DVD
VIDEO/AUDIO

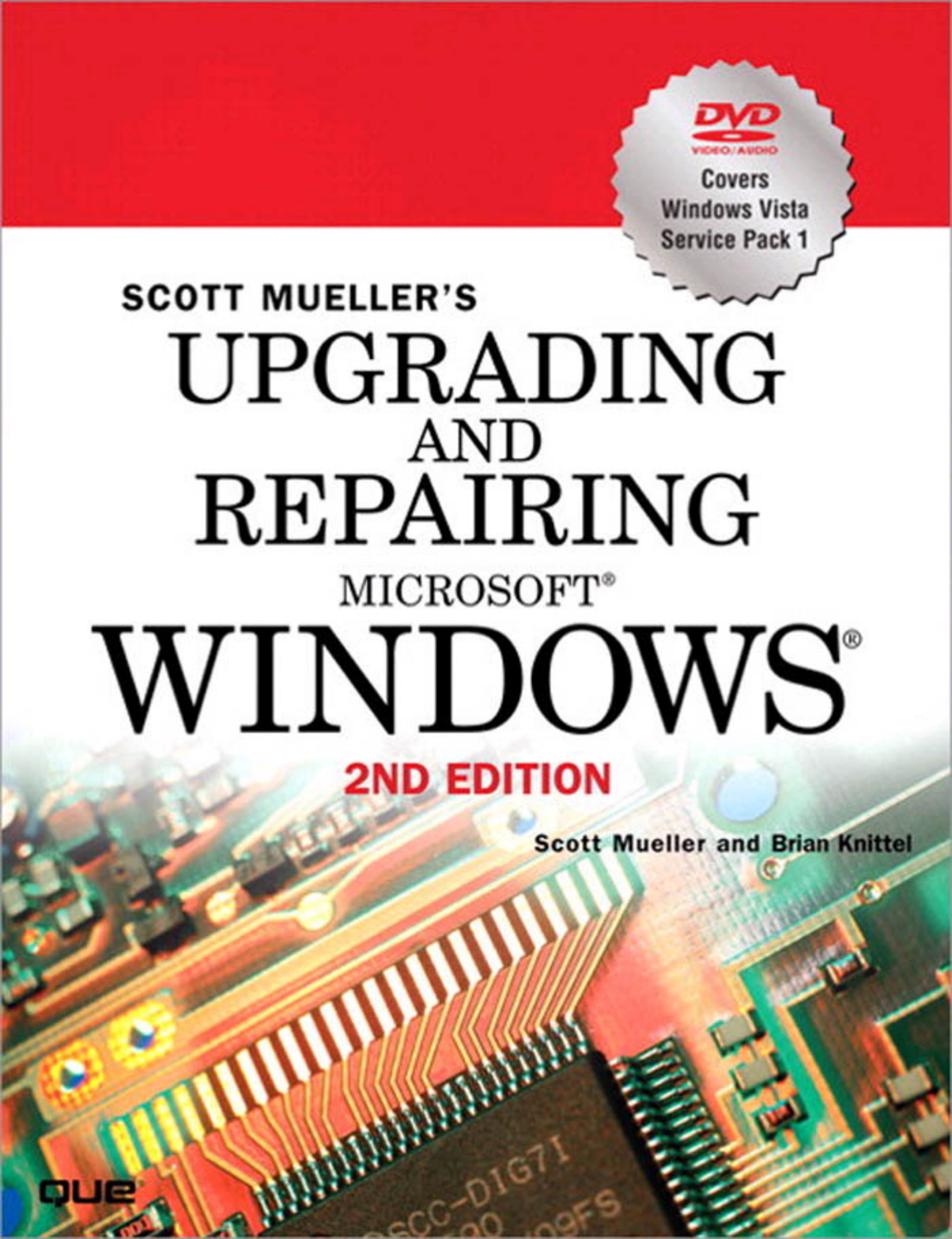
Covers
Windows Vista
Service Pack 1

SCOTT MUELLER'S

UPGRADING AND REPAIRING MICROSOFT® WINDOWS®

2ND EDITION

Scott Mueller and Brian Knittel



QUE®

Upgrading and Repairing Microsoft® Windows®, Second Edition

ISBN-13: 978-0-7897-3695-6
ISBN-10: 0-7897-3695-0

Library of Congress Cataloging-in-Publication Data
Mueller, Scott.
Upgrading and repairing Microsoft Windows / Scott Mueller, Brian Knittel. -- 2nd ed.
p. cm.
ISBN 978-0-7897-3695-6
1. Microsoft Windows (Computer file) 2. Operating systems (Computers) I. Knittel, Brian. II. Title.
QA76.76.O63M8444 2008
005.4'46--dc22

2008036253

Printed in the United States of America

First Printing: September 2008

Trademarks

Warning and Disclaimer

Bulk Sales

Que Publishing offers excellent discounts on this book when ordered in quantity for bulk purchases or special sales. For more information, please contact

U.S. Corporate and Government Sales
1-800-382-3419
corpsales@pearsontechgroup.com

For sales outside of the U.S., please contact

International Sales
international@pearson.com

Associate Publisher
Greg Wiegand

Acquisitions Editor
Rick Kughen

Development Editor
Todd Brakke

Managing Editor
Patrick Kanouse

Project Editor
Mandie Frank

Copy Editor
Margo Catts

Indexer
Ken Johnson

Proofreader
Mike Henry

Technical Editor
Mark Reddin

Publishing Coordinator
Cindy Teeters

Designer
Anne Jones

Introduction

Welcome to *Upgrading and Repairing Microsoft Windows, Second Edition*. This is the book for people who want to know more about how to use and support Microsoft Windows than most other books dare to detail. While covering all versions in many respects, this book devotes most coverage to Windows Vista and XP. Whether you want to install, manage, or troubleshoot the Windows operating system, this book goes far deeper than just the basics. Whether you support a large network of Windows machines, a few Windows PCs in a small office/home office environment, or just a single at-home system, this book can quickly turn you into an advanced Windows power user.

Is This Book for You?

Upgrading and Repairing Microsoft Windows, Second Edition is designed for people who want a thorough understanding of Windows and how it works without wasting time and pages on endless handholding through basic, everyday tasks. Each section fully explains management and troubleshooting issues related to Windows, including user management, networking, and security issues. Over the course of this book you'll develop a feel for what goes on behind the stylish graphical user interface so you can rely on your own judgment and observations and not some table of canned troubleshooting steps.

Upgrading and Repairing Microsoft Windows, Second Edition is written for people who will install, configure, maintain, and repair systems they use personally or in a corporate environment. To accomplish these tasks, you need a level of knowledge much higher than that of an average system user. You must know exactly which tool to use for a task and how to use the tool correctly. This book can help you achieve this level of knowledge.

Chapter-by-Chapter Breakdown

Chapter 1, "Windows Version History," examines the very beginnings of PC operating systems from DOS all the way through Windows XP and Vista, including the latest Service Packs. Microsoft operating systems have had quite a wild ride over the years and it's amazing to see how the operating system we all use almost every day has become what it is.

Chapter 2, "Windows Boot (Startup)," details the Windows startup process, including what takes place between power-up and the appearance of the Welcome screen. In addition, it includes detailed information about Windows services, which are processes that run in the background to provide support for Windows networking, searching, authentication, and management.

Chapter 3, "Installing Windows," explains procedures and issues regarding the preparation and installation of Windows. It includes detailed steps for baseline installations for single desktops as well as in a more complex networked environment.

Chapter 4, "Upgrading Windows," discusses how to upgrade Windows to a new version. You look at paths for upgrading existing systems to either Windows XP or Vista. Also shown are methods for migrating user settings and documents to new Windows computers.

Chapter 5, "Tweaking and Tuning Windows," shows you how to configure Windows for peak performance and usability, using the Windows configuration dialogs and special-purpose tools such as TweakUI and the Registry Editor. In addition, we'll give you a checklist you can use to identify and fix the most common Windows performance bottlenecks.

Chapter 6, "Networking Windows," tells you how to configure Windows to run a reliable and secure network at home or at the office. Whether you have two computers or two hundred, a network can immediately pay for itself—many times over—by letting you share printers, giving you access to files from any computer, and letting you share a single Internet connection among several computers.

Chapter 7, "Protecting and Securing Windows," covers the steps you can take to ensure your Windows PC is well protected from outside intrusion. Have you lost your administrator account password? Would you like some help protecting your computer from spyware and viruses? We'll help you learn how to recover lost passwords, use firewalls to block intruders, and protect your computer from viruses, spyware, and trojans. Learn how to take an active approach to security and harden your existing security to stop attacks before they start.

In Chapter 8, "Managing Windows," we cover the most important Windows management functions: adding and managing user accounts, hardware, device drivers, and hard disks. In addition, Chapter 8 gets down and dirty with Windows Backup, showing you how make essential backups of your precious data and how to restore those backups should the data on your hard drive be lost or corrupted.

In Chapter 9, "Windows Commands and Scripting," we cover Windows scripting essentials and the oft-forgotten-but-highly-useful world of the command prompt. The command prompt environment not only runs old MS-DOS programs, but also gives you access to a large number of efficient, concise, and powerful Windows management and operating tools. The chapter covers the general principles of command-line programs, configuration settings, and several important commands, as well as scripting and batch file procedures that you can use to automate complex jobs.

Chapter 10, "Windows File Systems," covers file systems. If you're currently running FAT32 drives and deciding whether to switch to NTFS, or if you just want to know everything there is to know about the file system, this is the place to look.

Chapter 11, "Windows Data Recovery," covers data recovery procedures. If you can't access your drive because of a corrupted master boot record (MBR) or volume boot record (VBR), you'll find information you can use to recover these sectors and regain access to your valuable data.

Chapter 12, "Windows Troubleshooting," looks at some of the more common problems encountered with Windows. Troubleshooting software is one part skill, one part craft, and one part knowing where to look for information. In this chapter, you'll look at how to identify Windows problems, and what tools and methods you should use to solve them. This chapter includes an extensive look at how to deal with a system that cannot stably boot, and how to use both the System Restore feature and the arcane but powerful XP Recovery Console and Vista Recovery Environment when you can't even log in to your user account.

This edition of *Upgrading and Repairing Windows* also includes online content that can be found at www.informit.com/title/9780789736956.

Appendix A, "Windows Tool Reference," describes several useful categories of Windows management, maintenance, configuration, monitoring, and data processing tools that you may not be familiar with. Most of them are not installed by Windows Setup but instead are hidden away in obscure folders on your Windows Setup CD-ROM. Several more are available from Microsoft via free download over the Internet, and some others must be purchased. In any case, we think you should know about all of them.

Appendix B, "Windows Command Reference," lists all the executable programs provided with Windows 9x/Me, NT/2000, and the various versions of XP and Vista, including application pro-

grams, services, system components, built-in commands, Control Panel applets, MMC Management snap-ins, and screen savers. You can browse this listing to find useful programs you might not be familiar with, or to help identify the many obscure programs that are run automatically by Windows.

Appendix C, "Remote Desktop and Remote Assistance," shows you how to set up the Windows Remote Desktop feature so that you can access your computer from anywhere in the world. It also includes information on third-party remote connection tools that offer alternatives to using Remote Desktop.

Getting the Most from This Book

Upgrading and Repairing Microsoft Windows, Second Edition is not a book that you read through once and never touch again. In fact, this is not a book that needs to be read straight through at all, although any Windows user will learn a great deal from doing just that.

This book is, in fact, a detailed and valuable reference that should be kept next to your PC (and your copy of the latest edition of *Upgrading and Repairing PCs*) at all times. The information shoehorned into every line of every page of this tome will help you put Windows to work the way it was meant to and keep it running for the long term.

Scott's Website—www.upgradingandrepairingpcs.com

Don't miss my book website at www.upgradingandrepairingpcs.com! Here, you'll find a cache of helpful material to go along with the book you're holding. I've loaded this site with tons of material, from video clips to monthly book updates. I use this spot to keep you updated throughout the year on major changes in both the PC hardware industry and the evolution of Windows. Each month, I write new articles covering new technologies released after this book was printed. These articles are archived so you can refer to them anytime.

You'll also find exclusive video clips available nowhere else!

I also use this site to tell you about some of the other fantastic *Upgrading and Repairing PCs* products, including

- *Upgrading and Repairing PCs*
- *Upgrading and Repairing PCs: Build a PC with Scott Mueller*
- *Upgrading and Repairing Laptops*
- *Upgrading and Repairing Servers*
- *Upgrading and Repairing Networks*

If you have technical questions, use my forum at http://forum.scottmueller.com. You can read the forum to see existing questions and answers, or sign up to post a question yourself.

Laptops have become the largest growing segment of PCs, and my new book *Upgrading and Repairing Laptops, 3rd Edition* covers these systems in great detail and is due out in spring 2008. Be sure to check the upgradingandrepairingpcs.com website for more information on all my latest books, videos, articles, and more!

Chapter

6

Networking Windows

Setting Up a Network

In this chapter, we're assuming that you are creating or adding to a network for a home or small office network, which in Microsoft's jargon is called a *workgroup network*. That said, much of this material still applies to corporate-style domain networks as well. There just isn't room in this book to cover every nuance of creating that type of network.

Windows has all the software you need already built in, but you *may* need to purchase some additional hardware components:

- An Ethernet (wired) or wireless network adapter for each computer. Virtually all new desktop and laptop computers have an Ethernet adapter built onto the motherboard, and many laptops have wireless networking built in as well, so you may not have to purchase these.
- For a wired network, an Ethernet switch or hub, or a cable/DSL sharing router with a built-in switch, and CAT-5 cables to run from each computer to the switch, as shown in Figure 6.1.
- For a wireless network, a wireless router or access point. This router or access point usually also has jacks for Ethernet connections so that wired connections can be made as well, if desired, as shown in Figure 6.2.

Here are the steps you'll want to follow:

- Get whatever extra hardware you need. The next section gives you a brief overview of the types of available hardware.
- Install your network adapters and cabling. I won't cover this part in detail in this book. (If you need more information on selecting and installing network hardware, refer to *Upgrading and Repairing Networks* or *Upgrading and Repairing PCs*, both published by Que.)
- If you are creating a wireless network, install your access point or wireless router according to the manufacturer's instructions.
- Set up Windows to use your network, as described under "Configuring a Workgroup Network," later in this chapter.

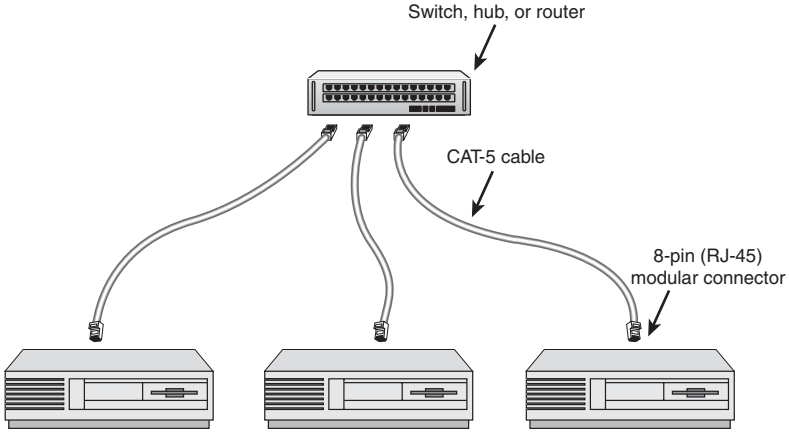


Figure 6.1 A basic wired Ethernet network, using CAT-5 cabling.

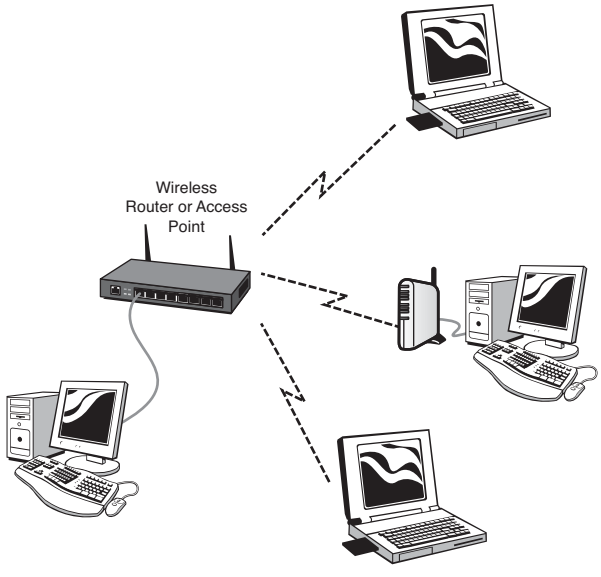


Figure 6.2 A wireless network with an access point or wireless Internet sharing router, and optional wired Ethernet connections.

If you're not already familiar with network hardware, the next section gives a quick overview of what's available. If you already have your hardware, skip ahead to "Wireless Networking" or if you're building a wired Ethernet network, "Configuring a Workgroup Network."

Network Hardware

Hardware for computer networking was once *very* expensive, but today networking hardware costs as little as $5 to $40 per computer. When you consider that a network can let you share a

single printer between two or more computers, or share a single high-speed Internet connection, a network can pay for itself the first day you set it up.

This section gives you a quick run-through of the various types of network hardware you can use to tie your computers together.

Wireless Versus Wired

A network lets your computers "talk" to each other. They can do this through wires or through radio signals, using one of the following types of networks:

- **Ethernet** uses a physical cable to connect the computers. Ethernet networking runs at either 10 million bits per second (Mbps), 100Mbps, or 1000Mbps (1Gbps). 100Mbps is the most common speed at present. (10Gbps Ethernet is coming, but it's not something the average home user needs to worry about yet.)
- **Wireless** or Wi-Fi networking sends data through radio signals over the air. Wireless networking doesn't require you to string cables between your computers, but it's less reliable (that is, it may stop working for a few seconds every once in a while, disrupting a long download or file transfer), and the signal sometimes has problems passing through walls and floors. Wireless networking comes in several flavors named after standards published by the International Association of Electrical and Electronics Engineers (IEEE). The wireless network types for home and small offices are named 802.11b, which runs at up to 11Mbps, 802.11g, which runs at up to 54Mbps, and 802.11n, which can run at up to 200Mbps or more and has better signal strength. "Up to" is the key phrase there. In real-world use, you'll get at most half of the rated maximum speed, and if signal quality is low, much less. Still, wireless speeds are fine for surfing the Internet, and if you have 802.11n, even big file transfers should perform well.

  Most current equipment is 802.11g. At the time this was written, the 802.11n standard was not yet finalized, although several manufacturers are presently selling "*pre-n*," that is, uncertified products that are *not* guaranteed to work well with products from other manufacturers. (They will presumably be upgradable via software when the final specification is made, but until the standard is finalized in late 2008, buy this stuff at your own risk.)

In addition to Ethernet and wireless, there are two lesser-used wired network types that don't require you to run new cables because they use your existing household wiring:

- **Powerline** networking sends data via radio signals sent through your electrical wiring, using adapters that plug into wall outlets. Powerline networking runs at 10Mbps, which is a bit slow by today's standards—it can take hours to back up a large hard disk over a 10Mbps connection. But it would be fine for sharing an Internet connection.
- **Phoneline** sends data via radio signals sent through your telephone wiring, using adapters that plug into telephone jacks. (All the jacks must be connected to the same telephone extension.) Phoneline networking also runs at relatively slow 10Mbps.

You can set up a network using any of these hardware types, and you can even mix and match the types if you want, using access points or devices called *bridges* to connect the different network types together. Wired Ethernet connections are the least expensive, the fastest, the easiest to set up, and the most reliable, but it can be annoying to have to run the cables around. So for example, you might use Ethernet connections to hook up several computers in close proximity, and then use a wireless access point or a powerline/Ethernet bridge to extend the network to a computer in another room.

Network Interface Adapters

Whatever type of network(s) you decide to use, you'll need a network interface adapter for each computer. Adapters come in several forms: internal (PCI) cards for desktop computers, PCMCIA cards for laptops, and USB adapters for either desktops or laptops. I'll briefly discuss each adapter type here:

- **Ethernet**—Typical internal adapters are PCI cards. These can cost as little as $5 each. USB and PCMCIA adapters are available for laptops at a slightly higher cost. Better yet, many desktops and most laptops have Ethernet built in already, so in most cases no add-on adapter is needed. Ethernet adapters are labeled "10/100Mbps" or "10/100/1000Mbps," meaning that they can run at any of the listed speeds, depending on the capability of the hub into which they're plugged.
- **Wireless**—There are some internal PCI adapters for desktops. Most are USB, for either desktops or laptops, or PCMCIA for laptops. Some manufacturers make PCI cards for desktops into which you plug a PCMCIA wireless network adapter. Many laptops have wireless built in, so no add-on adapter is needed. If you need to buy an adapter for a desktop, I recommend the USB variety because you can easily move these around to get the best signal reception.
- **Powerline**—Typically packaged as a box that plugs into a wall outlet and connects to your computer through a USB cable. Some adapters have Ethernet connectors instead, which you would connect to an Ethernet adapter in your computer, or to a hub.
- **Phoneline**—Typically internal (PCI) cards or external USB devices.

Cabling

If you are making a wired Ethernet network, you have to run a cable from each computer to the nearest hub (hubs are discussed in the next section). Ethernet cable is also called Unshielded Twisted Pair (UTP) cable because it looks like ordinary telephone cable, with four pairs of wire twisted together inside the cable's jacket. However, it's specially manufactured for computer use, and the electrical properties of the wire are very strictly controlled. UTP cable for networking use is rated according to the highest data speed that it's designed to carry, as listed in Table 6.1.

Table 6.1 Ethernet Cable Ratings

Ethernet Speed	Minimum Cable Rating
10MBps (10BASE-T)	CAT-3
100MBps (100BASE-T)	CAT-5
1000MBps (1000BASE-T)	CAT-5, but CAT-6 or CAT-5e is recommended

Even if you have only older, slower 10Mbps equipment, I recommend that you use at least CAT-5 cabling for all Ethernet networks.

Ethernet cables can't be cut and spliced in the normal way. If you need to connect cables from end to end, you *must* use CAT-5 certified plugs and jacks.

You can purchase premade CAT-5 cables (called *patch cables*) in varying lengths from computer stores or online. You can also purchase bulk cable, connectors, and a connector crimping tool and make your own, although that's beyond the scope of this book.

Be aware that the maximum length for Ethernet cabling is 100m (330 feet). If you have computers farther apart than this, you have to place the hub somewhere between them, or use multiple hubs in sequence, so that no single cable is more than 100m long. For a really long run, you may have to use fiber optic cable or wireless networking.

If your only goal is to connect two computers together with Ethernet, you can connect the two computers directly to each other, using a special cable called a *crossover cable*, which routes the send and receive data wires so that the cable can connect one Ethernet adapter directly to another. In most cases, however, you use regular Ethernet patch cables to connect each computer to a central hub or switch, as discussed in the next section.

Hubs and Switches

If you use a wired Ethernet network and have more than two computers or other devices, you need one or more switches or hubs. These devices route the signals between the computers. Hubs and switches serve the same purpose, so for the rest of this chapter, I'll just use the term *hub*. (See the sidebar "Switch? Hub? What's the Difference?" for an explanation of the two terms.)

A simple wired network was shown in Figure 6.1. If you have two or more groups of computers, separated by some distance, you can simplify your cabling job by using more than one hub, with just a single cable running between them, as shown in Figure 6.3.

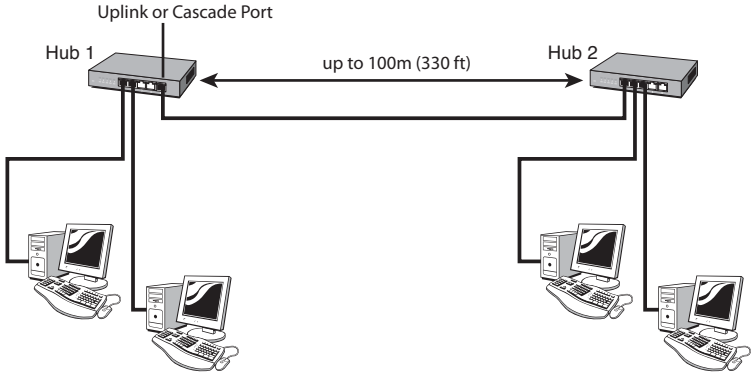


Figure 6.3 A more complex Ethernet network with more than one hub.

Hubs can generally adapt themselves to the various Ethernet speeds supported by the computers that you attach to them. Thus, they're marketed as "10/100Mbps" or "10/100/1000 Mbps." Most network adapters are rated 10/100, so these run at the higher 100Mbps speed when connected to a 10/100 hub. Higher-end desktops, some laptops, and most Macs usually have 10/100/1000Mbps adapters. If you have two or more computers with these high-speed (Gigabit) adapters, get a 10/100/1000 hub; otherwise, 10/100 is fine.

If you are going to be using wireless networking in addition to Ethernet, and/or you'll be sharing a DSL or cable Internet connection, you may not need to purchase a hub at all because most

wireless access points and DSL/cable sharing routers have a hub built in. Check for this before you spend the money on a standalone Ethernet hub.

Switch? Hub? What's the Difference?

The difference between a hub and a switch is subtle and almost irrelevant today. Here's the difference: Hubs are brainless devices. When a data packet arrives on any of its ports, it transmits the data back out on all its other ports. Thus, only one connected computer at a time can transmit data. A switch, on the other hand, has some processing power built in. It pays attention to the data that passes through it, and learns the physical network addresses of the computer(s) connected to each of its ports. When it receives a data packet addressed to a specific computer, it sends the packet out only through the port that leads to that computer. Thus, the other ports aren't clogged up with unnecessary data, and the switch can support several simultaneous independent "conversations" between its ports, each running at full speed.

Today, as I mentioned, the distinction is effectively irrelevant because the processing power and signal-handling circuits needed to build switches are available in a single, inexpensive silicon chip. As a result, there is no extra manufacturing cost involved, so nobody makes plain old hubs anymore. Today, all Ethernet hubs made are actually switches.

Wireless Access Points

Wireless networks function in one of two ways:

- In an *ad hoc* network, the computers that participate in the network communicate directly to each other through their antennas.
- In an *infrastructure* network, a device called an *access point* serves as a sort of referee. Each networked computer transfers data to the access point, which then relays it to the other computers. Access points also provide a means of connecting the wireless network to a wired Ethernet network so that wired-in computers can communicate with the wireless ones. Additionally, an access point makes it easy to connect a high-speed Internet connection to the network, where it can be shared by all the computers.

I don't discuss creating *ad hoc* networks in this chapter, but I do want to mention that Vista's Windows Meeting Space collaboration tool can automatically set up a temporary *ad hoc* wireless network to let a group of computers share files and applications during a meeting.

For the purpose of this book, I recommend that if you want to set up a wireless network for your home or office, you should set up an infrastructure network, by purchasing an 802.11g or 802.11n (or pre-n) access point that has both a wired Ethernet switch and Internet connection-sharing router capability built in.

Gateways and Routers

A *router* is a device that transmits data between two or more *separate* networks. Routers serve much the same function as post offices, which examine the mail they collect, deliver what they can, and forward the rest on to other post offices for *them* to deliver. A router doesn't get involved when data is being sent from one computer to another on the same network. But when data is intended for a computer on some other connected network, it's the router's job to forward the data from one network to another, to still others if need be, until it reaches its destination.

In corporate environments, routers are used to connect the local networks in separate offices or workgroups. In the home and small office, a router can connect your personal network to the Internet, which after all is nothing more than a bunch of networks just like yours, all connected together. (Tens of millions qualifies as a bunch, yes?) Routers that are specially designed to perform this Internet connection service are often called *Internet gateways*, or *connection-sharing routers*. Although routers intended for corporate use can cost thousands of dollars, home/small office connection-sharing routers can cost as little as $10, up to about $100 for models that include an 801.11n wireless network access point in the same unit. Connection-sharing routers have one 10Mbps or 10/100Mbps Ethernet socket that is used to connect to your DSL or cable modem. This is called the *WAN port*. (WAN stands for *Wide Area Network*.) Most sharing routers also include a 10/100 Ethernet switch (hub) for up to four wired Ethernet connections. These are labeled LAN ports. You can tack on additional switches or hubs if you need to connect more computers to the Internet.

Tip

If you have cable or DSL Internet service, I strongly recommend that you use a router (wired or wireless) to share the Internet connection with your network, rather than using Windows Internet Connection Sharing. These inexpensive ($10 to $40) devices simplify setup and provide increased security against hackers.

If you're setting up new DSL or cable Internet service, you may not even need to purchase a separate connection-sharing router. Your ISP may be able to give you a DSL or cable modem that has a sharing router built in.

The next section discusses wireless networking. If you're going to set up a standard, wired Ethernet network, you can skip ahead to "Configuring a Workgroup Network."

Wireless Networking

Wireless networking has become much faster, more reliable, and *much* less expensive year by year. At the time this book was written, 802.11g adapters cost about $40 per computer, less when on sale or with a rebate, and a wireless router costs about the same. The next generation of 802.11n (WiMax) equipment, when its specifications are finalized in late 2008, promise even faster speeds and greater range. The Multiple-Input Multiple-Output (MIMO) technology promises to extend the range of wireless networking from the current effective limit of about 100 feet indoors to considerably more.

If you do want to install a wireless network, you need to know that security risks are involved:

- If you don't enable wireless security, any passerby can connect to your network.
- If you use the old WEP encryption option, a motivated passerby can still easily connect.
- With Windows Simple File Sharing enabled on XP, or Password Protected Sharing disabled on Vista, anyone who is able to connect can read or modify your shared files. (Simple File Sharing is discussed later in this chapter.)
- Even without Simple File Sharing, anyone who connects could send spam or viruses from *your* Internet connection.

So, wireless security is important, but fortunately, it's not that difficult to manage.

Note

This section tells how to configure wireless networking for Windows Vista and Windows XP Service Pack 2 or later in a home or small office. If you are using an earlier version of Windows, consult the manual provided with your hardware for setup instructions.

Caution

If you want to set up an "open" wireless hotspot to freely share your Internet connection with friends, neighbors, customers, or the world, that's great, but you must not use file and printer sharing on the same network. If you use a wireless network for your own file sharing, configure your network with wireless security (preferably WPA) enabled, and then plug into it a second wireless router, set with a different SSID and a different channel, and disable wireless security only on that second network.

Wireless Network Basics

Wireless networking (Wi-Fi) transmits data on the same 2.2GHz radio frequency band used by wireless telephones, microwave ovens, and other consumer products. Many people are familiar with using Wi-Fi to connect to the Internet at airports, cafes, hotels, and the like. You can also use it, rather than cabled Ethernet networking, to connect your computers at home or the office. Wi-Fi has become common enough that in most urban and suburban neighborhoods you'll probably find that your computer can pick up three or four networks operated by your neighbors. To be able to distinguish your network's signal from other peoples', and to secure your network, you must make four choices when you set it up:

- A SSID (Service Set Identifier), a short name that you give your network, up to 32 characters in length. This could be your last name, company name, a pet's name, or whatever makes sense to you.
- An encryption type, which consists of a choice of protocol, and "strength" of the code used to secure the network against eavesdropping. The choices, in order of increasing security, are none, WEP 40-bit (also called 64-bit), WEP 128-bit (also called 104-bit), WPA, and finally WPA2, which is the most secure as of the time this was written. I'll discuss encryption schemes in more detail shortly.
- An encryption key, which is a string of hexadecimal digits—that is, the numbers 0 through 9 and the letters A through F. Some wireless networking software lets you generate a key from an ordinary text password, but this method may not work when you use equipment from different manufacturers.
- A channel, which selects the frequency used to transmit your network's data. In the U.S., this is a number between 1 and 11; the numbers may be different in other countries. The channel is set by your wireless access point. In the U.S., the most common channels used are 1, 6, and 11. Change the channel from its default setting only if you find that several other networks in your area use the same channel; if in doubt, try channel 6.
- MAC-level security, which lets you specify which network adapters can connect to your router. MAC-level security is cumbersome to set up and does nothing to repel a really determined hacker, so I won't discuss it further.

Wireless Network Security

When you are using a traditional, hard-wired network, your data is fairly safe from prying eyes because the signal is contained with the wires, and someone would have to physically connect to your wiring to steal information or freeload on your Internet connection. (Of course, if corporate spies or government agencies get involved, all bets are off.) Wireless networks, on the other hand, broadcast information over a range of at least hundred feet and up to hundreds of yards, and anyone passing with a computer could receive those signals.

To let you limit others' ability to read your data and use your network bandwidth, wireless networking manufacturers have come up with schemes to encrypt (scramble) the data sent on the wireless signal so that only someone possessing a secret code (key) can connect to, send, and read data from the network. The first such scheme was named Wired Equivalent Privacy, or WEP, but this name turned out to be just a bit overoptimistic—WEP security can be broken in just a few hours with a single computer and some freely available software. WEP was strengthened by extending the length of the secret key from 40 to 128 binary bits, but because of its design flaws, this didn't help all that much. The networking industry devised a new encryption protocol called Wi-Fi Protected Access, or WPA, which is *much* more secure than WPA, and the latest, new-and-improved security scheme is called WPA2, for WPA version 2. WPA and WPA2 are very secure as long as you choose a truly random key, as we'll discuss shortly.

Do you really have to worry about your network being broken into? *Maybe* not, but you can't really tell because the "enemy" is most likely someone you don't know and will never see. And although someone might "just" be after a free Internet connection, someone who'd deliberately break into your network could very well want to do things that could get *you* in hot water if the activity is traced back to your Internet connection: send spam, share copyrighted music and video, purchase items with stolen credit card numbers, exchange illegal pornography, communicate with terrorists, commit espionage, or who knows what? So you really do need to at least try to make this difficult; with luck anyone trying to tap into your network will move on to look for an easier target. (It's like locking your front door. Intruders can still break a window to get in, but you at least have to force them to break the window.)

The problem with wireless security is that the same scheme has to be used by all access points and computers on the network. If even one of your devices doesn't support WPA2 or WPA, you're stuck using the relatively insecure WEP. If your access point or router doesn't support WPA2 or WPA, you may be able to install updated firmware to get it—visit the manufacturer's website to check. Furthermore, if you have an older version of Windows on your network, you might have to settle for WEP. Here is a list of the various schemes supported by different versions of Windows:

- **Vista** (all versions)—Has built-in support for WPA2, WPA, and WEP.
- **XP Service Pack 3**—Has built-in support for WPA2, WPA, and WEP.
- **XP Service Pack 2**—Has built-in support for WPA, and WEP. You can add WPA2 support with a hotfix. Visit support.microsoft.com and search for KB893357.
- **Earlier versions of Windows**—Previous versions of Windows (Windows Me, 9x, 2000, and XP without SP2) support WEP, but not WPA. The manufacturer of your computer's wireless network adapter *may* be able to provide an updated driver that includes WPA support.

Select the best security method supported by *all* your network gear, including any access points or routers. For example, if your access point and all computers support WPA2, use WPA2. Otherwise, if all support WPA, use WPA. Use WEP only if you have one or more devices that can't manage WPA. And be sure to use a truly random key when you set up the network.

Creating a Random Encryption Key

In actual use, a key is a string of binary ones and zeroes, ranging from 40 to 256 bits or more in length, looking like this: 1100101000111010110101010001110101001010. That's just 40 bits, and you can imagine how hard it would be to type something like this correctly into a router and several computers. Usually, then, keys are expressed in the shorter hexadecimal notation, where each group of four bits is represented by the digits 0 through 9 and the letters A through F. The same 40-bit key in "hex" looks like this: CA3AD51D4A, which is much more manageable. A 128-bit WEP key* takes 26 hex characters, like this: 9552DCF6069263823BFFA19957.

Even this shorthand form of the key can be tedious and difficult to type correctly, so most wireless equipment manufacturers—and Windows itself—let you enter a key using a *passphrase* instead. A passphrase is a word or short phrase that the software converts into numbers, which it scrambles and from which it then extracts the necessary bits for the key. For WPA, which uses 256 bits for the key, most devices and drivers require a passphrase—there usually isn't even the option of specifying the key as 64 hex characters.

On the surface, passphrases appear to make things easier but they can actually introduce some serious problems. With WEP, not every device driver or access point uses the same mathematical scheme to derive the key. The same passphrase typed into Windows and into your access point could produce a different set of bits, and if that happened, your wireless connection would not work. WPA doesn't have this particular problem because the formula for turning the passphrase into a key is part of the standard, but it shares another problem with WEP: Any wireless encryption scheme can be broken if the intruder can guess your passphrase. Freely available WEP- and WPA-attacking software comes with a huge list of names, numbers, and words to try. If your passphrase is in the attacker's dictionary, he can connect in just a few minutes.

So although it's tempting to use your pet's name or your house number as a passphrase, to make a really secure network, you need to create a truly random key. This means that if you're using WPA or WPA2, you should create a 63-character random text string. If you *have* to use WEP, create a 26-digit random hex number. Save this random key in a text file, and use it to copy and paste the key into each of your computers and your router's setup screen. This is a bit more work than typing just "fluffy," but it's necessary if you want your network to be protected against intrusion.

**The WEP protocol automatically adds 24 bits to the key you specify. For 128-bit security, you are asked to specify only 104 bits of key, thus only 26 hex characters. Similarly, 64-bit WEP requires only 40 bits, or 10 hex characters for its key.*

The Wireless Network Setup Wizard provided with Windows XP and Vista can generate and install a truly random key for you. We discus this wizard in the next section. You can also create a randomly key manually, using these steps:

1. If you're using WPA, visit www.grc.com/passwords.htm and press the F5 key to refresh the web page. Under 63 Random Alpha-Numeric Characters, select all the text in the box, right-click, and select Copy. (You're best off using all 63 characters in this key, but you could shorten it and still have pretty decent security. Just don't use fewer than about 20 characters or so.)

   If you're using WEP, visit www.andrewscompanies.com/tools/wep.asp. Click on the Generate 128-bit Key button. Under Generated Key, select the text in the Hex box, right-click, and select Copy.
2. Click Start, [All] Programs, Accessories, Notepad. Click Edit, Paste.
3. Click File, Save As, and save the file with the name `Wireless key` in your [My] Documents folder, or better yet, to a removable USB drive, so that you can carry it around to your other computers.
4. Print this file and keep the hard copy in a safe place.

Now you can copy and paste in this key when Windows asks you for your wireless key. When you're configuring your wireless router or access point, paste this key into the device's configuration software or web page.

Setting Up a Wireless Network Access Point

When you set up a wireless router or access point, you are setting up what is called an *infrastructure network*. Before you start, you should read the previous three sections: "Wireless Network Basics," "Wireless Network Security," and "Creating a Random Encryption Key," which go over the choices you'll have to make along the way.

Note

You may see web pages that tell you to have your access point hide (not broadcast) its SSID for increased security, but this is useless advice. Cracking programs can determine your SSID whether it's broadcast or not.

There are three main ways to set up a new wireless router in your home or office:

- Use a special setup or "wizard" program provided by the manufacturer.
- Set up the access point manually, following the manufacturer's instructions.
- Use the Wireless Network Setup Wizard provided with Windows XP and Vista.

I'd suggest that you read the manual that comes with your router to see whether it comes with its own setup program. If it does, and if its instructions make sense and seem easier than what follows in this section, by all means use it and see whether it works. If you elect not to use it, try the Wireless Network Setup Wizard, described in the next section. As a last resort, configure the router manually, as described later in this chapter.

Using the Wireless Network Setup Wizard

The easiest way to set up a wireless network is to use the built-in wizards provided with Windows XP and Vista. These tools not only help you generate a truly secure, random key, they may also be able to automatically configure your wireless router or access point.

Tip

If your wireless router supports Microsoft's Windows Connect Now (Rally) technology, Windows can set up the router automatically, saving you a lot of time and trouble. Some routers have a USB port for this purpose, and others can do it through the network. So, before you start, if you can, connect your computer's Ethernet adapter to the wireless router using a CAT-5 patch cable. This gives the wizard the best chance of successfully configuring the router without you having to lift a finger. If your router has a USB port on it, you may also want to have a USB flash drive on hand, in case you need it later in this procedure.

Because the details vary greatly, I describe the XP and Vista wizards separately.

Windows Vista

If at least one of your computers has Windows Vista, use Vista to set up your wireless network, and then add the XP computer(s) later. To run the Vista wizard, follow these steps:

1. Click Start, Control Panel. Select Network and Internet, and then under Network and Sharing Center, select Connect To a Network.
2. Select Set Up a Connection or Network. Select Set Up a Wireless Router or Access Point, and then click Next.
3. Click Next and confirm the User Account Control prompt.
4. If you are asked `Do you want to turn on network discovery for all public networks?` click No, Make the Network I Am Connected to a Private Network.
5. If Windows can connect to and can configure the router directly through the network, it offers to do so. Select that option and follow the wizard's prompts to complete the setup procedure.

   If Windows can't directly control the router, it offers two other choices: Configure This Device Manually, or Create Wireless Network Settings and Save to USB Flash Drive. Even if your router doesn't have a USB flash drive port, select the Create option.
6. Enter the name (SSID) you selected for your network and click Next.
7. If *all* your computers and other wireless devices support WPA encryption, accept the proposed random passphrase and click Next.

   If *any* of your computers or other wireless devices doesn't support WPA (your TiVo, for instance), you must use WEP encryption. Click Show Advanced Network Security Options, and select WEP. A random WEP key is generated. Click Next to proceed.
8. If you have already set up file and printer sharing, select Keep the Custom Settings I Currently Have and click Next. You can also make one of the following selections here:
   - **Do Not Allow File and Printer Sharing**—Prevents other computers from accessing files and printers shared by your computer.

- **Allow Sharing with Anyone with a User Account and Password for This Computer**—Enables File and Printer Sharing by your computer, using Password Protected Sharing.
- **Allow Sharing with Anyone on the Same Network as This Computer**—Enables File and Printer Sharing by your computer, with Password Protected Sharing turned off.

Password Protected Sharing is described later in this chapter under "Simple File Sharing" (p. 356). Make the desired selection and click Next.

9. Plug a removable (USB) flash drive into your computer if you haven't done so already, and wait for it to be recognized. If a `What do you want to do with the contents of this drive?` prompt appears, or if an Explorer window opens, close it. Then, in the Wireless Wizard, select the drive under Save Settings To, and click Next. This copies a file containing wireless setup information and a setup program that can install these settings on Windows on XP and Vista. We talk more about this in a moment.
10. When the copying process is complete, click Print Network Settings to make a hard copy of the setup information. You many need this to configure your router, and you also need it as a backup of your network setup information. (Be sure to keep it in a safe place.) Click Next.
11. Windows prompts you to configure your access point and other computers. Windows might be able to configure your router directly over its Ethernet connection, if you made that connection as suggested in the earlier Tip. If it can't do that, and if your router has a USB slot, plug the flash drive that was prepared in step 9 into your router. Within 30 seconds, the router should blink its lights three times. This indicates that its wireless security settings have been configured. (Its Internet connection haven't been configured or changed, however, so you have to take care of that part separately.)

    If your router doesn't have a USB port, you have to configure it manually as described later in this section.

After the router is configured, you can take the USB flash drive to your other Vista and XP computers to configure them. Simply log on using a Computer Administrator–type account, and plug in the flash drive. This should run the setup program that the wizard put on the drive. You don't need to use the instructions in the next section to set up your XP computers—the setup program on the flash drive takes care of XP as well as Vista computers.

When all your other computers have been set up, if you want, you can bring the flash drive back to the original Vista computer and have the setup wizard erase the security information from the flash drive. This is up to you. You can always configure other computers manually by using the Network Settings printout you made in step 10. Finally, if you are using your wireless router to share a high-speed Internet connection, open the router's setup web pages and set up your Internet connection. I'll give a brief outline of this process later in this section under "Configuring a Wireless Router Manually."

Windows XP

If you don't have any Windows Vista computers, you can set up a new wireless network by using the Wireless Network Setup wizard provided with Windows XP, following these steps:

1. Start by logging on to a Computer Administrator account. Open My Network Places from the Start menu. In the Network Tasks list, select Set Up a Wireless Network for a Home or Small Office. When the wizard appears, select Set Up a New Wireless Network.
2. In the first screen, enter a name for your wireless network, select Automatically Assign a Network Key, and indicate that you want Windows to create a random key for you. Also, if *all* your wireless equipment supports WPA encryption, check the Use WPA box at the bottom of the screen. Then click Next, and Next again to proceed.
3. If you have a USB flash memory drive, or a USB-connected digital camera memory card reader that presents the memory cards as disk drives, select Use a USB Flash Drive. (You can also use a floppy disk, if you want, with this setting.) Alternately, you can also choose to copy the wireless settings manually. Make your selection and click Next.
4. If you chose to use the USB device, Windows asks you to insert the device. Plug it in and wait a moment. If Windows displays a What Do You Want to Do with This Drive dialog, or if an Explorer appears, close it. Then, select the corresponding drive letter. (You can also select your floppy drive here.) Click Next and Windows copies the necessary files.

   After Windows copies the files, remove the flash drive and take it to your router and/or other computers to configure them. If your router has a USB port, plug in the flash drive. Within 30 seconds the router should flash its lights three times to indicate that its wireless security settings have been configured. (Its Internet connection isn't configured or changed by this process, however, so you have to take care of that part separately.) If your router doesn't have a USB port, you'll configure it manually in a later step.
5. Configure your other Windows XP and Windows 9x computers:
   - If you're using a USB device, plug the device into the computer. The Wireless Network Setup Wizard should run automatically and add the computer to the wireless network.
   - If you're using a floppy disk, insert the disk in each computer, and use My Computer or Windows Explorer to locate and double-click the `SetupSNK.EXE` file. This adds the computer to the wireless network.
   - To add computers manually, wait until after the next step when you have a printout of the network settings. I discuss the manual procedure later under "Joining a Wireless Network."
6. Return to the original Windows XP computer, reinsert the flash drive, and Click Next in the Wireless Network Setup Wizard. Then click Print Network Settings to get a copy of the settings. This opens a window in Notepad. Click File, Print to get a hard copy. You definitely want to have this as a backup, and it will help you to configure your router if you have to configure it manually. Finally, click Finish.
7. If you have to configure your router manually, follow the instructions provided by the router's manufacturer and use the information on the printout you just made. The manual setup procedure is roughly outlined in the next section, "Configuring a Wireless Router Manually."

If you later need to add more computers to the network, you can rerun the wizard on the computer you started with, and it will walk you through the process of reinstalling the setup software on your USB drive, or reprinting the instruction sheet. Or, you can follow the procedure in the next section to join them to the network manually.

After all your computers have joined the wireless network, skip the next section and continue with "Configuring a Workgroup Network."

Configuring a Wireless Router Manually

If your router can't be configured automatically through the network or a USB flash drive, you have to configure it manually. The details, of course, vary from one manufacturer to another, so you have to read the instructions for your particular device. The manual procedure goes something like this:

1. Connect one of your computers to the access point's Ethernet port, using a CAT-5 patch cable, and power up the access point.
2. Note the IP address that is assigned to your computer's Ethernet adapter. To find this, view the Network Connections folder. (On XP, get there from Control Panel. On Vista, open the Network and Sharing Center and select Manage Network Connections.) Right-click Local Area Connection, and select Status. Click Details, and note your [IPv4] IP address. This will be something like 192.168.1.23.
3. Open Internet Explorer, and in the Address bar type your IP address, but change the last number to 1. In this example, I'd type 192.168.1.1. Then, press Enter.
4. You should be prompted to enter a username and password. The default name and password are described in your router's manual.
5. Set up the router's Internet connection. For cable Internet, you typically select the DHCP (automatic) option, and for DSL, you usually need to select the PPPoE option, requiring a username and password, but this varies from one ISP to another. Your ISP will have provided you with this setup information, and most are willing to talk you through setting up your wireless access point if you call the customer support line.

Note

You usually have to click OK or Save Changes after making a change on any of the router's setup pages, before you proceed to another page.

6. Select the Wireless Networking setup page and enter your chosen network name (SSID). Select WPA or WEP security. If there is a "key index" selection, select 1. In the box for the first key value, paste in the hexadecimal key you generated in the previous section.

This is *usually* all you have to do to get an access point up and running. After you have saved the last set of changes, you may need to restart your router. As soon as it's restarted, you should be able to disconnect the Ethernet cable and connect wirelessly.

Joining a Wireless Network

When your home or small office wireless network has been configured and you're ready to start using your computer(s), or, if you are taking your computer into someone's work or home and want to use the wireless network there, you have to take some steps to be able to use the network. You can use the Wireless Network Setup Wizard discussed in the previous section, or you can connect to and use the network by following this manual procedure. (The figures here show the Windows XP versions. The dialogs are slightly different on Vista, but the procedure is the same.)

1. In the notification area at the bottom corner of your screen, locate the Wireless Connection icon (shown here to the left). Double-click it.
2. Windows displays a list of the names (SSIDs) of the wireless networks that it "hears," as shown in Figure 6.4. Click on the network you want to use and click Connect.

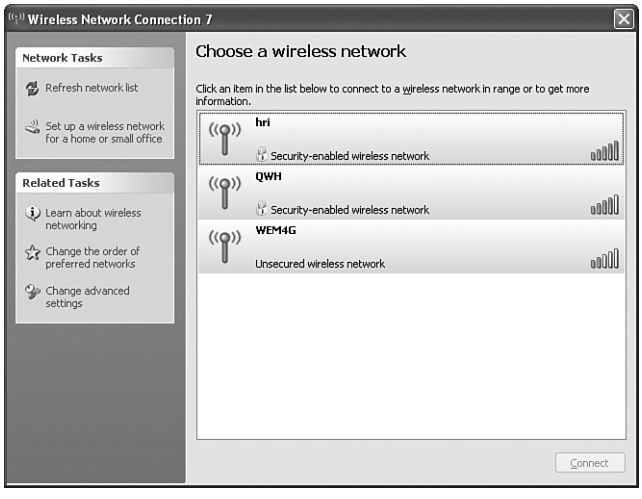


Figure 6.4 Windows displays the names of the networks whose signals it can receive.

Note

If the network you want to use doesn't appear, it could be because the signal is too weak. Also, some people prevent their routers from broadcasting SSID names over the airwaves. (This doesn't really provide much extra security; hackers can find the network anyway.) If the network you want to use isn't broadcasting its SSID, you have to enter the information manually.

3. Windows determines what type of security the network is using, and if the network is encrypted, prompts you to enter the network key. If the network uses WPA security, enter the passphrase, which is a string of letters, numbers, and/or punctuation. Be sure to enter it *exactly* as given to you. If the network uses WEP security, enter the 10- or 26-hex digit key.

Note

If you are using a wireless connection on a corporate network, your wireless configuration can and should be managed by your network administrators. Most likely, your administrator has installed a security "certificate" file that identifies your computer as one authorized to use the wireless network. And it's also likely that you won't have to configure any manual settings to use the network.

On Vista, you are asked whether the network is public or private. Take care answering this question! If you are in a public Wi-Fi hotspot such as a library, café, or business center, or even a client's office perhaps, select Public. File and printer sharing are disabled so that other computers on the network can't probe and possibly infect your computer with viruses. Select Private only if the wireless network was secured with a password or key, and you are sure that all the other computers on the network can be trusted.

After the wireless connections are made, you can continue setting up the rest of your network, as described in the following section.

Note

Microsoft has some experimental software available (for XP only) that lets you connect to more than one wireless network at the same time. If this sounds interesting, check out http://research.microsoft.com/netres/projects/virtualwifi/. No promises that it will work, but if you like to play around at the bleeding edge of technology, it's worth checking out.

Configuring a Workgroup Network

After your network hardware has been installed, whether it's wired or wireless, the next step is to make sure that Windows' networking software is set up correctly. This procedure is different for XP and Vista, so I'll go through the steps for each operating system separately. If you have both XP and Vista computers on your network, they'll work together just fine, as long as you set up both types using the following instructions. I cover XP first, then Vista.

After you've set up basic networking, you may want to make some optional settings. So after covering initial setup for XP and Vista, the remainder of this section covers the following topics:

- IP addressing options
- Networking with Windows 9x and Me
- Designating a master browser
- Providing a shared Internet connection

You may want to review all these topics before starting to set up your network.

Setting Up a Network on XP

Windows XP comes with a Networking Setup Wizard program that can automatically configure file sharing and Internet access for each of the computers on your network. The wizard lets you make a few basic choices, but otherwise takes care of all the technical details for you. You have to run this wizard at least once, whether you want to or not. For security reasons, Windows doesn't enable file and printer sharing until this wizard has been run at least once.

Note

If you're going to use Microsoft's Internet Connection Sharing to share an Internet connection over your LAN, configure the computer that will be sharing its Internet connection first. Establish and test its Internet connection, and only then configure the other computers. Internet Connection Sharing is discussed later in this chapter.

To start the wizard on XP, click Start, Control Panel, Network and Internet Connections, and Set Up or Change Your Home or Small Office Network. Read the "Checklist for Creating a Network" if you want, and then click Next. Follow the wizard through the following steps.

Select a Connection Method

The wizard asks you to select a statement that best describes your computer. The choices can be confusing, so consider them each carefully. They are

- **This Computer Connects Directly to the Internet. The Other Computers...Connect...Through This Computer**—Choose this if you want this computer to share its Internet connection with the rest of your LAN using Windows Internet Connection Sharing, which is discussed later in the chapter. *This* computer will connect to the Internet through a dial-up modem or a cable/DSL modem. In the latter case, you'll need two network adapters in this computer: one for the LAN connection and one to connect to the DSL or cable modem. In any case, be sure that you've already configured and tested your Internet connection before setting up the LAN.
- **This Computer Connects to the Internet Through Another Computer on My Network or Through a Residential Gateway**—Choose this if your network has a hardware Internet connection-sharing router, or if you've set up some *other* computer to share its connection with Internet Connection Sharing.

  Also, use this choice if your LAN has routed Internet service, such as that provided by a DSL, cable, ISDN, or Frame Relay router connected to your network hub, *and* the router for that service has been configured to filter out Windows networking traffic, which we'll discuss later in this chapter.

To get to the next three options, click Other. These alternatives are as follows:

- **This Computer Connects to the Internet Directly or Through a Network Hub. Other Computers on My Network Also Connect [this way]**—Select this if your computer uses its own dial-up or direct DSL/cable Internet connection, but you do *not* want to use Windows's Internet Connection Sharing to share the connection with the rest of your LAN.

  Also, use this selection if you use "multiple-computer" cable Internet service with no router. (I strongly urge you not to use this sort of connection—please read "Providing Shared Internet Access" later in this chapter for important warnings.)
- **This Computer Connects Directly to the Internet. I Do Not Have a Network Yet**—You would use this choice if you had a direct Internet connection (that is, a cable or DSL modem that uses a network adapter), but no LAN. Because you're setting up a LAN, this choice probably isn't appropriate.

  You *do* want to use this choice if you are setting up a network *only* to use a shared Internet connection, and don't want to share files with other computers. This might be the case if you are sharing an Internet connection in an apartment building or other public space, for instance. In this case, this choice indicates that you consider your network to be as untrustworthy as the Internet itself.

- **This Computer Belongs to a Network That Does Not Have an Internet Connection**—Select this if your computer will connect to the Internet using dial-up networking or AOL, or if your computer will never connect to the Internet.

Make the appropriate selection and click Next.

Select Your Internet Connection

If you chose one of the "This computer is directly connected to the Internet" choices, Windows presents a list of options for making that connection, listing your network adapters and your configured dial-up connections. Choose the connection that is used to reach the Internet and click Next. If you use a dial-up or PPPoE connection (frequently used with DSL service), choose the appropriate dial-up connection. Otherwise choose the network adapter that connects to your broadband modem.

Give This Computer a Description and Name

Enter a brief description of the computer (such as its location or primary user) and a name for the computer. Choose a name using just letters and/or numbers with no spaces or punctuation. Each computer on your LAN must have a different name.

If you're hard pressed to come up with names, try the names of gemstones, composers, Impressionist painters, or even *Star Wars* characters, as long as Mr. Lucas' lawyers don't hear about it. I use the names of islands in the Indonesian archipelago—with more than 25,000 to choose from there's little chance of running out of unique names!

Some Internet service providers, especially cable providers, require you use a name that they provide. (If you have a hardware connection-sharing device hooked up to your cable modem, enter that name into the hardware device and use any names you want on your LAN.)

Name Your Network

Choose a name for your network workgroup. This name is used to identify which computers should appear in your list of network choices later on. All computers on your LAN should have the same workgroup name. The wizard puts MSHOME into the name field, but I strongly suggest that you change it to WORKGROUP, which is the default on both earlier and later versions of Windows.

Caution

If you run the wizard again, it tries to change your workgroup name back to MSHOME. Be sure to change it back to WORKGROUP.

Also: The workgroup name *must* be different from all the computer names.

File and Printer Sharing

The wizard asks whether you want turn file and printer sharing on or off. Select Turn On File and Printer Sharing unless your network will contain computers that you don't trust; that is, computers in a public area, computers on a public wireless network, computers whose users you don't know, and so on. (If you later change your mind, or move your computer from one network to

another, you can turn file sharing on or off using the Exceptions tab on the Windows Firewall control panel.)

Ready to Apply Network Settings

The wizard lets you review your selections. Click Next to proceed.

You're Almost Finished…

You need to run the wizard on all the computers on your LAN at least once. If all the computers use Windows XP, select Just Finish the Wizard, and then run the wizard on each of your other computers. If you have computers running versions of Windows 95, 98, Me, NT, or 2000, you can create a disk that lets you run the wizard on these older machines, or you can use your Windows XP CD-ROM on these computers.

To use a disk, choose Create a Network Setup Disk, and insert a blank, formatted floppy disk. If you ran the wizard earlier and just changed some of the settings, choose Use the Network Setup Disk I Already Have, and reinsert the setup disk you created earlier. Otherwise, choose Just Finish the Wizard; I Don't Need to Run the Wizard on Other Computers.

Caution

Don't use this network setup disk on computers running Windows Vista.

Note

If you need to adjust the computer or workgroup name later, log on as a Computer Administrator, right-click My Computer, select Properties, and view the Computer Name tab. You can use a name-assignment wizard by clicking Network ID, or you can enter the information manually by clicking Change.

Now, continue with the next section to review the IP addressing choices made on your network, as discussed in the section titled "IP Addressing Options."

Setting Up a Network on Vista

Surprisingly, Windows Vista does not have a network setup wizard to walk you through setting up file sharing for a home or small office network. If you've just set up a wireless network, the procedure I described earlier under "Wireless Networking" took care of the wireless connection itself. But, after the wireless connection is set up, or if you've just installed a wired Ethernet or HomePNA (phoneline) network, you have to check or change a few other settings before you can share files and printers on your new network.

If your network is going to be used only to share an Internet connection, you don't need to perform these steps. But, if you do want to share files and/or printers among the computers on your network, you must check the following settings:

- Ensure that each computer has the same workgroup name.
- Enable file and printer sharing.
- If you use a third-party firewall product, permit file and printer sharing data to pass through the firewall.

I take you through these steps in detail in the following sections.

Each computer on the network must have a unique computer name. In addition, each computer has a workgroup name that should be the same on each of your computers. I recommend that you use WORKGROUP as the workgroup name—yes, it's unimaginative, but most Windows computers come with this name preset, so we'll go with it.

To check the workgroup name on your Vista computers, click Start, right-click Computer, and select Properties. The workgroup name is shown under the heading Computer Name, Domain and Workgroup Settings. If any computer has a different workgroup name, click the Change Settings button and approve the User Account Control prompt. When the System Properties dialog appears, click Change and type WORKGROUP under the Workgroup button. Click OK, and then let Windows restart.

Tip

If your network has computers running other versions of Windows, be sure that they use WORKGROUP as the workgroup name as well. If you use the Network Setup Wizard on an XP computer, be careful: It will try to change the workgroup name to MSHOME. At the appropriate step in the wizard, change the name back to WORKGROUP.

Enable File and Printer Sharing

To enable File and Printer Sharing on Vista, click Start, Control Panel. Select Network and Internet, and then Network and Sharing Center, shown in Figure 6.5.

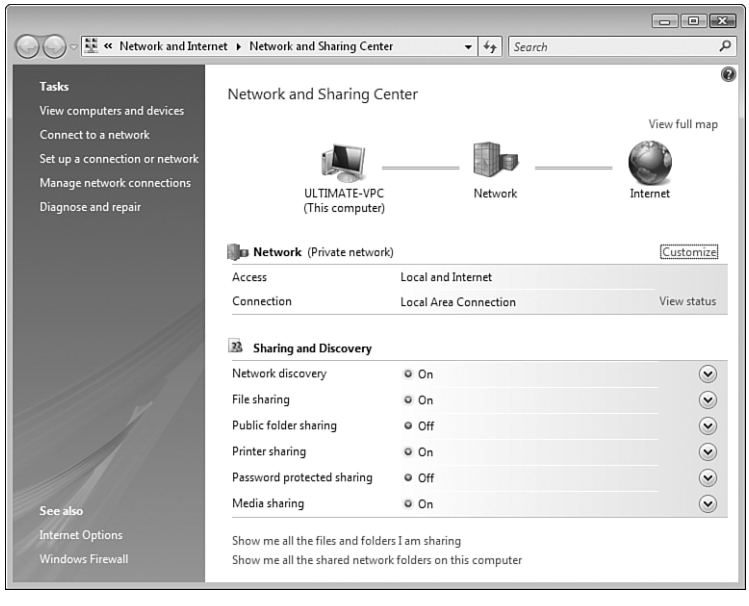


Figure 6.5 The Network and Sharing Center lets you control Vista's sharing features.

The first thing to note is the network type that you originally selected when you started Windows after installing your network. When you connect Vista to any network, wireless or wired, it probes

the other devices on the network to see whether it's been connected to the same network before, or if the network is new. The first time Vista is connected to a new network, it asks you whether the network is Public or Private. If you label the network Public, it's considered to be "dangerous" in that you wouldn't want to trust other users to see the contents of your computer, and so file sharing, network device discovery, and other services are disabled on that network connection. If you label the network Private, network services such as file sharing can be enabled.

So before you can share files, check the label next to your network's name (which is usually just Network). If the label is Public, click the word Customize. Check Private, click Next, confirm the User Account Control prompt, and then click Close.

Now, check the following settings:

- **Network Discovery**—Should be On.
- **File Sharing**—Should be On.
- **Public Folder Sharing**—The Public Documents folder is used for files that you want all users on your computer to be able to see and use. Set Public Folder Sharing feature to On if you want the Public Documents folder to visible to other users on your network as well.
- **Printer Sharing**—Should be On.
- **Password Protected Sharing**—I discuss this feature in more detail later in this chapter under "Simple File Sharing."
- **Media Sharing**—Set to On if you have a library of music and video that you want to make available to other users and to media playback devices on your network (such as the Roku Soundbridge).

If you need to change any of these settings, click the small v in the circle to the right of the feature name and change the setting. You will probably need to confirm a User Account Control prompt.

At this point, file and printer sharing is ready to go. There is one more step only if you've added a third-party firewall program to your computer.

Open Firewall

If you've added a third-party network firewall program to your computer, just setting File and Printer Sharing On may not be enough to let other computers "see" your computer or use any folders or printers you share. You may need to take extra steps to open your firewall to Windows file sharing data. You'll have to check the manufacturer's instructions for the specifics, but what you want to do is to permit inbound and outbound Windows File Sharing data traffic. If your firewall requires you to specify TCP and UDP port numbers, be sure that the following protocols and ports are open:

UDP port 135
UDP port 136
TCP port 137
TCP port 445

Open these ports to other computers on your same network (same subnet).

IP Addressing Options

Windows uses TCP/IP as its primary network protocol. Each computer on the network needs to have a unique IP address assigned to it. There are three ways that IP addresses can be assigned:

- Manually, in what is called *static* IP addressing. You would select an address for each computer and enter it manually.
- Dynamically, through the DHCP service provided by Internet Connection Sharing, a Windows NT/200x server, or a hardware connection-sharing router.
- Automatically, though Windows' Automatic Private Internet Protocol Addressing (APIPA) mechanism. If Windows computers are configured for dynamic IP addressing but there is no DHCP server present, Windows automatically assigns IP addresses. This is the least desirable option.

By default, a newly installed network adapter will be set up for dynamic addressing. I recommend that you do *not* rely on APIPA to configure your network. In my experience, it can cause horrendous slowdowns on your computers. If you don't have a device or computer to provide DHCP service, configure static TCP/IP addresses.

Configuring Dynamic (DHCP) IP Address Assignment

By default, Windows sets up newly installed network adapters to use dynamic IP address assignment, so for new adapters, you don't need to take any additional configuration steps.

Note

If you used static addressing in the past, just view the properties page for your network adapter, select Internet Protocol (TCP/IP), click Properties, and set both the IP Address and DNS settings to Obtain an Address Automatically.

You will need a computer or hardware device to provide DHCP service (which provides configuration information) to all your other computers. This is provided automatically by any Windows computer that runs Windows Internet Connection Sharing (there can be at most one such computer on a network), by the addition of an Internet connection-sharing router, or a wireless access point that includes an Internet connection-sharing feature. (Alternately, you could run the DHCP service on a Windows Server computer. These operating systems can be used on workgroup networks as well as domain networks, although setting them up is beyond the scope of this book.)

If you are using Windows Internet Connection Sharing, it assigns IP address 192.168.0.1 with a network mask of 255.255.255.0 to the network adapter in the sharing computer. Other computers should be configured for dynamic addressing and receive addresses from 192.168.0.2 on up.

If you are configuring a hardware Internet Connection Sharing router, you may need to enable and configure its DHCP server. Usually, the DHCP feature is enabled by default, so you do not need to configure it. If you do, you can use the following settings:

DHCP Server:	Enabled
Server IP address:	`192.168.0.1`
DHCP starting address:	`192.168.0.100`
Number of addresses:	`100`
DNS server(s):	(As provided by your ISP)

Some routers prefer to use a different subnet (range of network addresses)—for instance, `192.168.1.x`. Whichever range you use, be sure to use the same subnet range for any static IP addresses you assign. There is more information on setting up IP address ranges in the online Appendix C, "Remote Desktop and Remote Assistance" in the discussion of enabling Remote Desktop.

Configuring Static IP Addresses

You'll want to set up static (fixed) IP addresses for some or all of your computers in three situations:

- If your network has no shared Internet connection and no router, you'll want to assign static IP address for all your computers, so you won't be slowed down by the Automatic IP configuration mechanism.
- If you have computers that you want to reach from the Internet—for example, one or more computers that you want to be able to use via Remote Desktop—you'll want to assign a static IP address at least to those computers; the others can have their IP addresses assigned automatically.
- If you have network-attached printers or print servers, you'll need to assign static IP addresses to these devices. You need to enter these addresses when you're setting up Windows to use the printers.

The goal in assigning static IP addresses is to ensure that each computer on your network has a unique IP address, shared by no other, and that all the other TCP/IP setup information is the same on every computer.

I suggest you make a worksheet that lists the setup information for your network. Determining what settings to use depends on the type of network you have, which will be one of the following three choices:

- If your network does not have a router, *and* you are not using Windows Internet Connection Sharing, use the following values for your computers:

IP Address:	192.168.0.x, where x is a number from 200 on up
Network Mask:	255.255.255.0
Gateway Address:	Leave blank
DNS Server:	Leave blank

- If your network has a router, connect it and turn on one of your computers. Be sure that the router is configured and working, according to the manufacturer's instructions, and be sure that you can view web pages from the attached computer. Then click Start, All Programs, Accessories, Command Prompt. In the command prompt window, type **`ipconfig /all`** and press Enter. Make a note of the IP address, network mask, gateway address, and DNS server

listed in the window. (On Vista, ignore the IPv6 information, and ignore the information for networking adapters that have the word *Tunnel* or *Teredo* in their name.)

Then use the following values for any computers and devices that need a static IP address:

IP Address:	*a.b.c.x*, where *a.b.c* are the first three numbers of the IP address you saw in the Command Prompt window, and *x* is a number from 200 on up. This might end up being something like 192.168.1.200.
Network Mask:	As noted in the Command Prompt window, usually 255.255.255.0.
Gateway Address:	As noted in the Command Prompt window, usually something like 192.168.0.1.
DNS Server:	As noted in the Command Prompt window, usually the DNS addresses supplied by your ISP, or in some cases the same as the gateway address.

- If you are using Windows Internet Connection Sharing, use the following values for those computers and devices that need a static IP address:

IP Address:	192.168.0.*x*, where *x* is a number from 200 on up
Network Mask:	255.255.255.0
Gateway Address:	192.168.0.1
DNS Server:	192.168.0.1

I suggest that you then list on your worksheet all your computers and any printer devices. Next to each, write down "automatic" if you are letting the computer get its address automatically, or write down the IP address that you will be setting manually. This way you can keep track of which numbers have been used already. The finished worksheet might look something like this:

```
My Network:
Information from command prompt window:
IP Address:      192.168.0.2    (so: all IP addresses will start with 192.168.0)
Network Mask:    255.255.255.0
Gateway Address: 192.168.0.1
DNS Servers:     10.11.12.13
                 10.21.22.23

My IP Address assignments:
java             192.168.0.200   (want to access from Internet with Remote Desktop)
sumatra          automatic
bali             automatic
HPJetDirect      192.168.0.201   (print server)
```

With this worksheet in hand, configure each computer or device that requires a static IP address.

To assign an IP address to a computer running Windows XP, use the following steps:

1. Log on as a Computer Administrator.
2. Open the Network Connections window. Right-click the entry or icon for your LAN adapter (usually labeled Local Area Connection) and select Properties.
3. Select Internet Protocol (TCP/IP) and click Properties.
4. On the General tab, enter the selected IP address, subnet mask, default gateway, and one or two DNS server IP addresses, as shown in Figure 6.6.

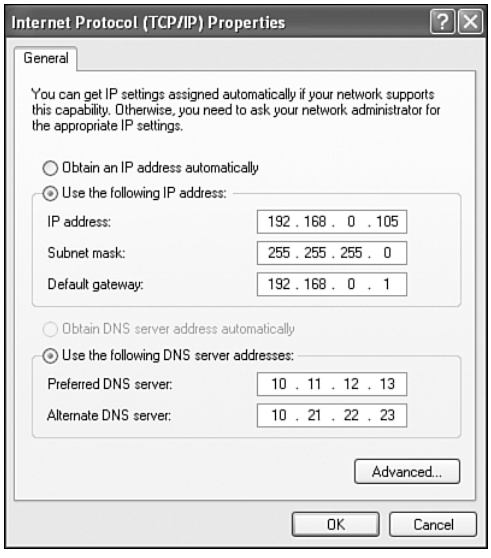


Figure 6.6 Enter static IP address information on the General tab.

5. You can configure your preferred Internet domain name (called the *preferred DNS suffix*) on the Network Identification page in the System Properties dialog. To get there, right-click [My] Computer and select Properties, or select Advanced, Network Identification in the Network Connections window. View the Computer Name tab, click Change, and then click More.

   You can also enter a preferred Internet domain name for each individual network or Internet connection. You might want to use your company's domain name on the network connection, and your ISP's domain name on a dial-up connection. To do this, view the network connection's properties dialog, click the Advanced button, select the DNS tab, and enter the domain name under DNS Suffix for This Connection, as shown in Figure 6.7.

   Also, if your ISP has provided you with more than two DNS server addresses, click Add to enter additional addresses on this same tab.

6. Unless your network's DNS server supports dynamic IP address registration, uncheck Register This Connection's Addresses in DNS.

7. Click OK to close the dialogs.

On Vista, follow these steps:

1. Click Start, right-click Network, and select Properties.
2. Select Manage Network Connections.
3. Locate the icon corresponding to your LAN adapter. It is probably named Local Area Connection or Wireless Connection. Right-click this icon and select Properties.
4. Confirm the User Account Control prompt.
5. Select Internet Protocol Version 4 (TCP/IPv4) and click Properties.

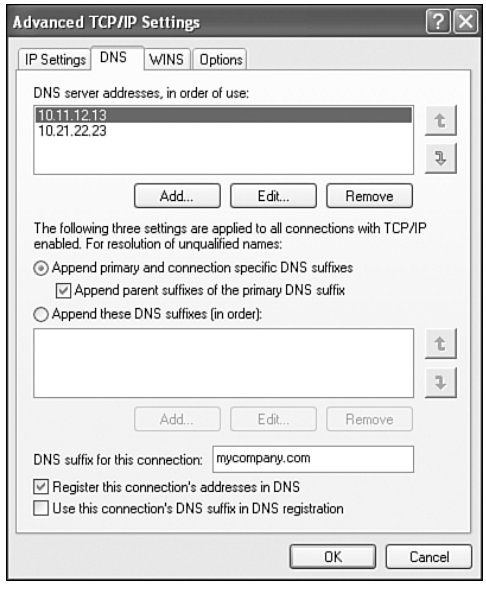


Figure 6.7 Enter per-connection DNS information on the connection's Advanced Properties DNS tab.

Then follow the steps previously described for assigning an IP address on Windows XP, starting at step 4.

Configuring Additional Useful Network Services

Besides the TCP/IP protocol and network services that are installed by default with Windows, you may want to install some additional services manually as part of your network setup.

Link Level Topology Discovery (LLTD) for XP

Windows Vista includes a network map feature that shows a diagram of the devices and computers on your network. The map is constructed from data collected by the Link Level Topology Discovery (LLTD) protocol. Vista comes with LLTD software preinstalled, but to get it in XP you must have Service Pack 3 installed. Thus, if you have computers running both Windows Vista and XP Service Pack 2 on your network, the XP SP2 computers don't show up on Vista's Network Map.

To install LLTD support on XP without installing Service Pack 3, perform the following steps on each of your XP computers:

1. Visit microsoft.com and search for "KB922120." Select the search result titled "Download Details: Link Layer Topology Discovery (LLTD) Responder (KB922120)."
2. Click Continue to perform Windows license validation.
3. Download and then run the small installer program.

Note

At the time this was written, LLTD responder software was not available for Windows Server versions, Mac OS X, or Linux, so computers running these operating systems also do not appear as connected computers in Vista's network map.

Internet Gateway Device Discovery and Control Client

If you are using a hardware Internet-sharing router or Windows Internet Connection Sharing, you should install the Internet Gateway Device Discovery and Control Client on all your Windows XP computers. This service places an icon in each computer's Network Connections folder that lets users monitor and manage the Internet connection that is hosted on the sharing computer or the router.

To install the Discovery and Control Service, follow these steps on each XP computer:

1. Log on as a Computer Administrator.
2. Open the Network Connections window.
3. From the menu, select Advanced, Optional Networking Components.
4. Select Networking Services and click Details.
5. Check both Internet Gateway Device Discovery and Control Client and UPnP User Interface, and click OK.
6. Click Next.

When this service has been installed, an icon appears in your Network Connections window for your router or other network devices. You can double-click this icon to open the device's setup and control page. What appears varies from device to device, but it's usually the device's built-in setup web page.

Universal Plug and Play

If you use a hardware connection-sharing router or Internet Connection Sharing, you may also want to consider enabling a feature called Universal Plug and Play (UPnP). UPnP provides a way for software running on your computer to communicate with the router. Here's what UPnP can do:

- It provides a means for the router to tell software on your computer that it is separated from the Internet by Network Address Translation. Some software—Remote Assistance and the video and audio parts of Windows Messenger in particular—ask the computer on the other end of the connection to establish a connection back to your IP address. On a network with a shared connection, however, the IP address that the computer sees is not the public IP address that the shared Internet connection uses. UPnP lets software such as Remote Assistance find out what its public IP address is. It also provides a way for the router to suggest alternate port numbers if several computers on the network want to provide the same service (for example, if several users send Remote Assistance requests).
- It provides a means for software running on the network to tell the router to forward expected incoming connections to the correct computer. Remote Assistance and Windows Messenger again are two good examples. When the computer on the other end of the

connection starts sending data, the router does not know to send it to your computer. UPnP lets UPnP-aware application programs automatically set up forwarding in the router.

- UPnP provides a means for printers and perhaps other types of as-yet-undeveloped hardware devices to announce their presence on the network so that Windows can automatically take advantage of the services they provide.

UPnP has a downside, however: It has no built-in security mechanism, so any program on any computer on your network could potentially take control of the router and open "holes" for incoming connections (and there are already some viruses and Trojan horses that take advantage of this). However, Windows Firewall or your third-party firewall package will still provide some protection. Windows Firewall warns you if an undesired program prepares to receive incoming network connections, and this cannot be disabled as long as you are not using a Computer Administrator user account. In addition, most third-party firewalls inform you if an unrecognized program requests either incoming or outgoing network connections. UPnP abuse is not yet a serious problem. If you use Remote Assistance or Windows Messenger, the benefits that UPnP provides mostly outweigh the risks.

To use UPnP, you must enable the feature in your router. It's usually disabled by default. If your router doesn't currently support UPnP, you may have to download and install a firmware upgrade from the manufacturer. Most routers now do support UPnP.

On Windows XP, UPnP is enabled by default. If you have a UPnP router or Windows Internet Connection Sharing running on your network, the Network Connections screen should display an icon for the router as shown in Figure 6.8.

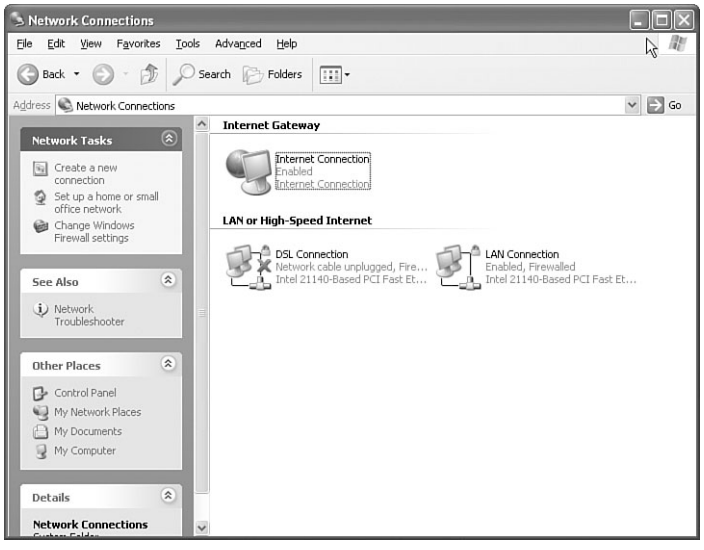


Figure 6.8 If your router supports UPnP, an Internet Gateway icon should appear in Network Connections.

Note

If the icon doesn't appear, click Advanced, Optional Networking Components, select Networking Services, and click Details. Be sure that Internet Gateway Device Discovery and Control Client is checked. While you're here, check UPnP User Interface as well—this enables support for future UPnP devices.

Then, on the task list, click Change Windows Firewall Settings. View the Exceptions tab and be sure that UPnP Framework is checked.

On Vista, UPnP is controlled by the Network Discovery setting, which is enabled by default on private networks and disabled on public networks. To manually control Network Discovery on Vista, follow these steps:

1. Click Start, Control Panel.
2. Select the Network and Internet link, and then select Network and Sharing Center.
3. At the bottom of the page, check the setting for Network Discovery. To change it, click the round ∨ button, select Turn On or Turn Off Network Discovery, click Apply, and then confirm the User Account Control prompt.

When UPnP is working, on XP you should see an icon for your router or gateway under the title Internet Connection in the Network Connections window. If you right-click this icon and select Status, you'll see a dialog similar to the one shown in Figure 6.9, displaying the status of the router's connection. If your Internet service uses a connection-based system such as PPPoE or standard dial-up service via a modem, this dialog may display a button that lets you connect to and disconnect from your ISP.

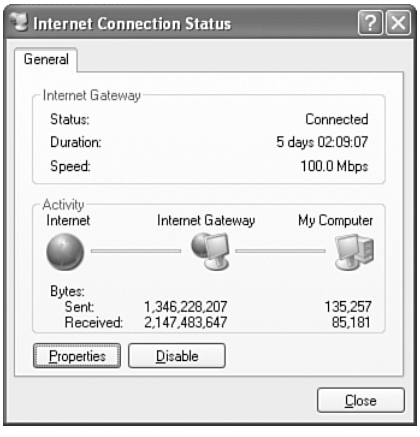


Figure 6.9 Router status displayed via UPnP.

Click Properties and then Settings to display a list of network services for which the router is forwarding incoming connections to computers on your network. This list shows only forwarding settings made via UPnP. Services you've forwarded using the setup screens on your router, such as Remote Desktop, as discussed in the online Appendix C, do not appear here and new settings should not be made here—they usually disappear when the router is reset.

On Vista, the icon appears in the Network Map in the Network and Sharing Center. All you can do with it is select Properties, and from the properties log, View Device Web Page. (The capability to monitor port forwarding is not available on Vista.)

Designating a Master Browser

Windows uses a database of known online computers to build the display known variously as Network Neighborhood, Computers Near Me, or View Workgroup Computers. The database is managed by a software service called the Browser Service. It runs on one of your computers, which is designated the "master browser." The master browser is selected by an automatic election held by the computers on the network. In addition, on a larger network some computers may be elected as backup browser servers.

Note

Vista adds an additional mechanism called the Link Level Discovery Protocol, which we discuss in the next section, but it still uses the Browser Service as well.

When you are running a network with different versions of Windows, or if your computers don't all have the exact same list of protocols installed, this service sometimes malfunctions: The election goes haywire (perhaps because of the Windows equivalent of the hanging chad), or the database is filled incorrectly, or other problems occur. The result is that the Network Neighborhood display doesn't function correctly even though the computers clearly can communicate with each other (for example, one can map network drives to folders shared by the invisible computers).

If you find that this occurs on your network, you may want to force the master browser service to run on a designated Windows XP or Vista computer that is always left on. This can help stabilize the list of local computers.

To make this work you have to configure one computer to always be the master browser, and configure all the other computers never to offer to be the master. To make these settings on a computer running Windows Vista, XP, 2000, or NT you have to edit the Registry key `HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\Browser\Parameters`. Two values can be altered (refer to Chapter 5, "Tweaking and Tuning Windows," for more details on editing the Registry):

Value	Possible Settings
`IsDomainMasterBrowser`	`True`—This computer will be the master browser
	`False`—Master is determined by election
`MaintainServerList`	`No`—Never serve as master
	`Yes`—Ask to be the preferred master
	`Auto`—Offer to be master if needed

If you want to force one computer to be the master browser in all circumstances, set the `IsDomainMasterBrowser` value to `True` on that computer and `False` on all others. If you want to set one computer to be the preferred browser, but let others step in if the master is unavailable,

just set the `MaintainServerList` key to `Yes` on the preferred computer, and be sure to turn it on before the others.

Simple File Sharing

Although most home users are typically happy letting anyone at any computer read or modify any file, business users need to restrict access to files with payroll, personnel, and proprietary information. Windows Vista, XP, and their predecessors, Windows NT and Windows 2000, were designed with business use in mind, so they require usernames and passwords for identification, and have a security system that lets computer owners restrict access to sensitive files on a user-by-user and file-by-file basis on each computer.

Unfortunately, on a Windows workgroup network, there is no centralized list of authorized usernames. This makes maintaining control of who is and isn't permitted to access network files on each computer difficult. Here's why: When you attempt to use a file or printer shared by another computer, Windows sends your username and password to the other computer. In versions of Windows *prior* to XP,

- If the username and password matched a user account already set up on the other computer, Windows used that account's permission settings to determine whether to grant you access to the file.
- If the user information didn't match, Windows prompted you to enter a username and password that the other computer would recognize.
- If you failed to provide a valid password, the remote Windows computer gave you the permissions assigned to the Guest account, which was usually disabled or didn't have permission to access the resource you wanted.

The advantage of this system was that it let you determine precisely which users could access specific files and printers. The disadvantage was that it required you to set up identical user accounts for each network user on every computer, and then grant these users permissions to view and modify shared files and folders.

Smaller business and home users found this security setup cumbersome to use and difficult to set up properly. This pushed people into sharing accounts and passwords, and otherwise avoiding good security practices, just to get the network to work. That's a risky approach, so Microsoft gave Windows XP a feature called *Simple File Sharing*. On Vista, the corresponding feature is called Password Protected Sharing, but the sense of having it turned on or off is reversed from XP. Here's how the features correspond:

XP	**Vista**
Simple File Sharing *Enabled*	Password Protected Sharing *Off*
Simple File Sharing *Disabled*	Password Protected Sharing *On*

When Simple File Sharing is enabled (or on Vista, when Password Protected Sharing is off),

- Network users are always given access to shared folders and printers, without being prompted for a username or password. They are automatically granted access to files and folders, using the permissions granted to the Guest account, even if Guest is disabled for direct logins.

- On XP only, the Security properties tab that is normally used to assign per-user permissions to files and printers is not displayed, even for files that are stored on a drive formatted with the NTFS file system. Files stored in directories in a user's profile folder (My Documents, for example) are automatically set up to permit access only by the owner, and files stored elsewhere are set up to permit access by anyone.
- Windows automatically assigns appropriate security permissions to folders and printers when you share them. If you check Allow Network Users to Change My Files, all network users can read, write, rename, or delete the contents of the shared folder. If you don't check this option, network users can view but not modify the contents.

The result is that with Simple File Sharing in effect, anyone who connects to your computer through the network has access to all shared files, folders, and printers shared by the computer, with no security enforcement of any kind. This has the advantage of eliminating all worries about having to manage accounts and passwords on multiple computers, but it does mean that you have to keep in mind these points:

- You don't get to pick and choose who gets access and who doesn't. Everyone gets access to every shared resource.
- If you have an unsecured wireless network with no WEP or WPA security key, anyone driving by your home or office can not only connect to your network, but also see and/or modify your shared files.
- On XP, the Shared Documents folder that appears under My Computer is automatically set up as a shared folder, the idea being that any files you place in it are available not only to other users on your computer, but to other users anywhere on your network. On Vista, you can control whether the Public Documents folder is shared on the network from the Network and Sharing Center.

In the end, it's a reasonable trade-off, as long as you keep in mind the fact that all shared files and folders are available to anyone who can connect to your network. You should also keep in mind that

- Simple File Sharing is always used on XP Home Edition, and cannot be disabled. This means that anyone can use any resource shared by a computer running XP Home Edition.
- Simple File Sharing is optional on XP Professional, when the computer is part of a workgroup network. It's enabled by default when Windows is installed, but you can disable it if you want to use user-level security on files and/or shared resources.
- Simple File Sharing is always disabled on an XP Professional or Vista computer that is joined to a domain network. User-level security is always used in this case.
- Simple File Sharing applies only to the resources shared by the computer running Windows XP and Vista. If you use XP to use folders shared by a computer running some other operating system, such as Windows Me or Mac OS X, that operating system's security system is used.

On an XP Professional computer that is not a member of a domain network, the Simple File Sharing feature can be disabled from the Tools, Folder Options, View tab in any Windows Explorer window, as shown in Figure 6.10. You must be logged on as a Computer Administrator to change the setting.

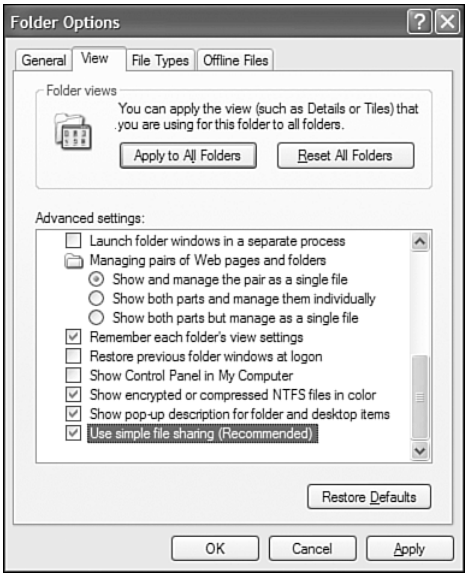


Figure 6.10 Simple File Sharing is enabled by default; disable it to use the old Windows NT/2000 access control system on a peer-to-peer network.

To change the Password Protected Sharing setting on Vista, follow these steps:

1. Click Start, Control Panel, Network and Internet, Network and Sharing Center.
2. Click the small round v button next to Password Protected Sharing. Click Turn On or Turn Off Password Protected Sharing as desired.
3. Click Apply, and then confirm the User Account Control prompt.

Tip

If you disable Simple File Sharing, remote users have to supply a username and password valid on your computer to use a shared resource on your computer. In this case, it vastly simplifies things if you set up an identical account for each user on each of your computers. For each user, pick a username and password, and use that same name and password on every computer.

Also, on XP if Simple File Sharing is disabled, your computer displays different dialog boxes when you go to share a folder, and you'll have access to the Security properties page on folders and printers. You can see both versions in the next section.

Sharing Resources

After your network is working, each computer can share selected resources—that is to say, folders and printers. The purpose of sharing is to make these folders and printers available to other computers, where they look and act *exactly* like folders on your own hard drive and printers connected to your own computer. This section briefly describes how to make resources available to other computers on the network.

Sharing Folders and Drives

By default, on a workgroup network Windows XP automatically shares the My Documents folder in the All Users profile folder; this is the folder that is listed as Shared Documents in My Computer.

Vista has a corresponding feature, but you must enable it. To do so, click Start, Control Panel, Network and Internet, Network and Sharing Center. If Public Folder Sharing is shown as Off, click the round v button next to it and select Turn On Public Folder Sharing.

Caution

Do not enable Public Folder Sharing if you are at an Internet café or on any other public network.

To make a file available to other users, simply drag it to the [Shared or Public] Documents folder on your computer, and users on other computers can locate it on the network and read or copy it. In many cases, having this one shared folder might be sufficient.

Sharing Folders on XP

You can share other folders as well. To do so, locate the folder in Windows Explorer and right-click it. From here, the procedure differs somewhat depending on whether you're using XP or Vista.

On XP, select Sharing. If you have Simple File Sharing enabled, the dialog in Figure 6.11 will appear.

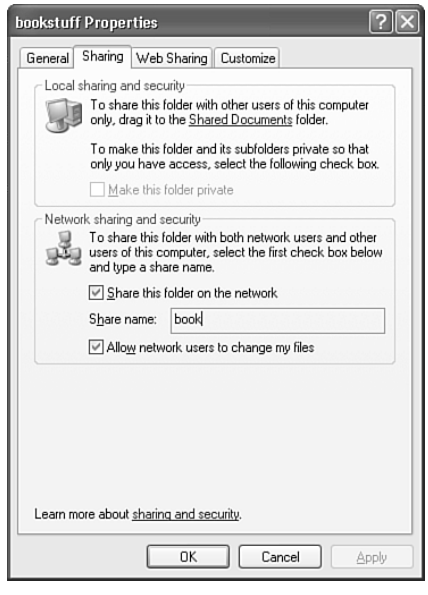


Figure 6.11 To share a folder, check Share This Folder on the Network and enter a share name.

Check Share This Folder on the Network and enter a share name, a name of up to 14 characters with no punctuation characters other than the underscore (_) or hyphen.

On an XP Professional computer on a workgroup network with Simple File Sharing enabled, or on a Windows XP Home Edition computer, you see a check box labeled Allow Network Users to Change My Files. If you do not check it, network users can view and copy the files, but they cannot modify or delete them.

On an XP Professional computer with Simple File Sharing disabled, or on a domain network, the Sharing tab appears as shown in Figure 6.12.

Figure 6.12 When Simple File Sharing is not active, there are more specific permission controls.

In this case, you can control permissions to read and write files on a per-user or per-group basis by clicking the Permissions button. These permissions work as *additional restrictions* to any imposed by NTFS file security, if the folder is on a drive formatted with NTFS.

For example, if the sharing permissions grant read/write access to Everyone, the file is still protected by whatever per-user permissions are assigned to the file; a network user simply has the same rights to the file that he or she would have if seated right at the computer. If the sharing permissions give Everyone just Read access, users can read files *if* the NTFS permissions let them, but in any case no network user can modify or delete files.

Sharing Folders on Vista

On Vista, after right-clicking a folder, select Share. The dialog shown in Figure 6.13 appears. By default, your own user account is listed.

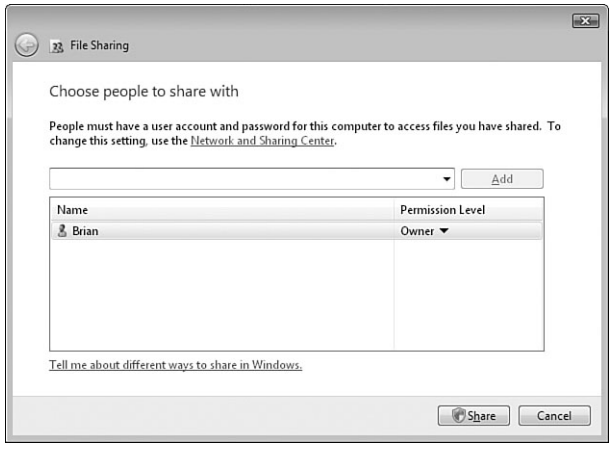


Figure 6.13 The File Sharing Wizard in Windows Vista.

- If Password Protected Sharing is turned on, use the drop-down list to select one or more other user accounts or group names (including the helpful catch-all Everyone), and click Add to give permission to read and/or save files in the shared folder.
- If Password Protected Sharing is turned off, add Everyone to the sharing list; this is the only entry that matters for network access.

As soon as one or more names are listed in the People to Share With list, you may adjust their Permission Level settings by selecting one of the following choices:

- **Owner, Co-Owner**—Can read, modify create, delete, rename, and change permissions on files.
- **Contributor**—Can read, modify create, delete, and rename files.
- **Reader**—Can read but not write, modify, or delete files.

Note

These permission settings do two things: They are used to add access rights (NTFS file permissions) to the folder, which are used for users who log on directly at the computer, *and* they are used for over-the-network access.

Click Share to finish the sharing process. After a folder has been shared, to adjust its sharing settings, view its Properties page and select the Sharing tab. The settings are nearly identical to those described previously for XP, so I won't repeat that discussion here.

Sharing Folders from the Command Line

From the command line, you can share a folder or drive with the command

```
net share sharename=drive:\fullpath
```

For example,

```
net share music=c:\musicfiles
```

or

```
net share cddrive=d:\
```

and can cancel a share with the command

```
net share sharename /delete
```

Note

You can prevent a share from being displayed when other users browse the network by adding a dollar sign ($) to the share name. For example, the share name **secret$** will not appear in the My Network Places display. This won't deter a motivated hacker, but it does discourage casual browsing. To use a resource that's been hidden this way, you have to explicitly use its name. For example, you can open ***computername**sharename*$** in Windows Explorer or you can map a network drive to this network path.

Note

Administrators may be used to using the built-in whole-drive shares that are automatically created for each disk drive on a Windows NT/2000/XP computer, for example, C$. However, these shares are available only to Computer Administrator users. You cannot reach these administrative shares on a Windows XP computer that has Simple File Sharing enabled because all network access takes place through the Guest user account.

You can also share entire drives by viewing and right-clicking the drive icon in [My] Computer. This is a great way to make a DVD-ROM, CD-ROM, floppy disk, or other disk available to all users on a network. In the case of DVD and CD drives, you can read but not write to these disks.

Sharing Printers

You can share any printer that is controlled by your computer. This includes printers directly cabled to your computer and printers driven using LPR or other direct network protocols.

To enable printer sharing, do the following:

1. Choose Start and view the Printers and Faxes folder.
2. Right-click the printer icon and choose Sharing, or select Properties and then select the Sharing tab.
3. Select Share This Printer, and enter a network name for the printer, as shown in Figure 6.14. Enter up to 14 characters, avoiding punctuation characters.
4. If your network has only Windows Vista/XP/2000 32-bit computers, click OK, and you're finished. Other network users can now use the shared printer.

Otherwise, continue to the next section to add extra printer drivers for other operating systems.

Installing Extra Printer Drivers

If you have computers running other versions of Windows or other CPU types, you can load the appropriate printer drivers for those operating systems now, and network users will receive them automatically when they connect to your printer. This step is optional, but it's a friendly thing to do.

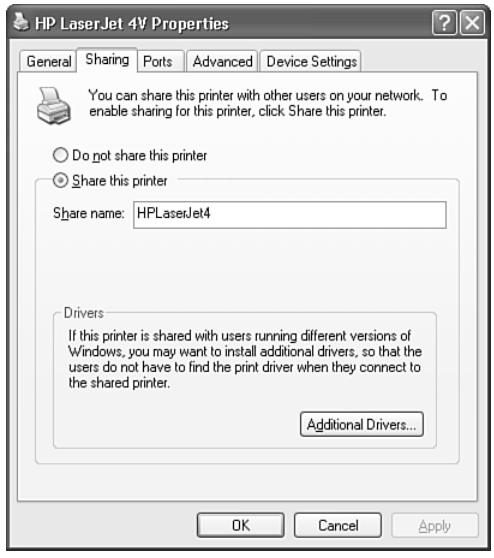


Figure 6.14 Enabling sharing for a printer.

View the Sharing tab in your printer's Properties dialog box and select the Additional Drivers button. Windows displays a list of supported operating systems and CPU types. The XP version is shown in Figure 6.15. (By the way, "Intel" refers to any Intel or compatible chips, such as those made by AMD or VIA/Cyrix.) On Vista, you can install only XP-/Vista-compatible drivers, in 32- and 64-bit flavors.

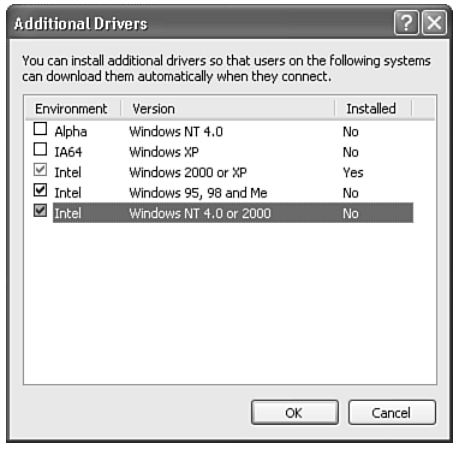


Figure 6.15 You can install drivers for additional operating systems or CPUs to make it easy for network users to attach to your printer.

Check the boxes for operating systems you want to support and click OK. Windows then goes through these one by one and asks for the appropriate driver disks. You can find these drivers on

the original installation disks for the alternative operating system, or often on disks provided with the printer, which might contain support for many operating systems on the same disk.

When installed, the alternative drivers are sequestered in your Windows folder and delivered to users of the other operating systems when they elect to use the networked printer.

Setting Printer Permissions

If you're on a domain network or have chosen to disable Simple File Sharing, you can control access to your shared printers with three security attributes that can be assigned to users or groups:

Permission	Lets User or Group
Print	Send output to the printer
Manage Printers	Change printer configuration settings, and share or unshare a printer
Manage Documents	Cancel or suspend other users' print jobs

You can use the Security tab in the printer's Properties dialog box to alter the groups and users assigned each of these permissions. The CREATOR OWNER name applies to the user who submitted a given print job.

You probably don't have to change the default permission settings unless you want to limit use of the printer by outside users in a domain environment only. In this case, delete Everyone, and add specific groups with Print permission.

Sharing Fax Modems and Other Devices

The software provided with Windows does not permit you to share a data modem, fax modem, scanner, or other input/output device over your network. You may find it as annoying as I do that the Windows Fax service is built to provide shared fax sending and receiving for a network, but the sharing capability is disabled in Windows XP and Vista.

If you want to be able to send faxes through a single phone line from several networked computers, the Windows Fax service on Windows 2000 Server or Windows Server 2003 *can* be shared. You can also purchase a third-party fax sharing program such as Symantec WinFax.

Shared scanners are a more complex matter. Some printer/scanners have network capability built in. (This isn't even a high-end feature anymore. The Brother all-in-one laser printer/scanner/copier I bought for $99 has it.) With network capability, anyone on the network can use the scanner from his own desk. But this may not really be necessary. Because a scanner has to be connected to one of your computers anyway, and you will need to stand there to put pages into the scanner, you can simply save the scans to a network shared folder and later pick up the files from another computer.

Avoiding Firewall Issues

If you find that you cannot access shared folders or printers on another network computer, or if other users cannot access resources that are shared by your computer, it's possible that Windows

Firewall or a third-party firewall is interfering. You may need to make a configuration change to let file and printer sharing work. However, in doing so, you must be *very careful* not to make your computer more accessible than absolutely necessary.

Use this checklist to enable file and printer sharing on both the computer that is sharing resources and the computer that is attempting to use them.

- On XP, be sure that you have run the Network Setup Wizard at least once. File and printer sharing are silently disabled until you do so.
- If the computer is running Vista or Windows XP Service Pack 2 or later, be sure that the Windows Firewall service is not blocking you. Open the Control Panel. On XP, open Security Center, and then Windows Firewall. On Vista, select Allow a Program Through Windows Firewall. Select the General tab. The Firewall should be On, and Don't Allow Exceptions should *not* be checked. On the Exceptions tab, be sure that File and Printer Sharing is checked.
- If you are using a third-party firewall service such as Norton Internet Security, be sure that this firewall is also configured to permit Windows File and Printer Sharing between computers on your subnet. The exact method for doing this varies from one product to another, but most have a fairly easy and explicit way to enable Windows file and printer sharing.

In general, you *cannot* safely share files and printers between computers that are not on the same network subnet—that is, directly connected on a network that is controlled by a single router.

Caution

If your computer is directly connected to the Internet, it is exceedingly dangerous to disable Windows Firewall or your third-party firewall package. Your computer may quickly become infected by viruses and Trojan horse programs that are constantly scouring the Internet looking for unprotected Windows computers.

Providing Shared Internet Access

Although you could give each computer its own dial-up modem or broadband modem, one of the principal advantages of installing a network is gaining Internet access for all your computers through a single connection. There are two simple ways to provide shared Internet access for a home or small office network:

- If you have cable or DSL broadband Internet service, get a hardware Internet connection-sharing router. It's easy to set up, costs little or nothing, provides a certain amount of added security to your network, lets you add on additional computers with no setup effort, and can let you use both wired and wireless connections at the same time.
- If you use standard dial-up Internet service (not AOL dial-up service), use the Windows Internet Connection Sharing service to share the connection with others through your network. This is an acceptable solution although the "sharing" computer must be turned on to use the Internet from your other computers.

Note

You cannot share an AOL dial-up connection, nor can you share connections to discount ISPs that require the use of their proprietary dial-up software.

Caution

For homes with more than one computer, some cable Internet providers may require you to connect your computers and cable modem to a hub, rather than to a router. However, this is dangerous—it exposes all your computers directly to the Internet. If you still have this sort of setup, I strongly recommend that you purchase a hardware cable/DSL connection-sharing router to place in between your cable modem and your computers. Otherwise, you *must not* enable File and Printer Sharing on your network.

Shared network connections provided by hardware routers and Windows Internet Connection Sharing (ICS) use a mechanism called *Network Address Translation* (NAT) to mediate between the computers on your network and the Internet via a single connection and single public IP address. The router or ICS computer has two connections, one to the Internet via a dial-up, cable, or DSL modem, and one to your LAN, as illustrated in the top part of Figure 6.16.

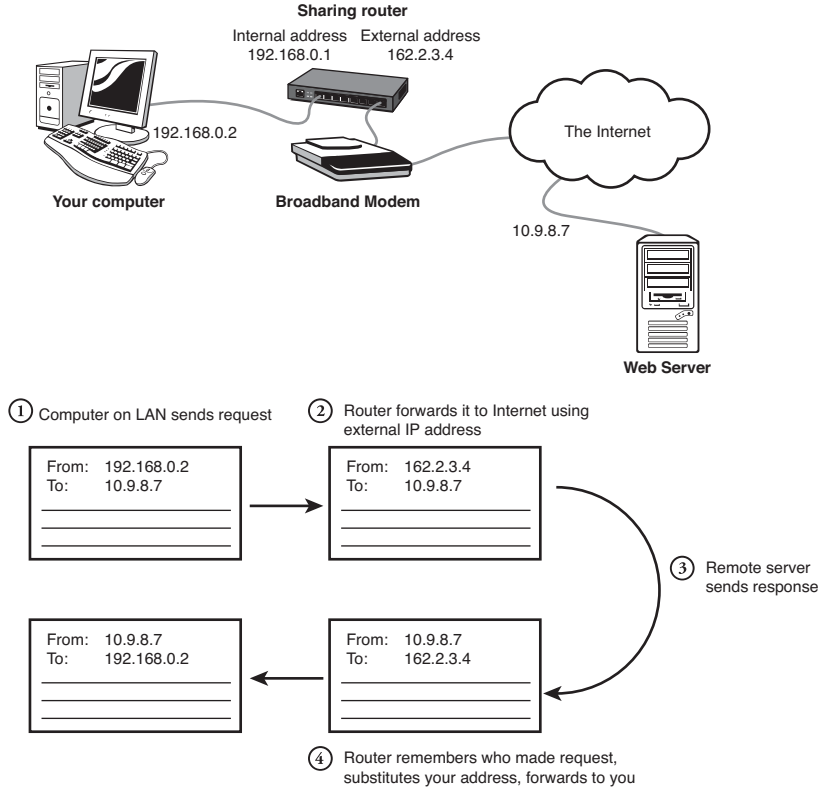


Figure 6.16 A connection-sharing router acts as an intermediary between your LAN and the Internet.

When one of your computers attempts to contact a website, it sends a data packet to the router or computer running ICS to be forwarded to the Internet, as illustrated in the bottom part of Figure 6.16. As it passes the outgoing network data packet to the Internet, the router replaces the packet's "from" address—the private IP address assigned to your computer—with the router's

public address, so that the reply from the remote server will be returned through the Internet to the router. The router remembers from whom the request came, replaces the response's "to" network address with your computer's private address, and transmits it on its LAN connection.

This mechanism works quite well for communication initiated by computers on your network. When outside computers attempt to contact you, however, it's another story. If you have a web or email server on your network, for instance, the connection-sharing router or computer can be configured to send packets for particular network services to the correct computer; this is called *port forwarding*. Otherwise, incoming connection attempts are simply discarded. In this way NAT protects you against random probing by hackers, and it's very helpful to have this as a second level of protection in addition to Windows Firewall.

Adding a Connection-Sharing Router

Connection-sharing routers almost always have one 10Mbps Ethernet port that is used to connect to a cable or DSL modem, and have a second connection for your LAN. This LAN connection can take several forms:

- There may be a single 10/100Mbps Ethernet port.
- There may be four or more 10/100Mbps Ethernet ports, giving you a built-in switching hub.
- There may be a built-in wireless networking access point.
- There may be a combination of the preceding.

Because wireless devices and laptops are becoming so common, and because it's very nice to be able to offer wireless connectivity to friends and visitors even if you don't use it yourself, I recommend purchasing an 802.11g or 802.11n wireless router with a built-in four port switch. Routers without wireless can sometimes be found for $0 after rebate, but usually fall in the U.S. in the $10 to $40 range. If you shop carefully and look for a sale or rebate offer, wireless routers with four-port switches can also frequently be purchased for $10 to $40, so you're getting a lot of connectivity for no additional cost.

Note

If you are planning to use Voice over IP (VoIP) telephone service, contact your VoIP provider to see what sort of routers it supports.

You will need to ensure that your ISP provides you with a cable or DSL modem with an Ethernet port; USB or internal PCI adapters do not work with a router. Use a standard Ethernet patch cable to connect the modem to the Internet or WAN port on the router.

Then connect one of your computer's LAN adapters to one of the ports on the router, using another standard Ethernet patch cable.

Note

Even if you're going to use wireless connections, it's usually required, or at least easier, to use a wired connection to initially set up the router.

When you connect your computer's Ethernet port to the router, Windows automatically requests an IP address and configures the port's TCP/IP settings from default values provided by the router. You should then be able to open your web browser and view the router's setup web page, using the URL `//192.168.0.1` or `//192.168.1.1`, as instructed by your router's installation manual.

Your router establishes the connection to your ISP on your behalf, so you need the same information that you'd need to establish the connection directly through Windows. For a DSL connection, this often involves a username and password. For a cable connection, this often requires that you set the router's hostname to a specific name, or you may have to provide the router's MAC address (its Ethernet hardware address code) to your ISP; this number is usually printed in tiny letters on a label on the bottom of the router. Alternatively, if you've already used your cable Internet service by directly connecting your computer, you might be able to have the router *clone* your computer's MAC address—that is, copy your computer's address and use it on its Internet port so that your ISP doesn't have to make any changes.

Tip

If you previously had your computer connected directly to your cable or DSL modem, power the modem off and back on after you've connected it to the sharing router. This removes your computer's physical (MAC) address from the modem and from your ISP's end of the connection.

After installing the router, run the Network Setup Wizard on all your Windows XP computers. The wizard is described earlier in this chapter, under "Configuring a Workgroup Network." When asked to select a connection method, select This Computer Connects to the Internet Through Another Computer on My Network or Through a Residential Gateway.

On Windows Vista, you should not need to run any setup wizards—Vista automatically detects that you have an Internet connection on the network. However, if you've added a connection-sharing router to an existing network, you may need to adjust any fixed IP addresses you've manually assigned to computers on your network.

After Setting Up a Shared Connection

After the shared connection is set up, all your computers can use it automatically, through the network. The only problem you might run into is with Internet Explorer. If you previously used dial-up Internet, or if you previously had your broadband modem connected directly to your computer, and now Internet Explorer tries to establish a connection whenever you open it, perform the following steps:

1. Open Internet Explorer.
2. If the menu bar is not visible, press and release the Alt key. Select Tools, Internet Options.
3. Select the Connections tab. In the middle of the dialog, select Never Dial a Connection, and click OK.

This keeps Internet Explorer from attempting to make a direct Internet connection.

Using Windows Internet Connection Sharing

All Windows versions since Windows 98 Second Edition have a software version of NAT called Internet Connection Sharing (ICS). It does in software what a connection-sharing router does in hardware. If you have cable or DSL Internet service, I strongly recommend that you use a hardware router.

But, if you really want to, you can use the Windows ICS service to share a broadband connection. You may also want to use ICS if you have standard dial-up Internet service. Internet Connection Sharing can let you use dial-up Internet from two or more computers at once, without tying up additional phone lines—a neat trick. It does, however, require you to leave the computer that is set up to share its connection turned on all the time; at least, it must be on anytime anyone wants to use the Internet.

To set up ICS, select one of your computers to be the one that is to share its Internet connection. Set up and test its Internet connection first, before creating a LAN. For dial-up Internet, get the "sharing computer's" dial-up connection working first, before you connect your network. For broadband Internet, connect the "sharing computer's" network adapter to your cable or DSL modem, and get the Internet connection working first. Only then install a second network adapter that you'll use to hook up to your other computers.

Finally, configure the shared connection. The procedure depends on whether you're using XP or Vista.

Setting Up ICS on Windows XP

On XP, log on as a Computer Administrator. Run the Network Setup Wizard, covered earlier in the chapter, under "Configuring a Workgroup Network." The important points are as follows:

- When you're asked to selection a connection method, select the first choice, This Computer Connects Directly to the Internet. The Other Computers…Connect…Through This Computer.
- When asked to choose a connection, select the entry for the dial-up connection to your ISP.

Complete the rest of the Network Setup Wizard as described earlier in the chapter. If you had set up your LAN previously, be sure to enter the same workgroup name you used originally because the wizard wants to change the setting to MSHOME every time you run it.

When the wizard completes, go to the Network Connections window and locate the icon that represents your Internet connection. It should now say "Firewalled, Shared" and possibly "Disconnected." Right-click it and select Properties. View the Networking tab. In the list of components used by the connection, be sure that *only* Internet Protocol (TCP/IP) and QoS Packet Scheduler are checked. This prevents file sharing from being exposed to the Internet. The firewall does that, too, but it doesn't hurt to be extra safe.

Then restart your computer. Log on again, and try to view a web page (such as www.google.com). Your computer should automatically connect to your ISP, dialing or signing on if necessary. If the web page doesn't appear, you have to resolve the problem before continuing.

When the sharing computer can connect properly, run the Network Setup Wizard on your other Windows XP computers, except for one detail: When you run the wizard, select This Computer

Connects to the Internet Through Another Computer on My Network or Through a Residential Gateway.

Setting Up ICS on Windows Vista

To set up ICS on Vista, set up and test your Internet connection first. Be sure that it's working before you proceed. Then follow these steps on the "sharing" computer:

1. Click Start, Control Panel, Network and Internet, Network and Sharing Center. Under Tasks, select Manage Network Connections.
2. If you are using broadband Internet with a cable or DSL modem connected to your computer through its Ethernet adapter, locate the Local Area Connection icon for this connection, right-click it, and select Rename. Change the name from Local Area Connection to DSL Modem Connection or Cable Modem Connection or some other appropriate name. Confirm the User Account Control Prompt.

   Then right-click this icon and select Properties. Under This Connection Uses the Following Items, *uncheck* every item except QoS Packet Scheduler, Internet Protocol Version 4 (TCP/IPv4), and the two Link-Layer Topology Discovery items.

   You use a second network adapter to connect to the other computers on your network. If you haven't installed it yet, shut Windows down, unplug the computer, and install the adapter now. Power the computer back up, log on, and return to the Network Connections window.
3. If your Internet service is connection-based (standard dial-up, or DSL using a login name and password), right-click your Dial-up or Broadband Connection icon and select Connect so that your Internet connection will be up during the remaining steps. Then right-click it, select Properties, and confirm the User Account Control prompt.

   Otherwise, if you have always-on Internet service, such as that provided by most cable providers, right-click the Cable Modem Connection icon that you renamed earlier, right-click it, select Properties, and confirm the User Account Control prompt.
4. Select the Sharing tab, and check Allow Other Network Users to Connect Through This Computer's Internet Connection. If a drop-down list labeled Home Network Connection is visible, select the network connection that corresponds to the LAN adapter that connects to your other computers, *not* the connection that goes to your DSL or cable modem. Click OK.
5. When the process finishes, you may close the Properties dialog.

Now other users should be able to connect to the Internet through the shared connection. If your Internet service is connection-based, on their Network Connections windows they should see an icon representing the shared connection. They can right-click this icon to establish or disconnect the Internet connection if necessary.

For one last setup step, see "After Setting Up a Shared Connection" at the end of the previous section.

Setting Up Remote Access to Your Computer

Appendix C provides detailed instructions for setting up remote access to your computer. Appendix C is available on the CD-ROM that accompanies this book and online at www.informit.com/title/9780789736956.

INDEX

SYMBOLS

NUMBERS

A

B

C

D

E

F

G

H

I

J - K

L

M

N

O

P

Q - R

S

T

U

V

W

X

Y - Z