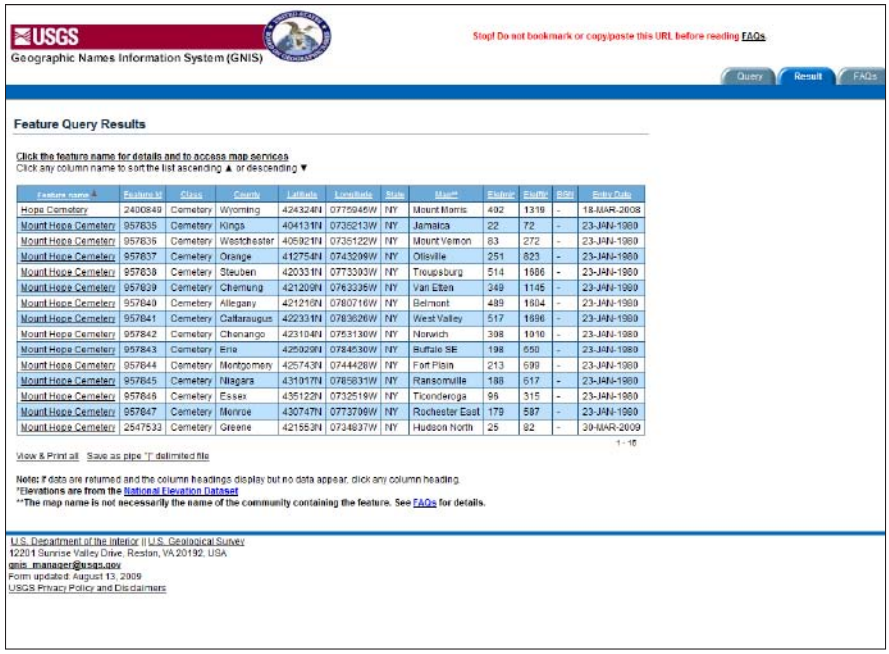


Figure 3-4: A list of cemeteries in New York State with the name Mount Hope.

Just like finding cemeteries with Uncle Sam's (celestial) help, you can use GPS coordinates to help locate where your relatives migrated within the United States. Why not just use a map? Like I said, I get lost on the way to the bathroom, so simply finding a location on a map, perhaps in another state, and driving there is not a reasonable expectation.

Instead, you can use the GPS navigation skills you discovered in the preceding chapter to travel to locations you want to visit as part of your genealogy research. Remember, these towns may be so small that they are difficult enough to find on a map. By using your GPS receiver, especially one designed for automobile use, you can find those homesteads quicker by following the coordinates.

Don't forget to write down and make available the locations' coordinates to genealogists, homesteads, farms, county courthouses, and local libraries.

Glossary

802.11 series: Wireless standards that include 802.11a, 802.11b, 802.11g, 802.11n, and other current and future related standards. Generally, 802.11g and 802.11n are used for Wi-Fi hotpots.

802.11a: The first 802.11 standard in the 5 GHz range, which offers 54 Mbit/sec.

802.11b: The original 11Mbit/sec wireless standard in the 2.4 GHz spectrum.

802.11g: An improvement on 802.11b that gives 54 Mbit/sec.

802.11i: A standard that dictates how wireless security is to be handled. This is currently implemented in WPA2.

802.11n: The latest wireless standard that, as of this book's publishing, is still a draft standard. When the standard is complete, you might need a firmware upgrade to your router to comply.

802.1x: An authentication scheme for Wi-Fi. Mostly used in corporate environments.

access point: A wireless device that serves as a communications hub for Wi-Fi clients.

ad hoc mode: A mode in Wi-Fi networking where one computer connects directly to another computer, bypassing a central access point.

adware: Software that interferes with Internet advertising, or that which inserts extra advertising into your Web browser.

analog: Something that relies on wave forms that can take on many values, such as human speech or radio waves.

antenna: A metal rod or wire used to transmit and receive radio signals. All wireless technologies use some kind of antenna, even if it's so small you cannot see it.

band: A group of frequencies.

BlackBerry: A handheld device made by Research in Motion (RIM) that lets you access your e-mail and browse the Web anywhere there is wireless coverage.

Bluetooth: A wireless technology operating in the frequency range of Wi-Fi communications, but has a much shorter range. Mostly used as a substitute for cables on the desktop (keyboards, mice) and in cell phone applications (wireless link between a headset and phone).

botnet: A collection of computers infected with malware that forces the computer to do work on behalf of the botnet owner. This work might be attacking a Web site or sending out e-mail spam.

bridge: Lets you connect two or more networks together. For your purposes, it usually means connecting a wireless network to a wired network.

cable modem: A device that connects between your cable TV company's Internet connection and your network or computer. It enables you to send and receive information over the Internet using a coaxial cable that runs into your home.

cellular phone: A mobile telephone that uses a network of short-range transmitters to communicate with the landline phone system.

coaxial cable: Cable used for cable TV and some other applications.

cordless phone: A wireless phone usually used inside the home or yard that operates over one of three frequency bands: 900 MHz, 2.4 GHz, or 5.8 GHz.

cracker: Someone who hacks into a network with malicious intent.

DHCP: The dynamic host configuration protocol provides a way to automatically allocate IP addresses to computers on a network.

digital: A signal, composed of 1s and 0s, used to transmit information.

Digital Media Adapter: A device that plays back audio or video files streamed over a network that have been encoded in some digital format.

DLNA: Short for Digital Living Network Alliance, an industry consortium. DLNA defines protocols for consumer electronics devices to connect to PCs and each other.

Domain Name Service (DNS): A global system of computes and a protocol that lets you convert names like `www.dummies.com` to an IP address.

driver: Software that allows hardware to communicate with your computer's operating system. Each piece of hardware, such as a network adapter, has its own driver. The manufacturer usually provides the driver.

DRM (Digital Rights Mangement): Methods to protect digital media from unauthorized copying.

DSL: A digital subscriber line which allows you to receive the Internet over the same wires as your telephone service. This is one way to get broadband Internet access.

DSL modem: A device that connects between your telephone company's DSL connection and your network or computer. It enables you to send and receive information over the Internet using a telephone line that runs into your home.

eBook: Also, eBook Reader. eBook readers are hardware consisting of an electronic paper display suitable for reading documents.

encryption: Scrambling information as a way to secure it.

ePaper: ePaper is a display technology that's reflective, rather than generating its own light. These displays do not require that the display be refreshed, so they use very little power.

Ethernet: A protocol that describes how most computers can talk to each other, either over wired or wireless medium.

ExpressCard: The next generation of PC cards for laptops. ExpressCards are around the same size as a PC Card but have a different pinout.

firewall: Software that inspects incoming and outgoing traffic, and allows or blocks it, depending on your security policy.

firmware: A small software program inside hardware, such as routers, that controls the hardware.

Fiber optics: long glass fibers that carry network signals in the form of light instead of electricity. Fiber optics have much greater range than copper wire.

GHz: Gigahertz. A wave with a frequency of 1 GHz oscillates 1 billion times per second.

global positioning system: Worldwide network of satellites operated by U.S. Defense Department that enables civilian and military users to pinpoint their location on Earth.

GPS: *See* global positioning system.

hacker: Originally referred to a person who was able to perform great technical feats. In recent times, it has become synonymous with "cracker." *See* cracker.

HDTV: High-definition TV.

hotspot: A wireless access point that's found in a public place such as a library or coffee shop.

hub: A hardware device used to connect two or more network devices.

IEEE: The standards body responsible for Ethernet and most wireless protocols. Pronounce this as "eye triple e."

infrastructure mode: A mode in Wi-Fi networking where computers connect through one or more access points. This is the most popular way of creating a wireless network.

instant messaging: IM. A technology that allows for real-time, two-way text communications between two or more individuals. Yahoo!, MSN, and AOL operate the largest IM networks.

interference: Electrical noise or conflicting radio signals that cause a deterioration in the radio signal in Wi-Fi and other wireless communications.

Internet service provider (ISP): A company that sells you access to the Internet. This is usually a cable or telephone company.

IP address: A number in the format *xxx.xxx.xxx.xxx* that designates a host address on the Internet. Each domain name, such as `www.google.com`, has one or more associated IP addresses.

KB: Kilobytes.

Kb: Kilobits.

kHz: Kilohertz. A wave with a frequency of 1 kHz oscillates 1,000 times per second.

Kindle: Amazon's eBook reader, which is tied closely to Amazon's book-shopping service. Two current versions are available, the Kindle 2 and Kindle DX, with different-sized screens.

LAN: Local access network. A network found inside a home or a single building.

malware: Malicious software that tries to do something bad to your computer, such as steal information or delete files.

MAC address: Media Access Control. A wireless hardware device's unique number that identifies it on a network.

MB: Megabytes.

Mb: Megabits.

Mbps: Megabits per second.

mini-PCI adapter: A wireless network adapter that can be installed in newer laptops that include a mini-PCI slot, freeing the laptop's PC card slot for other uses.

multimedia: One of many forms of media. Can include photos, video, and music.

network: A way to connect two or more computers.

network adapter card: A wireless device that allows a laptop, desktop, or handheld computer to connect to a Wi-Fi network. Also called a network interface card (NIC), a network adapter card transmits and receives data over the network.

network-attached storage (NAS): A NAS drive is a standalone device to store data and programs, which are accessible over a network.

network interface card: NIC. *See* network adapter card.

number portability: The ability to keep your current cell or landline phone number when you either switch carriers or move to a new residence.

OTA: Also, over-the-air. Receiving digital TV signals from local broadcast stations via an antenna.

PC Card: An adapter inserted into a laptop slot to allow the computer to receive and transmit Wi-Fi radio signals.

PCI adapter: An adapter card inserted inside a desktop computer to allow the computer to receive and transmit Wi-Fi radio signals.

PDA: Personal digital assistant.

peer-to-peer mode: *See* ad hoc mode.

peripheral: A device that connects to a computer.

phishing: A technique where someone sends you an e-mail pretending to be from your bank or other service. When you follow the instructions in the e-mail, you are giving your personal information to the bad guy, not the bank.

ping: A method of sending a packet to a computer to see if it's accessible.

Pre-Shared Key (PSK): An authentication method for wireless networks that relies on the computer and the access point having a secret that they both know.

QoS: Quality of Service. This refers to technology that can prioritize streaming media packets, so the audio or video stream is delivered without dropped video frames or lost audio.

range extender: A piece of wireless gear that acts as a repeater for wireless signals so that you can be farther from the access point.

RF: Radio frequency. Electromagnetic waves that operate on frequencies from about 3 kHz to 300 GHz. Every wireless device uses a frequency.

router: A device that sits between your Internet service provider and your network, routing Internet traffic to its proper destination.

satellite radio: Paid services that stream large numbers of radio channels from orbiting satellites to satellite-capable receivers. The service most common in the United States is Sirius XM Radio.

Service Set Identifier: An identifier that a Wi-Fi network uses to identify itself.

SmartWatch: A wristwatch produced by one of several manufacturers that can receive news and information using a wireless network. Created by Microsoft.

SMS: Short message service. A text service offered on phones using the GSM digital cellular telephone system. The messages are limited to 160 alphanumeric characters.

spyware: Software that captures information such as your keystrokes and Web browsing habits and sends them to someone else.

SSID: *See* Service Set Identifier.

streaming: The process of sending multimedia information between two or more computers.

TCP/IP: Transmission Control Protocol/Internet protocol. A suite of protocols for sending information over the Internet and local networks. Because everyone on the Internet speaks TCP/IP, your computer can talk to any other computer that allows it.

universal serial bus: USB. A standard for sending and receiving data between a computer and a peripheral device, such as a wireless access card. USB 1.1 moves data at up to 12 Mbps, while the newer version (2.0) can handle up to 480 Mbps.

USB: *See* universal serial bus.

virtual private network: A technology that permits secure communications between two points. A VPN tunnels through the public Internet, sending and receiving encrypted information.

virus: A piece of malware that replicates itself to spread, and usually attaches itself to another piece of software.

VPN: *See* virtual private network.

WAN: Wide-area network. In the larger sense, this refers to a network that connects different cities. Most routers label the port that connects to the Internet as the WAN.

WEP: *See* wired equivalent privacy.

WPA: *See* Wi-Fi protected access.

Wi-Fi: Wireless fidelity. Wi-Fi permits communications over the 2.4 and 5.0 GHz bands within a radius of up to 300 feet. Wi-Fi is used to create wireless networks and hotspots, allowing anyone with the proper wireless equipment to connect.

Wi-Fi protected access: WPA. A transition mechanism to fix problems in the WEP protocol until the full 802.11i specification could be implemented.

Wi-Fi protected access version 2: WPA2. The current generation of wireless privacy extensions, based on the IEEE 802.11i standards. WPA2 fixes problems with WPA and WEP that would let crackers get into your network.

Wi-Fi Protected Setup (WPS): A mechanism to automatically configure a wireless device to a supported access point.

wired equivalent privacy: WEP. The first encryption standard, vulnerable to hackers, for securing Wi-Fi networks. WPA2 is now supported by all manufacturers, so WEP should not be used anymore.

Windows Vista: Microsoft's latest operating system, which provides many built-in wireless networking functions.

wireless: Communications that use radio waves rather than wires.

zombie: A computer that has been infected with malware that causes that computer to operate as part of a botnet.

Index

Numerics

A

B

C

D

E

F

G

H

I

J

K

L

M

N

O

P

Q

R

S

T

U

V

W

X

Z

Notes

Notes

Declare your independence from wires! Here's what you need to make it happen

All types of personal electronics have wireless capacity these days — you just need to know how to take advantage of it. The minibooks in this handy guide help you choose the right networking hardware, configure printers for wireless access, synchronize your smartphone with your wireless network, plug security leaks, and even get into GPS!

- ***Yank the plug* — discover the hardware you'll need and consider the pros and cons of being "always on"**
- ***Plan the network* — decide what to include and make your shopping list**
- ***Configure* — learn how Windows facilitates wireless networking and how to create a bridge between wired and wireless**
- ***Feel secure* — get the rundown on wireless vulnerabilities and how to lock them down**
- ***Hit the road* — know how to preserve your laptop battery, watch TV from anywhere with SlingBox™, and use hotspots**
- ***Network everything* — explore cell phone services, cordless phones, FRS radio, Bluetooth®, and other technologies**
- ***Entertain* — expand with wireless home entertainment, streaming audio and video, and Amazon's eBook service**
- ***Find yourself* — get the scoop on wireless GPS units and what to do with them**

Open the book and find:

- **What you can do on a wireless network**
- **Tips for planning a network without going broke**
- **How to play music with a media server**
- **Internet threats and how to foil them**
- **Ways to balance your wants with your budget**
- **All about wireless cards**
- **Why you should consider a DSS phone**
- **Cool ways to use GPS**

Go to Dummies.com®
for videos, step-by-step examples, how-to articles, or to shop!

Sean Walberg manages the national network of a financial services company. **Loyd Case** is Editor for the ExtremeTech technology Web site. **Joel Durham Jr.** is a freelance writer and former tech editor of *PC Gamer* magazine. **Derek Torres** is a technical communicator, author, and Microsoft registered partner.

For Dummies®
A Branded Imprint of
WILEY

$34.99 US / $41.99 CN / £24.99 UK

ISBN 978-0-470-49013-6