CHAPTER 25

The Internet

In this chapter, you will learn how to

- Explain how the Internet works
- Connect to the Internet
- Use Internet software tools

Imagine coming home from a long day at work building and fixing PCs, sitting down in front of your shiny new computer, double-clicking the single icon that sits dead center on your monitor…and suddenly you're enveloped in an otherworldly scene, where 200-foot trees slope smoothly into snow-white beaches and rich blue ocean. Overhead, pterodactyls soar through the air while you talk to a small chap with pointy ears and a long robe about heading up the mountain in search of a giant monster.… TV show from the SciFi channel? Spielberg's latest film offering? How about an interactive game played by millions of people all over the planet on a daily basis by connecting to the Internet? If you guessed the last one, you're right.

This chapter covers the skills you need as a PC tech to help people connect to the Internet. It starts with a brief section on how the Internet works, along with the concepts of connectivity, and then it goes into the specifics on hardware, protocols, and software that you use to make the Internet work for you (or for your client). Let's get started!

Historical/Conceptual

How the Internet Works

Thanks to the Internet, people can communicate with one another over vast distances, often in the blink of an eye. As a PC tech, you need to know how PCs communicate with the larger world for two reasons. First, knowing the process and pieces involved in the communication enables you to troubleshoot effectively when that communication goes away. Second, you need to be able to communicate knowledgeably with a network technician who comes in to solve a more complex issue.

Internet Tiers

You probably know that the Internet is millions and millions of computers all joined together to form the largest network on earth, but not many folks know much about how these computers are organized. To keep everything running smoothly, the Internet is broken down into groups called *tiers*. The main tier, called *Tier 1*, consists of nine companies called *Tier 1 providers*. The Tier 1 providers own long-distance, high-speed fiber-optic networks called *backbones*. These backbones span the major cities of the earth (not all Tier 1 backbones go to all cities) and interconnect at special locations called *network access points* (*NAPs*). Anyone wishing to connect to any of the Tier 1 providers must pay large sums of money. The Tier 1 providers do not charge each other.

Tier 2 providers own smaller, regional networks and must pay the Tier 1 providers. Most of the famous companies that provide Internet access to the general public are Tier 2 providers. *Tier 3 providers* are even more regional and connect to Tier 2 providers.

The piece of equipment that makes this tiered Internet concept work is called a backbone router. *Backbone routers* connect to more than one other backbone router, creating a big, interwoven framework for communication. Figure 25-1 illustrates the decentralized and interwoven nature of the Internet. The key reason for interweaving the backbones of the Internet was to provide alternative pathways for data if one or more of the routers went down. If Jane in Houston sends a message to her friend Polly in New York City, for example, the shortest path between Jane and Polly in this hypothetical situation is this: Jane's message originates at Rice University in Houston, bounces to Emory University in Atlanta, flits through Virginia Commonwealth University in Richmond, and then zips into SUNY in New York City (Figure 25-2). Polly happily reads the message and life is great. The Internet functions as planned.

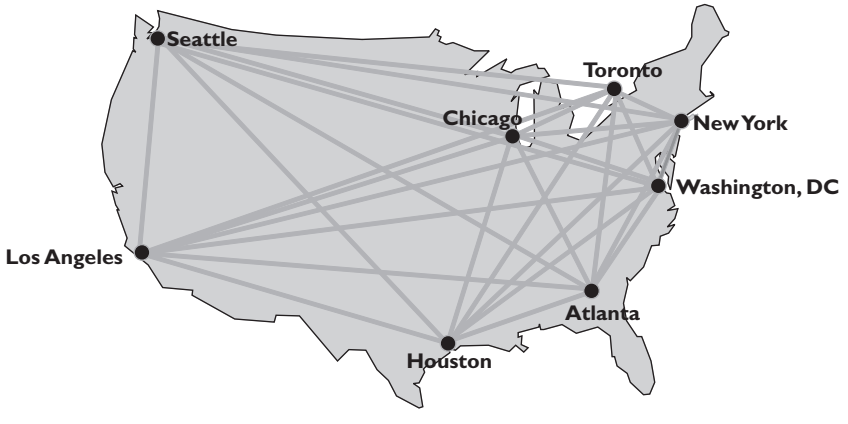


Figure 25-1 Internet Tier 1 connections

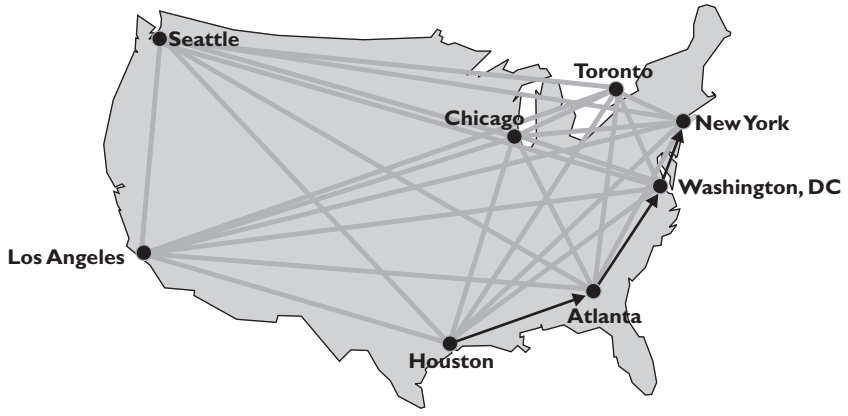


Figure 25-2 Message traveling from Houston to NYC

But what happens if the entire southeastern United States experiences a huge power outage and Internet backbones in every state from Virginia to Florida go down? Jane's message would bounce back to Rice and the Rice computers. Being smart cookies, the routers would reroute the message to nodes that still functioned—say, Rice to University of Chicago, to University of Toronto, and then to SUNY (Figure 25-3). It's all in a day's work for the highly redundant and adaptable Internet. At this point in the game (2009), the Internet simply cannot go down fully—barring, of course, a catastrophe of Biblical proportions.

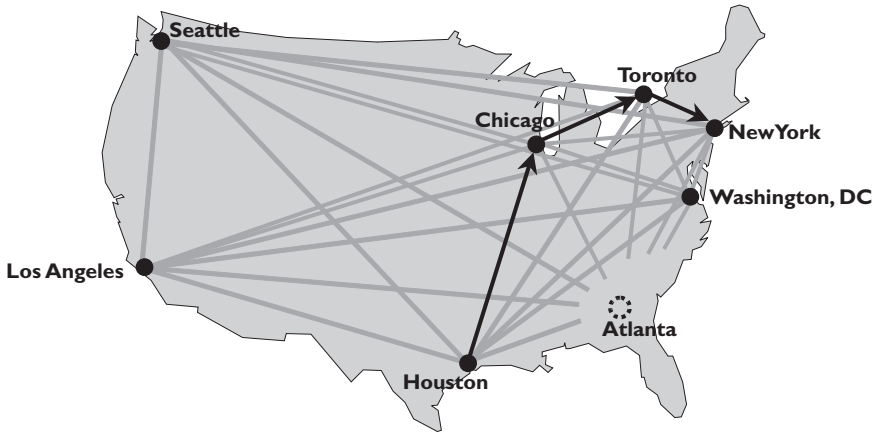


Figure 25-3 Rerouted message from Houston to NYC

TCP/IP—The Common Language of the Internet

As you know from all the earlier chapters in this book, hardware alone doesn't cut it in the world of computing. You need software to make the machines run and create an interface for humans. The Internet is no exception. TCP/IP provides the basic software structure for communication on the Internet.

Because you spent a good deal of Chapter 23, "Local Area Networking," working with TCP/IP, you should have an appreciation for its adaptability and, perhaps more importantly, its extendibility. TCP/IP provides the addressing scheme for computers that communicate on the Internet through IP addresses, such as 192.168.4.1 or 16.45.123.7. As a protocol, though, TCP/IP is much more than just an addressing system. TCP/IP provides the framework and common language for the Internet. And it offers a phenomenally wide-open structure for creative purposes. Programmers can write applications built to take advantage of the TCP/IP structure and features, creating what are called TCP/IP services. The cool thing about TCP/IP services is that they're limited only by the imagination of the programmers.

You'll learn much more about TCP/IP services in the software and "Beyond A+" sections of this chapter, but I must mention one service that you've most likely worked with yourself, whether you knew them by that term or not. The most famous service is the *Hypertext Transfer Protocol* (*HTTP*), the service that provides the structure for the *World Wide Web* ("the Web," for short), the graphical face of the Internet. Using your *Web browser*—a program specifically designed to retrieve, interpret, and display Web pages—an almost endless variety of information and entertainment is just a click away. I can't tell you how many times I've started to look up something on the Web, and suddenly it's two hours later and I still haven't looked up what I started out wanting to know, but I don't actually care, because I've learned some amazing stuff! But then when I do go look it up, in just minutes I can find information it used to take *days* to uncover. The Web can arguably claim the distinction of being both the biggest time-waster and the biggest time-saver since the invention of the book!

At this point, you have an enormous, beautifully functioning network. All the backbone routers connect with fiber and thick copper cabling backbones, and TCP/IP enables communication and services for building applications for humans to interface across the distances. What's left? Oh, that's right: how do you tap into this great network and partake of its goodness?

Internet Service Providers

Every Tier 1 and Tier 2 provider leases connections to the Internet to companies called *Internet service providers* (*ISPs*). ISPs essentially sit along the edges of the Tier 1 and Tier 2 Internet and tap into the flow. You can, in turn, lease some of the connections from the ISP and thus get on the Internet.

NOTE Microsoft calls the connections ISPs make to the Internet *access points*, which I think is a very bad name. You'd think we'd be able to come up with new terms for things! Instead, some folks in this industry continue rebranding things with the same phrases or catchwords, only serving to confuse already bewildered consumers.

ISPs come in all sizes. Comcast, the huge cable television provider, has multiple, huge-capacity connections into the Internet, enabling its millions of customers to connect from their local machines and surf the Web. Contrast Comcast with Unísono, an ISP in San Miguel de Allende, Mexico (Figure 25-4). Billed as the "Best Internet Service in San Miguel," it services only a small (but delightful) community and the busy tourist crowd.

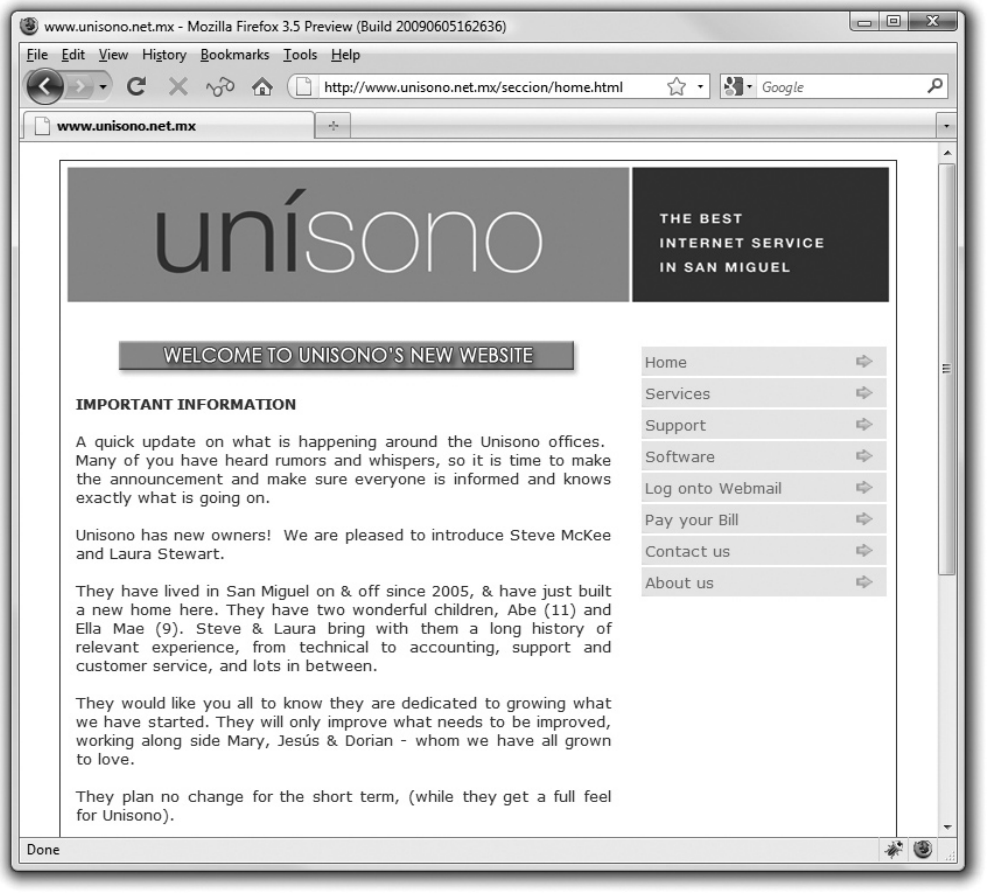


Figure 25-4 Unísono homepage

Connection Concepts

Connecting to an ISP requires two things to work perfectly: hardware for connectivity, such as a modem and a working cable line; and software, such as protocols to govern the connections and the data flow (all configured in Windows) and applications to take

advantage of the various TCP/IP services. Once you have a contract with an ISP to grant you access to the Internet, the ISP gives you TCP/IP configuration numbers and data so you can set up your software to connect directly to a router at the ISP that becomes your gateway to the Internet. The router to which you connect at the ISP, by the way, is often referred to as the *default gateway*. Once you configure your software correctly, you can connect to the ISP and get to the greater Internet. Figure 25-5 shows a standard PC-to-ISP-to-Internet connection. Note that various protocols and other software manage the connectivity between your PC and the default gateway.

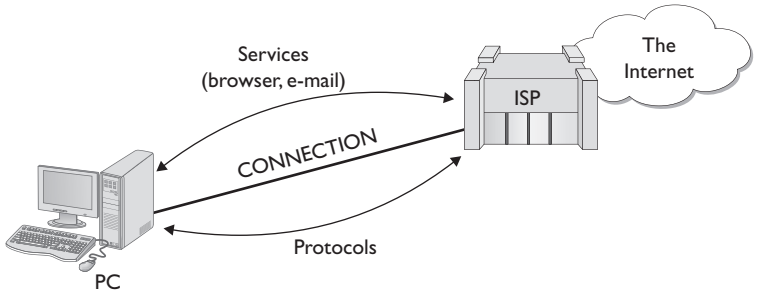


Figure 25-5 Simplified Internet connectivity

Essentials

Connecting to the Internet

PCs commonly connect to an ISP by using one of seven technologies that fit into four categories: dial-up, both analog and ISDN; dedicated, such as DSL, cable, and LAN; wireless; and satellite. Analog dial-up is the slowest of the bunch and requires a telephone line and a special networking device called a modem. ISDN uses digital dial-up and has much greater speed. All the others use a regular Ethernet NIC like you played with in Chapter 23, "Local Area Networking." Satellite is the odd one out here; it may use either a modem or a NIC, depending on the particular configuration you have, although most folks will use a NIC. Let's take a look at all these various connection options.

Dial-up

A dial-up connection to the Internet requires two pieces to work: hardware to dial the ISP, such as a modem or ISDN terminal adapter; and software to govern the connection, such as Microsoft's *Dial-up Networking* (*DUN*). Let's look at the hardware first, and then we'll explore software configuration.

Modems

At some point in the early days of computing, some bright guy or gal noticed a colleague talking on a telephone, glanced down at a PC, and then put two and two together: why not use telephone lines for data communication? The basic problem with this

idea is that traditional telephone lines use analog signals, while computers use digital signals (Figure 25-6). Creating a dial-up network required equipment that could turn digital data into an analog signal to send it over the telephone line, and then turn it back into digital data when it reached the other end of the connection. A device called a modem solved this dilemma.

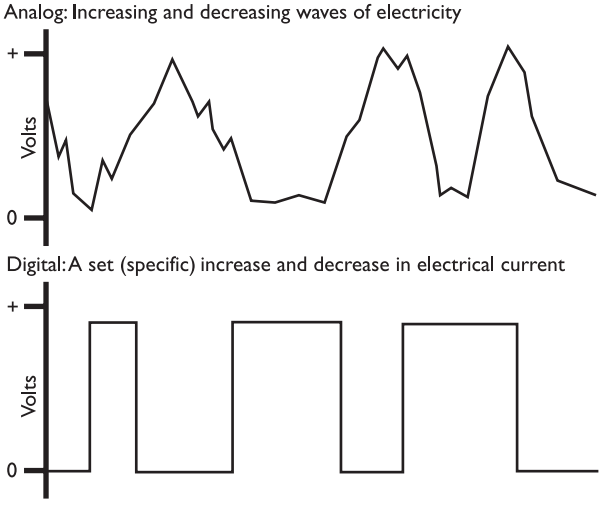


Figure 25-6 Analog signals used by a telephone line versus digital signals used by the computer

Modems enable computers to talk to each other via standard commercial telephone lines by converting analog signals to digital signals, and vice versa. The term *modem* is short for modulator/demodulator, a description of transforming the signals. Telephone wires transfer data via analog signals that continuously change voltages on a wire. Computers hate analog signals. Instead, they need digital signals, voltages that are either on or off, meaning the wire has voltage present or it does not. Computers, being binary by nature, use only two states of voltage: zero volts and positive volts. Modems take analog signals from telephone lines and turn them into digital signals that the PC can understand (Figure 25-7). Modems also take digital signals from the PC and convert them into analog signals for the outgoing telephone line.

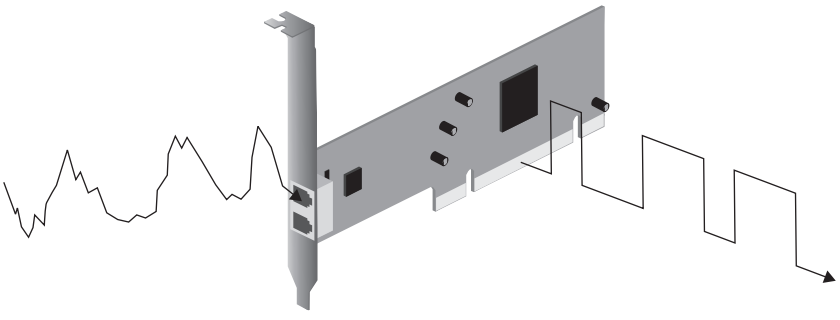
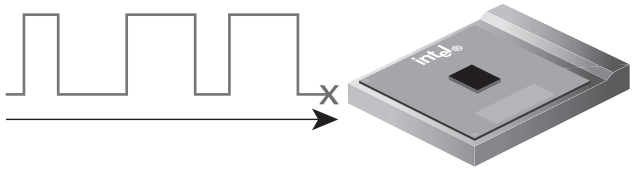


Figure 25-7 Modem converting analog signal to digital signal

A modem does what is called *serial communication*: It transmits data as a series of individual ones and zeroes. The CPU can't process data this way. It needs parallel communication, transmitting and receiving data in discrete 8-bit chunks (Figure 25-8). The individual serial bits of data are converted into 8-bit parallel data that the PC can understand through the *universal asynchronous receiver/transmitter* (*UART*) chip (Figure 25-9).

Figure 25-8 CPUs can't read serial data.



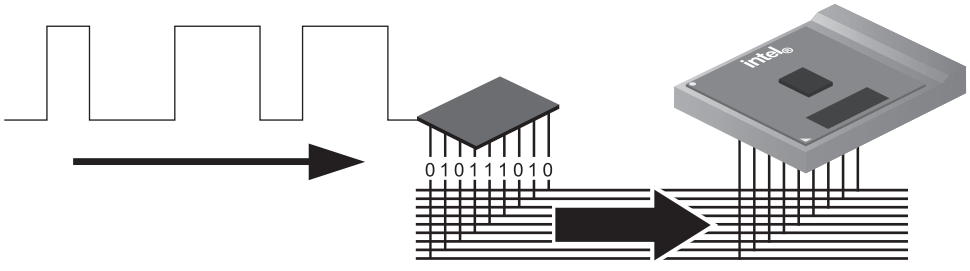


Figure 25-9 The UART chip converts serial data to parallel data that the CPU can read.

There are many types of UARTs, each with different functions. All serial communication devices are really little more than UARTs. *External* modems can convert analog signals to digital ones and vice versa, but they must rely on the serial ports to which they're connected for the job of converting between serial and parallel data (Figure 25-10). Internal modems can handle both jobs because they have their own UART built in (Figure 25-11).

Phone lines have a speed based on a unit called a *baud*, which is one cycle per second. The fastest rate that a phone line can achieve is 2,400 baud. Modems can pack multiple bits of data into each baud; a 33.6 kilobits per second (Kbps) modem, for example, packs 14 bits into every baud: 2,400 × 14 = 33.6 Kbps. Thus, it is technically incorrect to say, "I have a 56 K baud modem." The correct statement is, "I have a 56 Kbps modem." But don't bother; people have used the term "baud" instead of *bits per second* (*bps*) so often for so long that the terms have become functionally synonymous.

Modern Modem Standards: V.90 versus V.92 The fastest data transfer speed a modem can handle is based on its implementation of one of the international standards for modem technology: the *V standards*. Set by the International Telecommunication Union (ITU), the current top standards are V.90 and V.92. Both standards offer

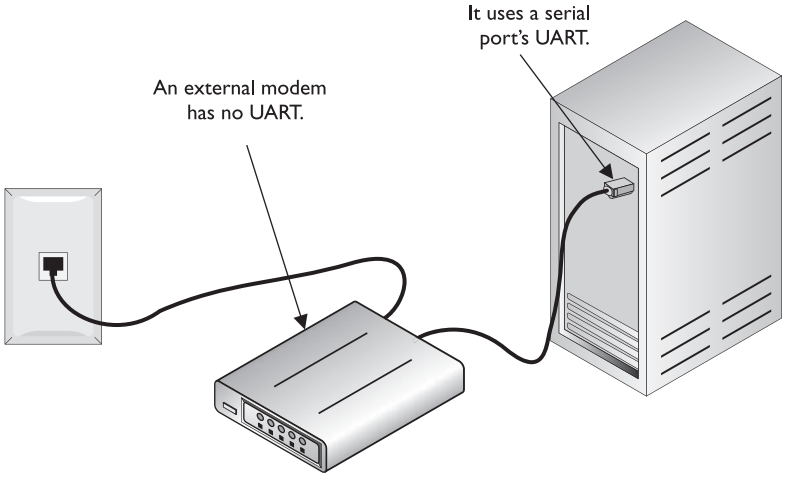


Figure 25-10 An external modem uses the PC's serial port.

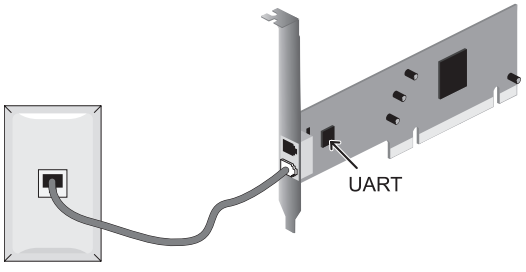


Figure 25-11 An internal modem has UART built in.

download speeds of just a hair under 56 Kbps, but they differ in upload speeds: up to 33.6 Kbps for V.90, and up to 48 Kbps for V.92 modems. To get anywhere near the top speeds of a V.90 or V.92 modem requires a comparable modem installed on the other line and connecting telephone lines in excellent condition. In practice, you'll rarely get faster throughput than about 48 Kbps for downloads and 28 Kbps for uploads.

Flow Control (Handshaking) Flow control, also known as *handshaking*, is the process by which two serial devices verify a conversation. Imagine people talking on a CB radio. When one finishes speaking, he will say "over." That way the person listening can be sure that the sender is finished speaking before she starts. Each side of the conversation is verified. During a file transfer, two distinct conversations take place that require flow control: local (between modem and COM port) and end-to-end (between modems).

The modems themselves handle end-to-end flow control. PCs can do local flow control between the modem and COM port in two ways: hardware and software. Hardware flow control employs extra wires in the serial connection between the modem and the COM port to let one device tell the other that it is ready to send or receive data. These extra wires are called *ready to send* (*RTS*) and *clear to send* (*CTS*), so hardware

handshaking is often called RTS/CTS. Software flow control uses a special character called XON to signal that data flow is beginning, and another special character called XOFF to signal that data transmission is finished; therefore, software handshaking is often called XON/XOFF. Software handshaking is slower and not as dependable as hardware handshaking, so you rarely see it.

Bells and Whistles Although the core modem technology has changed little in the past few years, modem manufacturers have continued to innovate on many peripheral fronts—pardon the pun and the bad grammar. You can walk into a computer store nowadays, for example, and buy a V.92 modem that comes bundled with an excellent fax machine and a digital answering machine. You can even buy modems that you can call remotely that will wake up your PC (Figure 25-12). What will they think up next?

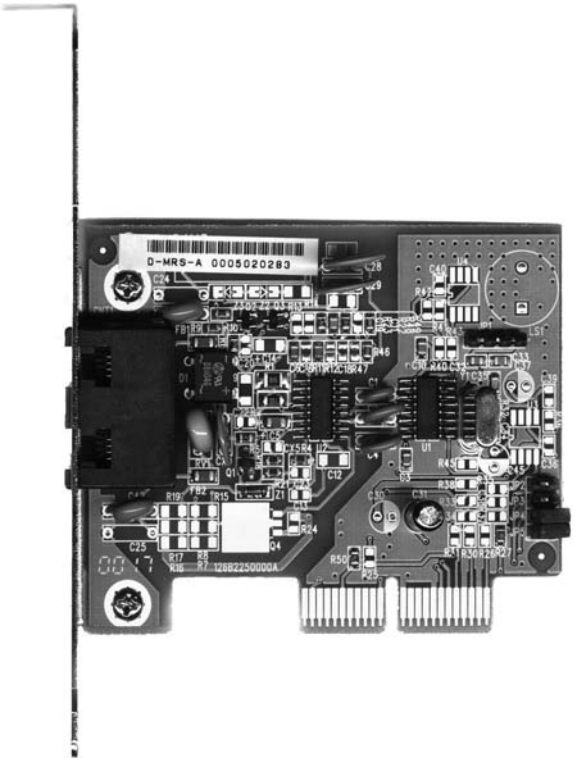
Figure 25-12 Some of the many features touted by the manufacturer of the SupraMax modem

NOTE You can test a modem by plugging in a physical device called a *loopback plug*, and then run diagnostics.

Modem Connections Internal modems connect to the PC very differently than external modems. Almost all internal modems connect to a PCI or PCI Express expansion bus slot inside the PC, although cost-conscious manufacturers may use smaller modems that fit in special expansion slots designed to support multiple communications features such as modems, NICs, and sound cards (Figure 25-13). Older AMD motherboards used Audio/Modem Riser (AMR) or Advanced Communication Riser (ACR) slots, while Intel motherboards used Communication and Networking Riser (CNR) slots.

NOTE AMR, ACR, and CNR slots have gone away, though you'll still find them on older systems. Current systems use built-in components or PCIe ×1 slots for modems, sound, and NICs.

Figure 25-13
A CNR modem



External modems connect to the PC through an available serial port (the old way) or USB port (Figure 25-14). Many older PCs came with 9-pin serial ports, whereas most external modems designed to connect to a serial port come with a 25-pin connector. That means you will probably need a 9-to-25-pin converter, available at any computer store, to connect your external modem. Serial ports are now quite rare as virtually all computers today have two or more USB ports.

Figure 25-14
A USB modem

Don't fret about USB versus serial for your modem connection, as the very low speeds of data communication over a modem make the physical type of the connection unimportant. Even the slow, aging serial interface more than adequately handles 56 Kbps data transfers. If you have the option, choose a USB modem, especially one with a volume control knob. USB offers simple plug and play and easy portability between machines, plus such modems require no external electrical source, getting all the power they need from the USB connection.

Dial-up Networking

The software side of dial-up networks requires configuration within Windows to include information provided by your ISP. The ISP provides a dial-up telephone number or numbers, as well as your user name and initial password. In addition, the ISP will tell you about any special configuration options you need to specify in the software setup. The full configuration of dial-up networking is beyond the scope of this book, but you should at least know where to go to follow instructions from your ISP. Let's take a look at the Network and Internet Connections applet in Windows XP.

Network Connections To start configuring a dial-up connection in Windows XP, open the Control Panel. Select Network and Internet Connections from the Pick a category menu and then choose *Set up or change your Internet connection* from the Pick a task menu The Internet Properties dialog box opens with the Connections tab displayed (Figure 25-15). All your work will proceed from here.

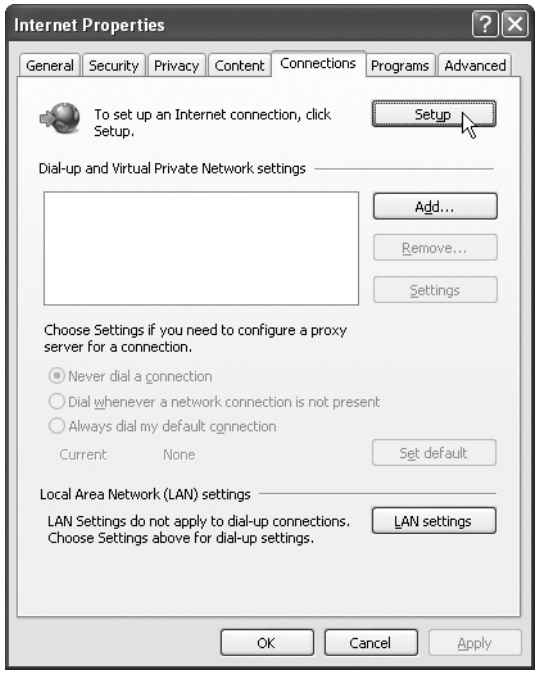


Figure 25-15 The Connections tab in the Internet Properties dialog box

Click the Setup button to run the New Connection Wizard (Figure 25-16), and then work through the screens. At this point, you're going to need information provided by your ISP to configure your connection properly. When you finish the configuration, you'll see a new Connect To option on the Start menu if your system is set up that way. If not, open up Network Connections, and your new dial-up connection will be available. Figure 25-17 shows the option to connect to a fictitious ISP, Cool-Rides.com.

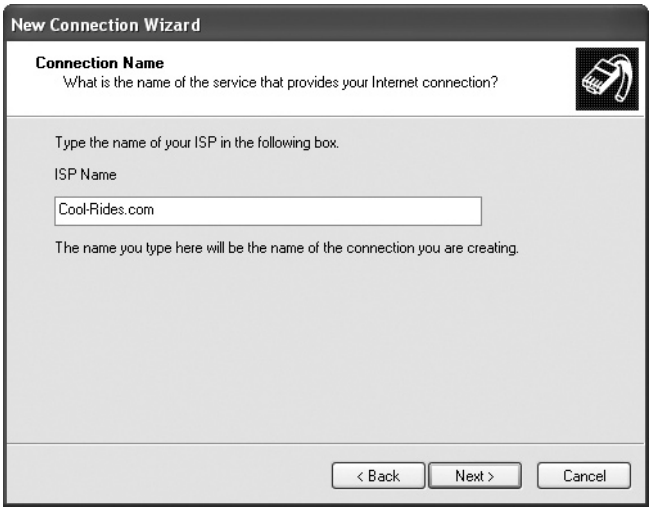


Figure 25-16 The New Connection Wizard

Figure 25-17 Connection options in Network Connections

PPP Dial-up links to the Internet have their own special hardware protocol called *Point-to-Point Protocol* (*PPP*). PPP is a streaming protocol developed especially for dial-up Internet access. To Windows, a modem is nothing more than a special type of network adapter. Modems have their own configuration entry in the Network Connections applet.

Most dial-up "I can't connect to the Internet"–type problems are user errors. Your first area of investigation is the modem itself. Use the modem's properties to make sure the volume is turned up. Have the user listen to the connection. Does she hear a dial tone? If she doesn't, make sure the modem's line is plugged into a good phone jack. Does she hear the modem dial and then hear someone saying, "Hello? Hello?" If so, she probably dialed the wrong number! Wrong password error messages are fairly straightforward—remember that the password may be correct but the user name may be wrong. If she still fails to connect, it's time to call the network folks to see what is not properly configured in the Dial-up Networking settings.

ISDN

A standard telephone connection comprises many pieces. First, the phone line runs from your phone out to a network interface box (the little box on the side of your house) and into a central switch belonging to the telephone company. (In some cases, intermediary steps are present.) Standard metropolitan areas have a large number of central offices, each with a central switch. Houston, Texas, for example, has nearly 100 offices in the general metro area. These central switches connect to each other through high-capacity *trunk lines*. Before 1970, the entire phone system was analog; over time, however, phone companies began to upgrade their trunk lines to digital systems. Today, the entire telephone system, with the exception of the line from your phone to the central office, and sometimes even that, is digital.

During this upgrade period, customers continued to demand higher throughput from their phone lines. The old telephone line was not expected to produce more than 28.8 Kbps (56 K modems, which were a *big* surprise to the phone companies, didn't appear until 1995). Needless to say, the phone companies were very motivated to come up with a way to generate higher capacities. Their answer was actually fairly straightforward: make the entire phone system digital. By adding special equipment at the central office and the user's location, phone companies can now achieve a throughput of up to 64 K per line (see the paragraphs following) over the same copper wires already used by telephone lines. This process of sending telephone transmission across fully digital lines end-to-end is called *integrated services digital network* (*ISDN*) service.

ISDN service consists of two types of channels: Bearer, or B, channels and Delta, or D, channels. B channels carry data and voice information at 64 Kbps. D channels carry setup and configuration information and carry data at 16 Kbps. Most providers of ISDN allow the user to choose either one or two B channels. The more common setup is two B/one D, usually called a *basic rate interface* (*BRI*) setup. A BRI setup uses only one physical line, but each B channel sends 64 K, doubling the throughput total to 128 K. ISDN also connects much faster than modems, eliminating that long, annoying, mating call you get with phone modems. The monthly cost per B channel is slightly more than a regular phone line, and usually a fairly steep initial fee is levied

for the installation and equipment. The big limitation is that you usually need to be within about 18,000 feet of a central office to use ISDN.

The physical connections for ISDN bear some similarity to analog modems. An ISDN wall socket usually looks something like a standard RJ-45 network jack. The most common interface for your computer is a device called a *terminal adapter* (*TA*). TAs look much like regular modems, and like modems, they come in external and internal variants. You can even get TAs that are also hubs, enabling your system to support a direct LAN connection.

NOTE Another type of ISDN, called a primary rate interface (PRI), is composed of twenty-three 64-Kbps B channels and one 64-Kbps D channel, giving it a total throughput of 1.5 megabits per second. PRI ISDN lines are also known as T1 lines.

DSL

Digital subscriber line (*DSL*) connections to ISPs use a standard telephone line but special equipment on each end to create always-on Internet connections at blindingly fast speeds, especially when compared with analog dial-up connections. Service levels vary around the United States, but the typical upload speed is ~768 Kbps, while download speed comes in at a very sweet ~3+ Mbps!

NOTE The two most common forms of DSL you'll find are *asynchronous (ADSL)* and *synchronous (SDSL)*. ADSL lines differ between slow upload speed (such as 384 Kbps, 768 Kbps, and 1 Mbps) and faster download speed (usually 3–7 Mbps). SDSL has the same upload and download speeds, but telecom companies charge a lot more for the privilege. DSL encompasses many such variations, so you'll often see it referred to as xDSL.

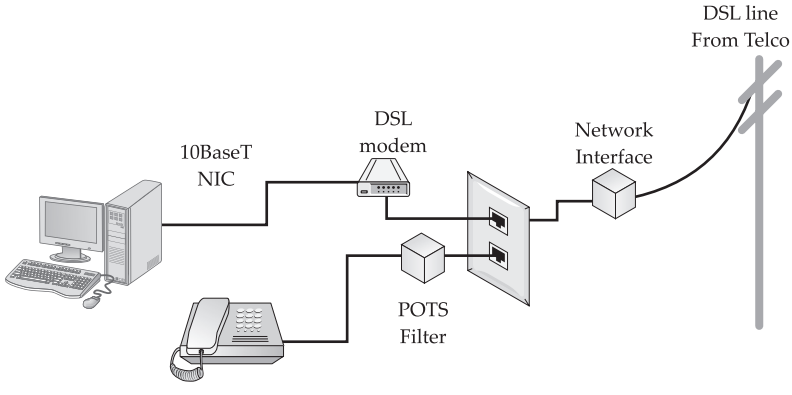
DSL requires little setup from a user standpoint. A tech comes to the house to install the DSL receiver, often called a DSL modem (Figure 25-18), and possibly hook up a wireless router. The receiver connects to the telephone line and the PC (Figure 25-19). The tech (or the user, if knowledgeable) then configures the DSL modem and router (if there is one) with the settings provided by the ISP, and that's about it! Within moments, you're surfing at blazing speeds. You don't need a second telephone line. You don't need to wear a special propeller hat or anything. The only kicker is that your house has to be within a fairly short distance from a main phone service switching center, something like 18,000 feet.

Cable

Cable offers a different approach to high-speed Internet access, using regular cable TV cables to serve up lightning-fast speeds. It offers faster service than most DSL connections, with a 1–10 Mbps upload and 6–50+ Mbps download. Cable Internet connections are theoretically available anywhere you can get cable TV.

Figure 25-18
A DSL receiver

Figure 25-19
DSL connections



Cable Internet connections start with an RG-6 or RG-59 cable coming into your house. The cable connects to a cable modem that then connects to a NIC in your PC via UTP Ethernet cable. Figure 25-20 shows a typical cable setup. One nice advantage of cable over DSL is that if you have a TV tuner card in your PC, you can use the same cable connection (with a splitter) to watch TV on your PC. Both DSL and cable modem Internet connections can be used by two or more computers if they are part of a LAN, including those in a home.

NOTE The term *modem* has been warped and changed beyond recognition in modern networking. Both DSL and cable fully digital Internet connections use the term *modem* to describe the box that takes the incoming signal from the Internet and translates it into something the PC can understand.

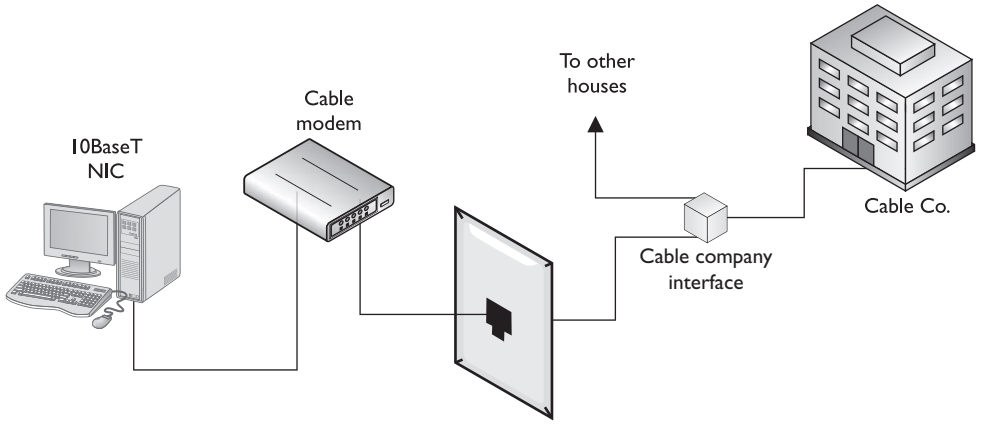


Figure 25-20 Cable connections

LAN

Most businesses connect their internal local area network (LAN) to an ISP via some hardware solution that Network+ techs deal with. Figure 25-21 shows a typical small-business wiring closet with routers that connect the LAN to the ISP. You learned all about wiring up a LAN in Chapter 23, "Local Area Networking," so there's no need to go through any basics here. To complete a LAN connection to the Internet, you need to add a second NIC or a modem to one of the PCs and then configure that PC as the default connection. We'll revisit this idea in a moment with Internet Connection Sharing.

Wireless

Every once in a while a technology comes along that, once the kinks are smoothed out, works flawlessly, creating a magical computing experience. Unfortunately, the various wireless networking technologies out there today don't fulfill that dream yet. When they work, it's like magic. You walk into a coffee shop, sit down, and flip open your laptop computer. After firing up your Internet browser, suddenly you're quaffing lattes and surfing Web sites—with no wires at all.

Suffice it to say that connecting to the Internet via wireless means that you must connect to a cellular network or to a LAN that's wired to an ISP. The local Internet café purchases high-speed Internet service from the cable or telecom company, for example, and then connects a wireless access point (WAP) to its network. When you walk in with your portable PC with wireless NIC and open a Web browser, the wireless NIC communicates with the *fully wired* DHCP server via the WAP and you're surfing on the Internet. It appears magically wireless, but the LAN to ISP connection still uses wires.

Cellular networking is even more seamless. Anywhere you can connect with your cell phone, you can connect with your cellular network–aware portable or laptop computer.

Figure 25-21
A wiring closet

NOTE One form of wireless communication does not require local wires. For *Wireless broadband*, the ISP must put up a tower, and then any building within the line of sight (perhaps up to 10 miles) can get a high-speed connection.

Satellite

Satellite connections to the Internet get the data beamed to a satellite dish on your house or office; a receiver handles the flow of data, eventually sending it through an Ethernet cable to the NIC in your PC. I can already sense people's eyebrows raising. "Yeah, that's the download connection. But what about the upload connection?" Very

astute, me hearties! The early days of satellite required you to connect via a modem. You would upload at the slow 26- to 48-Kbps modem speed, but then get super-fast downloads from the dish. It worked, so why complain? You really can move to that shack on the side of the Himalayas to write the great Tibetan novel and still have DSL- or cable-speed Internet connectivity. Sweet!

Satellite might be the most intriguing of all the technologies used to connect to the Internet today. As with satellite television, though, you need to have the satellite dish point at the satellites (toward the south if you live in the United States). The only significant issue to satellite is that the distance the signal must travel creates a small delay called the *satellite latency*. This latency is usually unnoticeable unless the signal degrades in foul weather such as rain and snow.

Windows Internet Connection Sharing

Internet Connection Sharing (*ICS*) enables one system to share its Internet connection with other systems on the network, providing a quick and easy method for multiple systems to use one Internet connection. Modern Windows versions (Windows 2000 through Windows 7) also provide this handy tool. Figure 25-22 shows a typical setup for ICS. Note the terminology used here. The PC that connects to the Internet and then shares that connection via ICS with other machines on a LAN is called the *ICS host* computer. PCs that connect via LAN to the ICS host computer are simply called client computers.

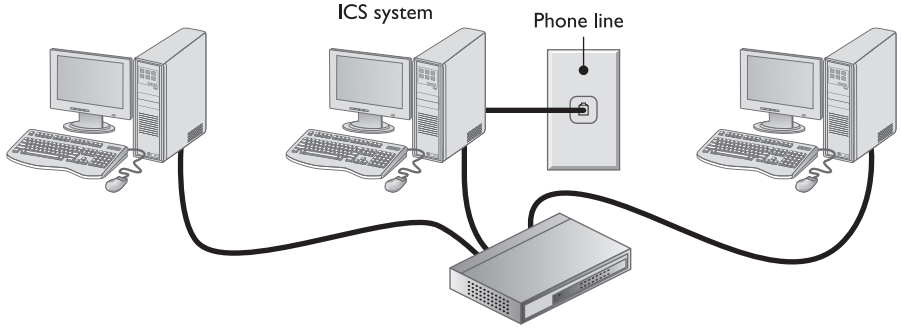


Figure 25-22 Typical ICS setup

To connect multiple computers to a single ICS host computer requires several things in place. First, the ICS host computer has to have a NIC dedicated to the internal connections. If you connect via dial-up, for example, the ICS host computer uses a modem to connect to the Internet. It also has a NIC that plugs into a switch. Other PCs on the LAN likewise connect to the switch. If you connect via some faster service, such as DSL that uses a NIC cabled to the DSL receiver, you'll need a second NIC in the ICS host machine to connect to the LAN and the client computers.

Setting up ICS in Windows is very simple. If you are using Windows 2000 or XP, open the properties dialog for My Network Places. If you are using Windows Vista or 7, open the Network and Sharing Center and click on *Manage network connections* (Vista) or *Change adapter settings* (7) in the left-hand task list. Now access the properties of the connection you wish to share.

Click the Sharing tab (Windows 2000, Vista, and 7) or the Advanced tab (Windows XP), and select *Enable Internet connection sharing for this connection* (Windows 2000) or *Allow other network users to connect through this computer's Internet connection* (Windows XP–7, Figure 25-23). Clients don't need any special configuration but should simply be set to DHCP for their IP address and other configurations.

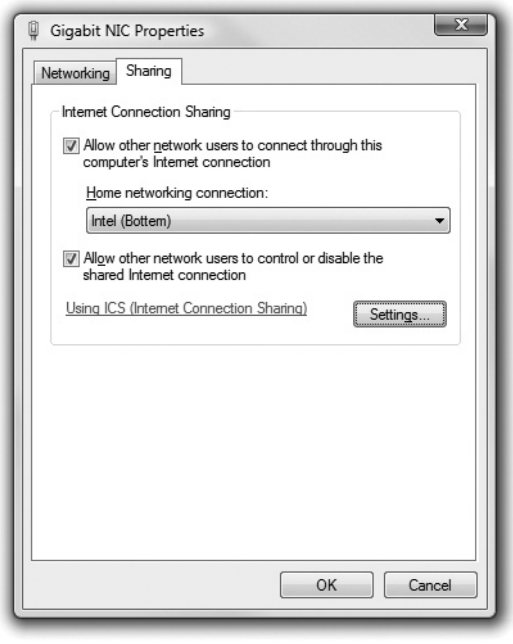


Figure 25-23 Enabling Internet Connection Sharing in Windows Vista

Hardware Connection Sharing

Although Windows Internet Connection Sharing works, it has a major drawback—you must leave the computer running all the time so the other computers on the network can access the Internet. This is where the small home router fits perfectly. Several manufacturers offer robust, easy-to-configure routers that enable multiple computers to connect to a single Internet connection. These boxes require very little configuration and provide firewall protection between the primary computer and the Internet, which you'll learn more about in Chapter 26, "Securing Computers." All it takes to install one of these routers is simply to plug your computer into any of the LAN ports on the back, and then to plug the cable from your Internet connection into the port labeled Internet or WAN.

A great example of a home router is the Linksys WRT54G (Figure 25-24). This little DSL/cable router, for example, has four 10/100 Ethernet ports for the LAN computers,

Figure 25-24
Common home router with Wi-Fi

and a WiFi radio for any wireless computers you may have. The Linksys, like all home routers, uses a technology called *Network Address Translation*, or *NAT* for short. NAT performs a little network subterfuge: it presents an entire LAN of computers to the Internet as a single machine. It effectively hides all of your computers and makes them appear invisible to other computers on the Internet. All anyone on the Internet sees is your *public* IP address. This is the address your ISP gives you, while all the computers in your LAN use private addresses that are invisible to the world. NAT therefore acts as a firewall, protecting your internal network from probing or malicious users from the outside.

Basic Router Configuration

These small routers require very little in the way of configuration if all you need is basic Internet connection sharing. In some cases, though, you may have to deal with a more complex network that requires changing the router's settings. The vast majority of these routers have built-in configuration Web pages that you access by typing the router's IP address into a browser. The address varies by manufacturer, so check the router's documentation. If you typed in the correct address, you should then receive a prompt for a user name and password, as in Figure 25-25. As with the IP address, the default user name and password change depending on the model/manufacturer. Once you enter the correct credentials, you will be greeted by the router's configuration page (Figure 25-26). From these pages, you can change any of the router's settings. Now look at a few of the basic settings that CompTIA wants you to be familiar with.

Figure 25-25 Router asking for user name and password

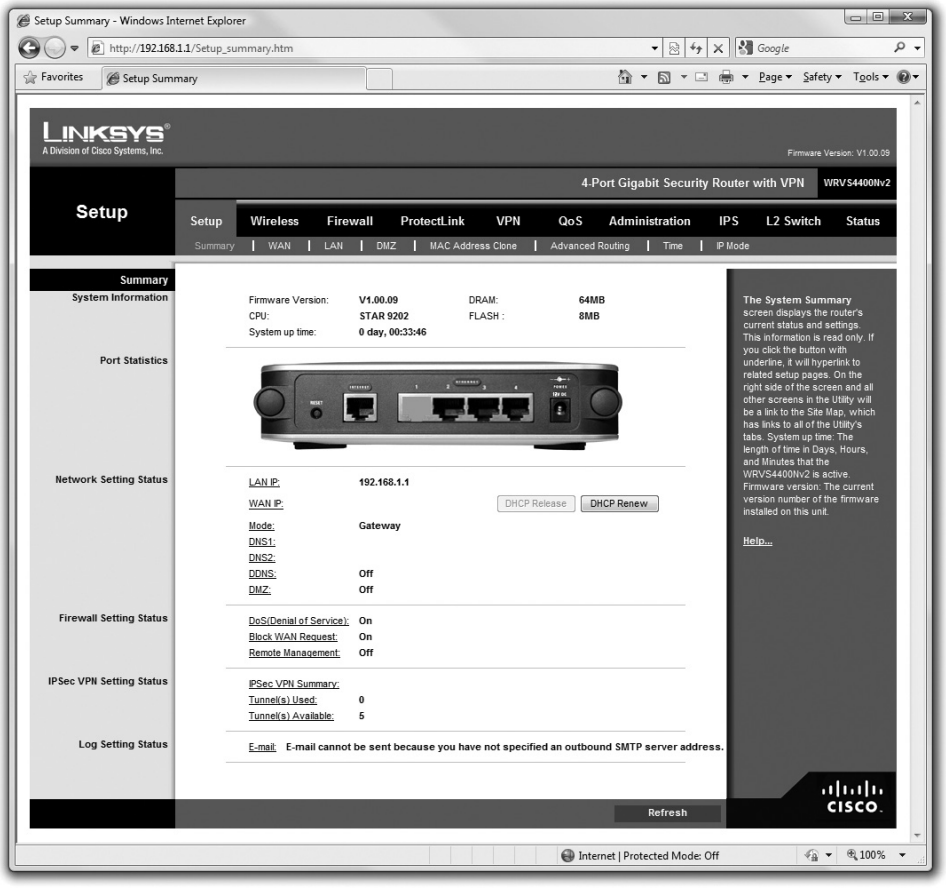


Figure 25-26 Configuration home page

Changing User Name and Password One of the first changes you should make to your router after you have it working is to change the user name and password to something other than the default. This is especially important if you have open wireless turned on, which you'll recall from Chapter 24, "Wireless Networking." If you leave the default user name and password, anyone who has access to your LAN can easily gain access to the router and change its settings. Fortunately, router manufacturers make it easy to change a router's login credentials. On this Linksys of mine, for example, I just click on the Administration tab and fill in the appropriate boxes as shown in Figure 25-27.

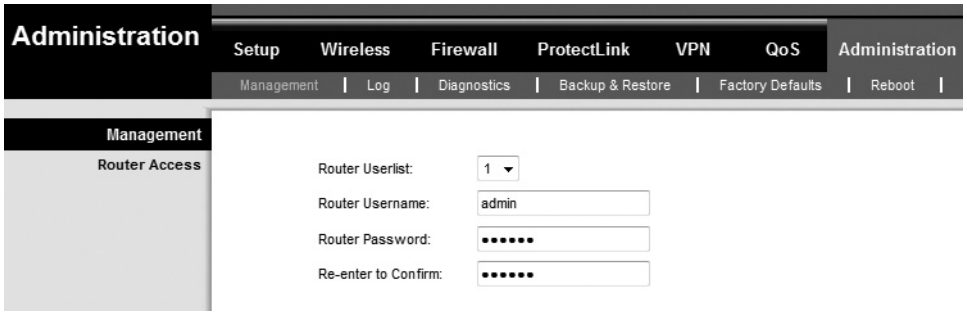


Figure 25-27 Changing the username and password

Disabling DHCP If you are configuring a router for a small office, the router's built-in DHCP server might conflict with a domain controller on your network. These conflicts, although not dangerous, can cause a lot of frustration and shouting as everyone's network connections stop working. To avoid this blow to inter-office relations, you should disable the DHCP server in the router before you plug it into the network. To do this, use a separate computer such as a laptop, or unplug your computer from the wall and plug it into the new router to log in. Once on the configuration screen, you will see a configuration page similar to the one in Figure 25-28.

CAUTION Once the DHCP server is disabled, the router will no longer hand out IP addresses, so you must make sure that the router's IP address is in the correct subnet of your office's LAN. If it isn't, you need to change it before you disable DHCP.

On my router, all that is needed it to enter the new address and subnet at the top of the screen shown in Figure 25-28. If you are unsure what address you need, ask your network administrator or CompTIA Network+ tech. Once you have the router's IP address taken care of, all you need to do is click the Disable radio button and save the settings. Now you can safely plug your router into the LAN without risking the ire of Internet-less coworkers.

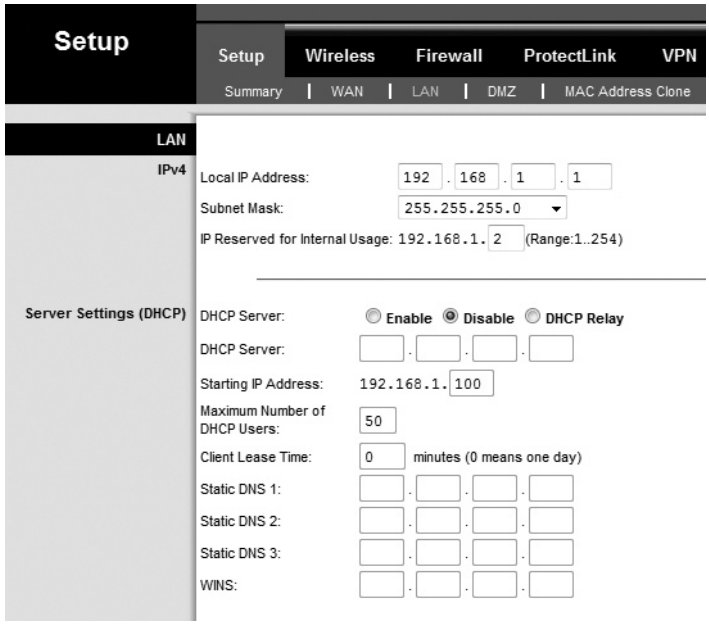


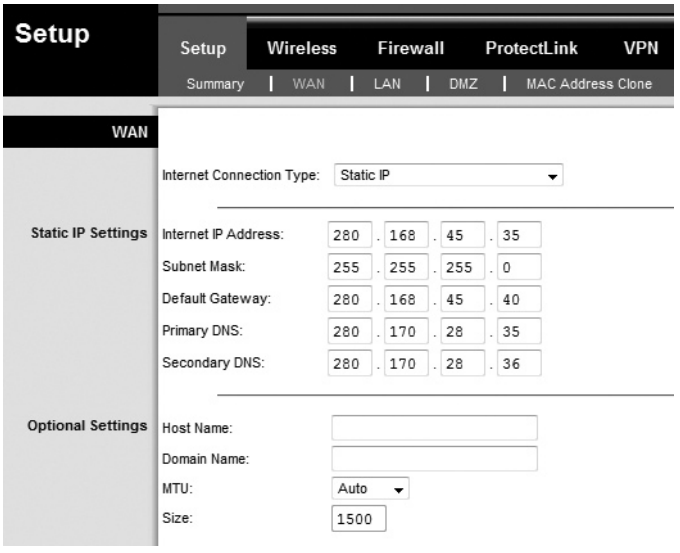
Figure 25-28 Configuring DHCP server

Setting Static IP Addresses With that all taken care of, let's look at setting up the router to use a static IP address for the Internet or WAN connection. In most cases, when you plug in the router's Internet connection, it receives an IP address using DHCP just like any other computer. Of course, this means that your Internet IP address will change from time to time, which can be a bit of a downside. This does not affect most people, but for some home users and businesses, it can present a problem. To solve this problem, most ISPs enable you to order a static IP. Once your ISP has allocated you a static IP address, you must manually enter it into your router. You do this the same way as all the previous changes you've just looked at. My router has a WAN configuration tab where I can enter all the settings that my ISP has provided me (Figure 25-29). Remember, you must change your connection type from Automatic/DHCP to Static IP to enter the new addresses.

Updating Firmware

Routers are just like any other computer in that they run software—and software has bugs, vulnerabilities, and other issues that sometimes require updating. The router manufacturers call these "firmware updates" and make them available on their Web sites for easy download. To update a modern router, you simply have to download the latest firmware from the manufacturer's Web site to your computer. Then you enter the router's configuration Web page and find the firmware update screen. On my router, it looks like Figure 25-30. From here, just follow the directions and click Update. A quick word of caution: Unlike a Windows update, a firmware update gone bad can *brick* your router. In other words, it can destroy the hardware and make it as useful as a brick sitting on your desk. This rarely happens, but you should keep it in mind when doing a firmware update.

Figure 25-29
Entering a static IP address



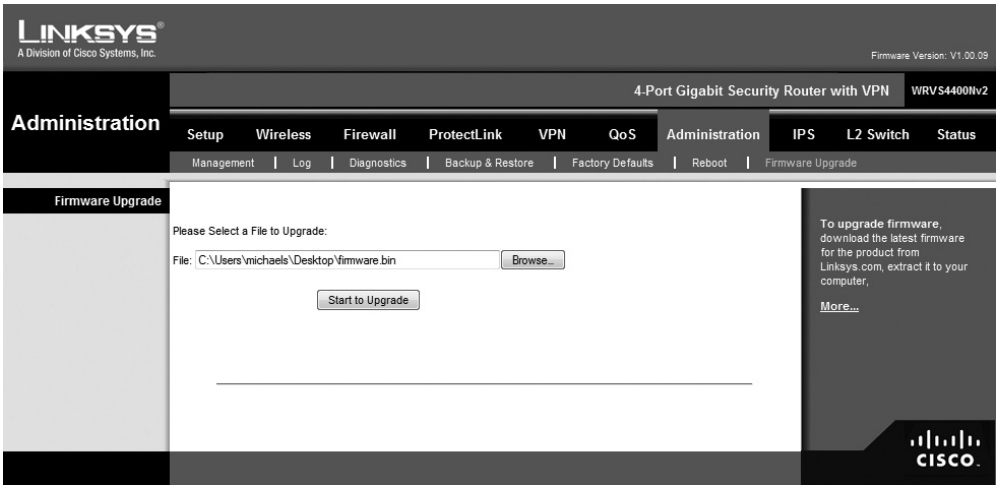


Figure 25-30 Firmware update page

Internet Software Tools

Once you've established a connection between the PC and the ISP, you can do nothing on the Internet without applications designed to use one or more TCP/IP services, such as Web browsing and e-mail. TCP/IP has the following commonly used services:

- World Wide Web (HTTP and HTTPS)
- E-mail (POP and SMTP)

- Newsgroups
- FTP
- Telnet
- VoIP

Each of these services (sometimes referred to by the overused term *TCP/IP protocols*) operates by using defined ports, requires a special application, and has special settings. You'll look at all eight of these services and learn how to configure them. As a quick reference, Table 25-1 has some common port numbers CompTIA would like you to know.

Table 25-1 TCP/IP Service Port Numbers

TCP/IP Service	Port Number
HTTP	80
HTTPS	443
FTP	20, 21
POP	110
SMTP	25
TELNET	23

The World Wide Web

The Web provides a graphical face for the Internet. *Web servers* (servers running specialized software) provide Web sites that you access by using the HTTP protocol on port 80 and thus get more or less useful information. Using Web-browser software, such as Internet Explorer or Mozilla Firefox, you can click a link on a Web page and be instantly transported—not just to some Web server in your home town—to anywhere in the world. Figure 25-31 shows Firefox at the home page of my company's Web site, www.totalsem.com. Where is the server located? Does it matter? It could be in a closet in my office or on a huge clustered server in Canada. The great part about the Web is that you can get from here to there and access the information you need with a click or two of the mouse.

Although the Web is the most popular part of the Internet, setting up a Web browser takes almost no effort. As long as the Internet connection is working, Web browsers work automatically. This is not to say you can't make plenty of custom settings, but the default browser settings work almost every time. If you type in a Web address, such as the best search engine on the planet—www.google.com—and it doesn't work, check the line and your network settings and you'll figure out where the problem is.

Configuring the Browser

Web browsers are highly configurable. On most Web browsers, you can set the default font size, choose whether to display graphics, and adjust several other settings. Although all Web browsers support these settings, where you go to make these changes

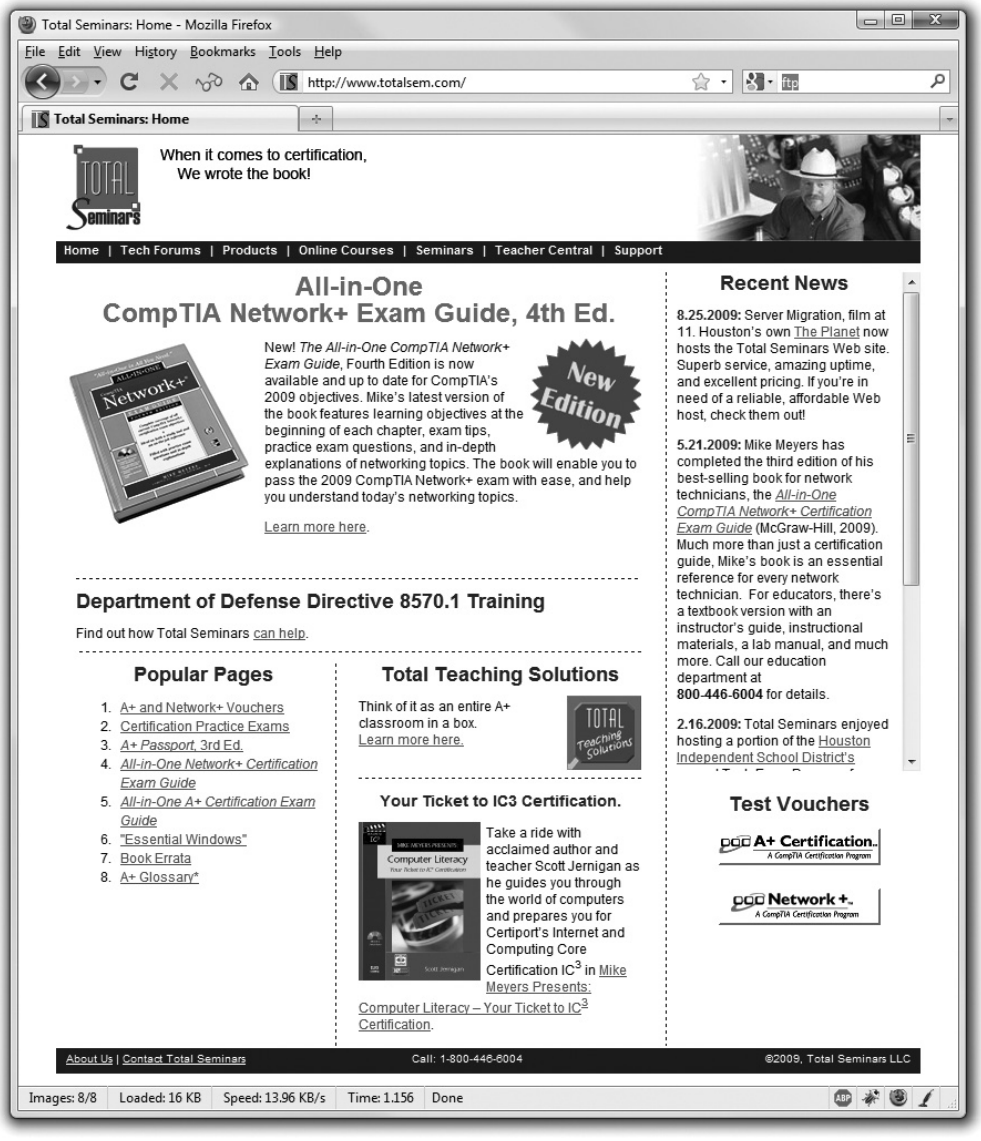


Figure 25-31 Mozilla Firefox showing a Web page

varies dramatically. If you are using the popular Internet Explorer that comes with Windows, you will find configuration tools in the Internet Options Control Panel applet or under the Tools menu.

Proxy Server Many corporations use a *proxy server* to filter employee Internet access, and when you're on their corporate network you have to set your proxy settings

within the Web browser (and any other Internet software you want to use). A *proxy server* is software that enables multiple connections to the Internet to go through one protected PC, much as ICS works on a home network. Unlike ICS, which operates transparently to the client PCs by manipulating IP packets (we say that it operates at Layer 3—the Network layer in the OSI model—see Chapter 23, "Local Area Networking"), proxy servers communicate directly with the browser application (operating at Layer 7, the Application layer). Applications that want to access Internet resources send requests to the proxy server instead of trying to access the Internet directly, both protecting the client PCs and enabling the network administrator to monitor and restrict Internet access. Each application must therefore be configured to use the proxy server. To configure proxy settings in Internet Explorer, choose Tools | Internet Options. Select the Connections tab. Then click the LAN Settings button to open the Local Area Network (LAN) Settings dialog box (Figure 25-32).

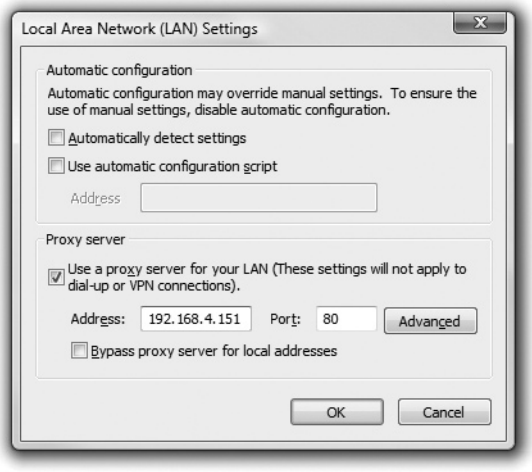


Figure 25-32 The LAN Settings dialog box

Note that you have three options here, with automatic detection of the proxy server being the default. You can specify an IP address and port for a proxy server by clicking the third checkbox and simply typing it in as shown in Figure 25-32.

In some cases, companies have different proxy servers for different programs, such as FTP. You can enter those proxy addresses by clicking the Advanced button and entering the individual addresses. You can also add addresses that should not go through the proxy servers, such as intranet sites. These sites can be added in the Exceptions box down at the bottom of the dialog (Figure 25-33). Your network administrator will give you information on proxy servers if you need it to configure a machine. Otherwise, you can safely leave the browser configured to search automatically for a proxy server. If proxy servers are not used on your network, the automatic configuration will fail and your browser will try to connect to the Internet directly, so there is no harm in just leaving *Automatically detect settings* checked.

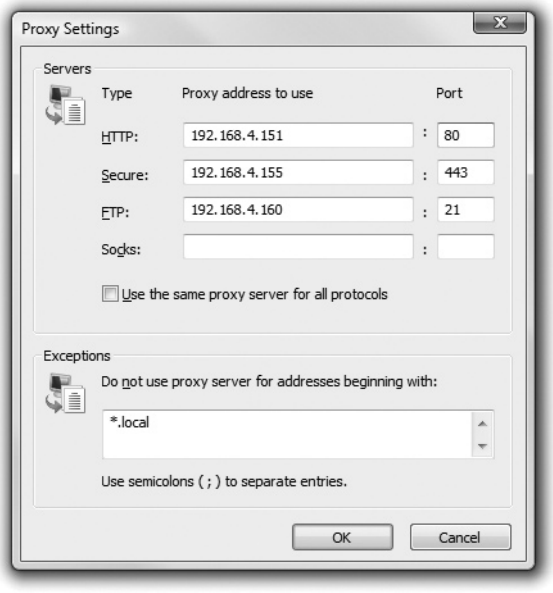


Figure 25-33 Specifying the proxy server address

Security and Scripts While we're on the subject of configuration, make sure you know how to adjust the security settings in your Web browser. Many Web sites come with programs that download to your system and run automatically. These programs are written in specialized languages and file formats such as Java and Active Server Pages (ASP). They make modern Web sites powerful and dynamic, but they can also act as a portal to evil programs. To help with security, all better Web browsers let you determine whether you want these potentially risky programs to run. What you decide depends on personal factors. If your Web browser refuses to run a Java program (you'll know because you'll get a warning message, as in Figure 25-34), check your security settings because your browser may simply be following orders! To get to the security configuration screen in Internet Explorer, choose Tools | Internet Options and open the Security tab (Figure 25-35).

Internet Explorer gives you the option of selecting preset security levels by clicking the Custom level button on the Security tab and then using the pull-down menu (Figure 25-36). Changing from Medium to High security, for example, makes changes across the board, disabling everything from ActiveX to Java. You can also manually select which features to enable or disable in the scrolling menu, also visible in Figure 25-36.

Security doesn't stop with programs. Another big security concern relates to Internet commerce. People don't like to enter credit card information, home phone numbers, or other personal information for fear this information might be intercepted by hackers. Fortunately, there are methods for encrypting this information, the most common being *Hypertext Transfer Protocol Secure* (*HTTPS*). Although HTTPS looks a lot like HTTP from

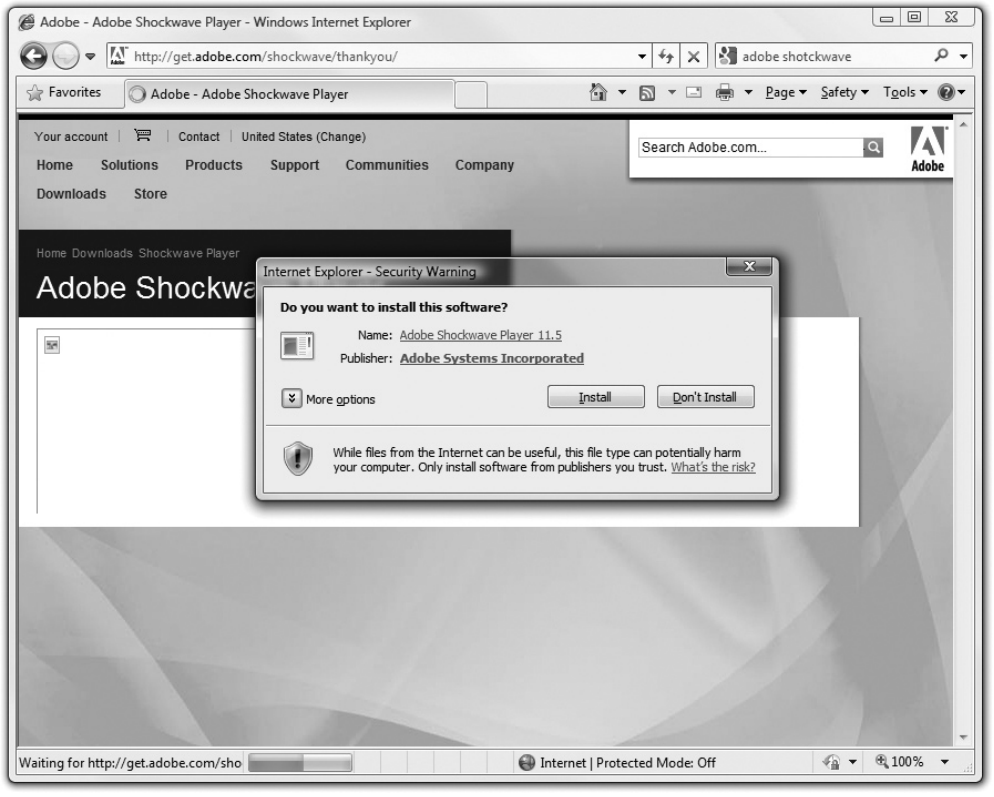


Figure 25-34 Warning message about running ActiveX

the point of view of a web browser, HTTPS uses port 443. It's easy to tell if a Web site is using HTTPS because the Web address starts with *HTTPS*, as shown in Figure 25-37, instead of just *HTTP*. The Web browser also displays a lock symbol in the lower-right corner to remind you that you're using an encrypted connection.

NOTE Depending on the Web site and your Web browser, you might also see a lock in the address bar or even different colors appearing on the address bar when accessing an HTTPS site. While these extras may vary from site to site and browser to browser, you can always count on seeing the lock in the bottom right-hand corner and the HTTPS in the address.

There's one security risk that no computer can completely defend against: you. In particular, be very careful when downloading programs from the Internet. The Internet makes it easy to download programs that you can then install and run on your system. There's nothing intrinsically wrong with this unless the program you download has

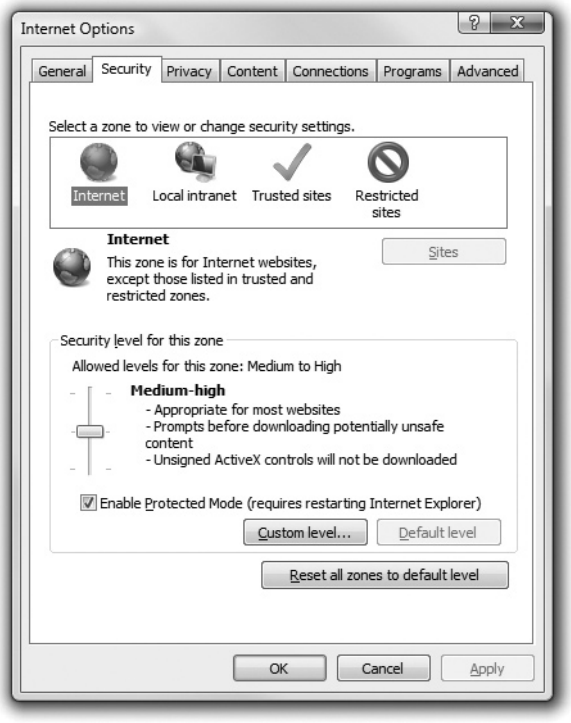


Figure 25-35
The Security tab in the Internet Options dialog box

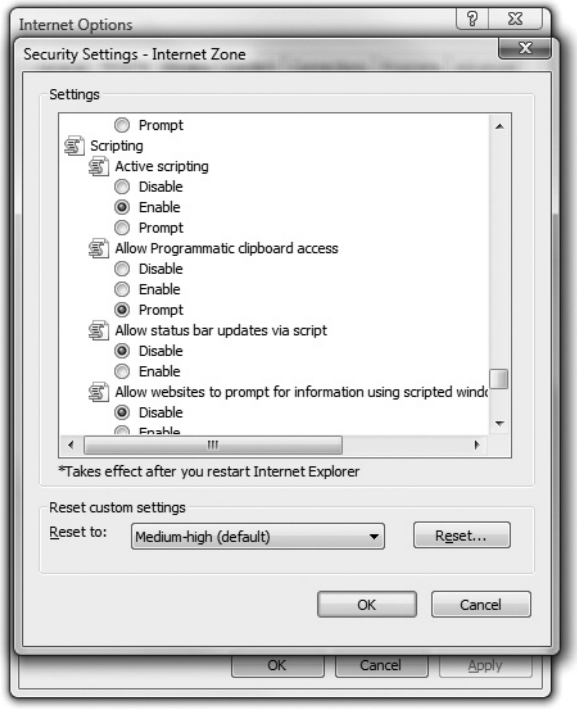


Figure 25-36
Changing security settings

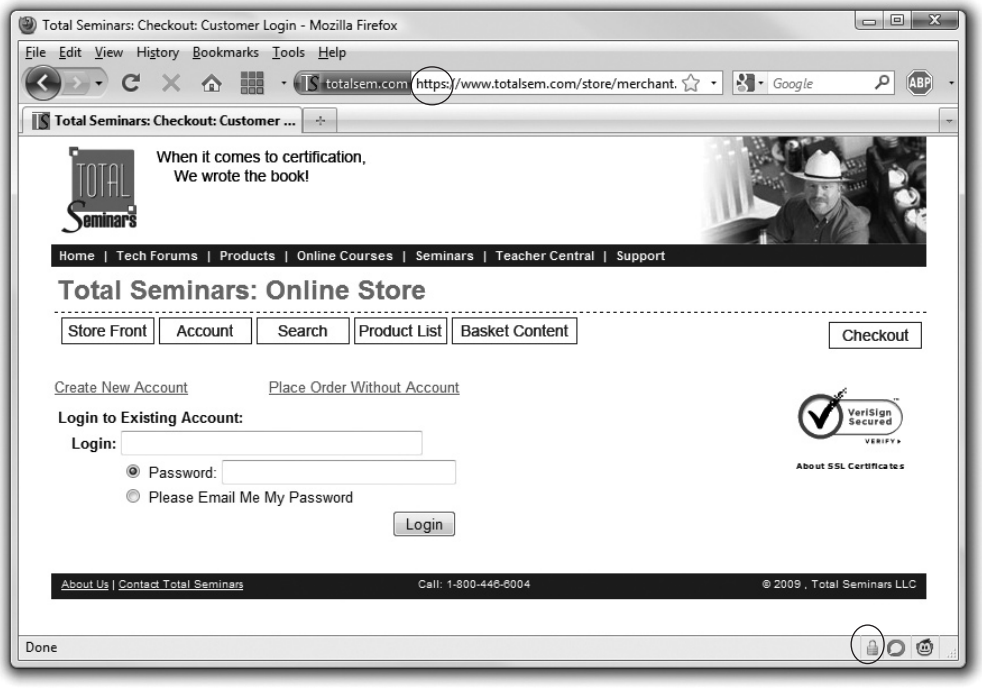


Figure 25-37 A secure Web page

a virus, is corrupted, contains a Trojan horse, or is incompatible with your operating system. The watchword here is *common sense*. Only download programs from reliable sources. Take time to read the online documentation so you're sure you're downloading a version of the program that works on your operating system. Finally, always run a good antivirus program, preferably one that checks incoming programs for viruses before you install them! Failure to do this can lead to lockups, file corruption, and boot problems that you simply should not have to deal with.

NOTE See Chapter 26, "Securing Computers," for the scoop on Trojans and other viruses.

E-mail

You can use an e-mail program to access e-mail. The three most popular are Microsoft's Outlook Express, Windows Mail, and Mozilla's Thunderbird. E-mail clients need a little more setup. First, you must provide your e-mail address and password. All e-mail addresses come in the now-famous *accountname@Internet domain* format. Figure 25-38 shows e-mail information entered into the Windows Mail account setup wizard.

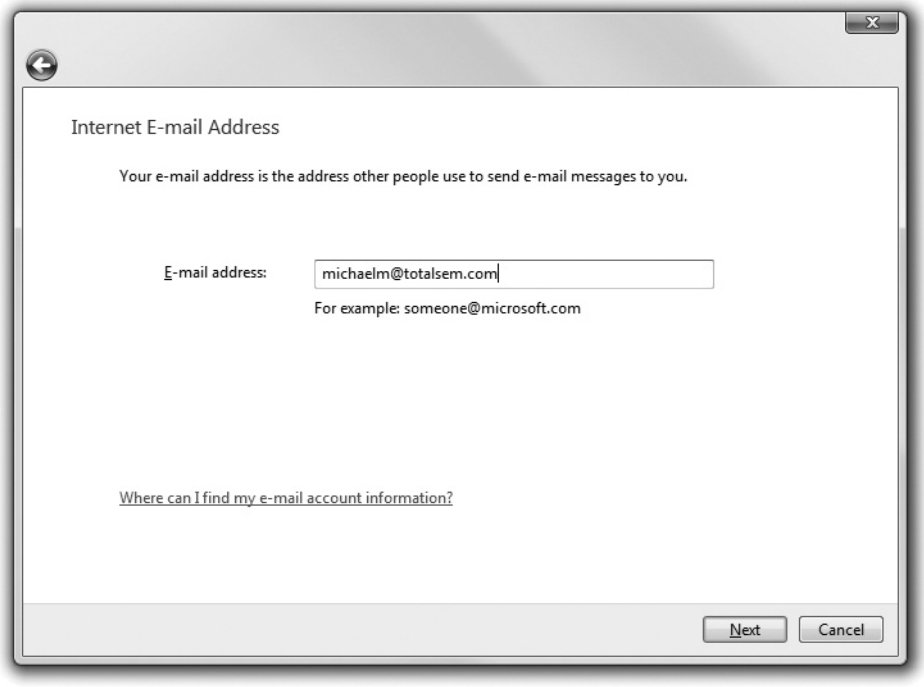


Figure 25-38 Adding an e-mail account to Windows Mail

Next you must add the names of the *Post Office Protocol version 3* (*POP3*) or *Internet Message Access Protocol version 4* (*IMAP4*) server and the *Simple Mail Transfer Protocol* (*SMTP*) server. The POP3 or IMAP server is the computer that handles incoming (to you) e-mail. POP3 is by far the most widely used standard, although the latest version of IMAP, *IMAP4*, supports some features POP3 doesn't. For example, IMAP4 enables you to search through messages on the mail server to find specific keywords and select the messages you want to download onto your machine. Even with the advantages of IMAP4 over POP3, the vast majority of incoming mail servers use POP3.

EXAM TIP Make sure you know your port numbers for these e-mail protocols! POP3 uses port 110, IMAP uses port 143, and SMTP uses port 25.

The SMTP server handles your outgoing e-mail. These two systems may often have the same name, or close to the same name, as shown in Figure 25-39. Your ISP should provide you with all these settings. If not, you should be comfortable knowing what to ask for. If one of these names is incorrect, you will either not get your e-mail or not be able to send e-mail. If an e-mail setup that has been working well for a while suddenly gives you errors, it is likely that either the POP3 or SMTP server is down or that the DNS server has quit working.

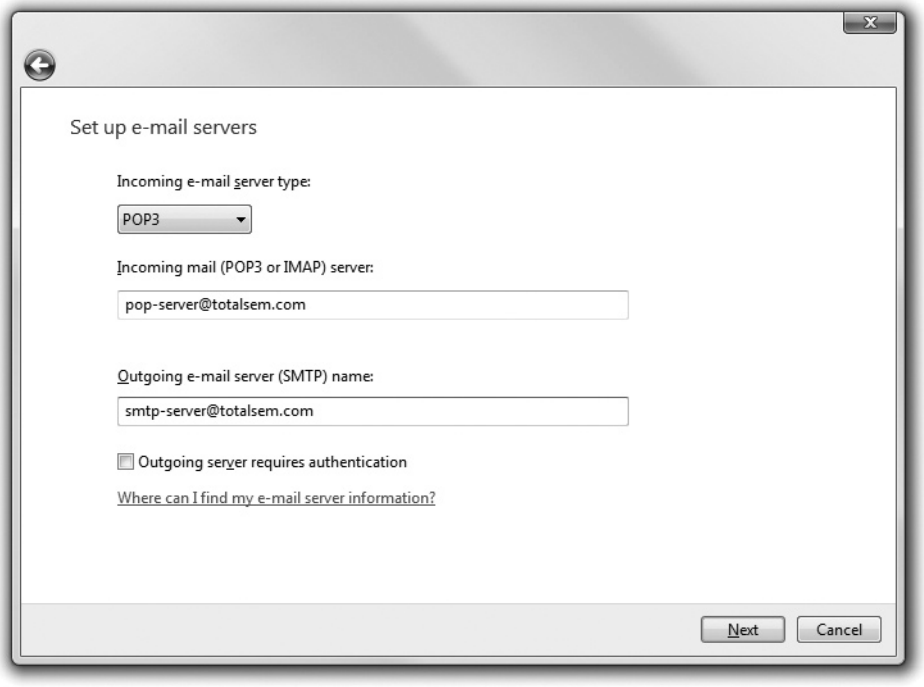


Figure 25-39 Adding POP3 and SMTP information in Windows Mail

When I'm given the name of a POP3 or SMTP server, I use PING to determine the IP address for the device, as shown in Figure 25-40. I make a point to write this down. If I ever have a problem getting mail, I'll go into my SMTP or POP3 settings and type in the IP address (Figure 25-41). If my mail starts to work, I know the DNS server is not working.

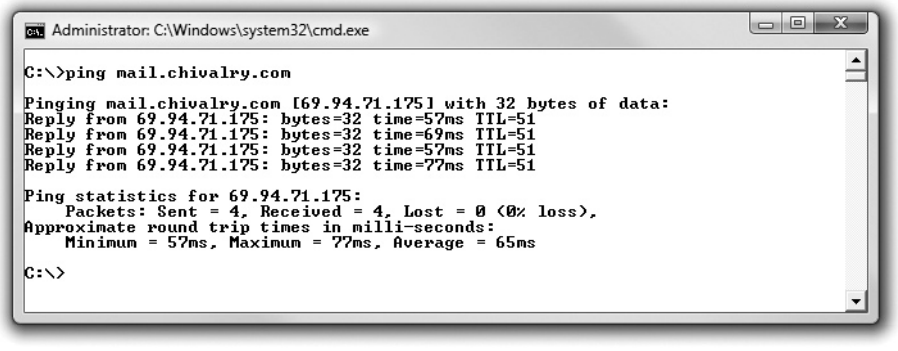


Figure 25-40 Using PING to determine the IP address

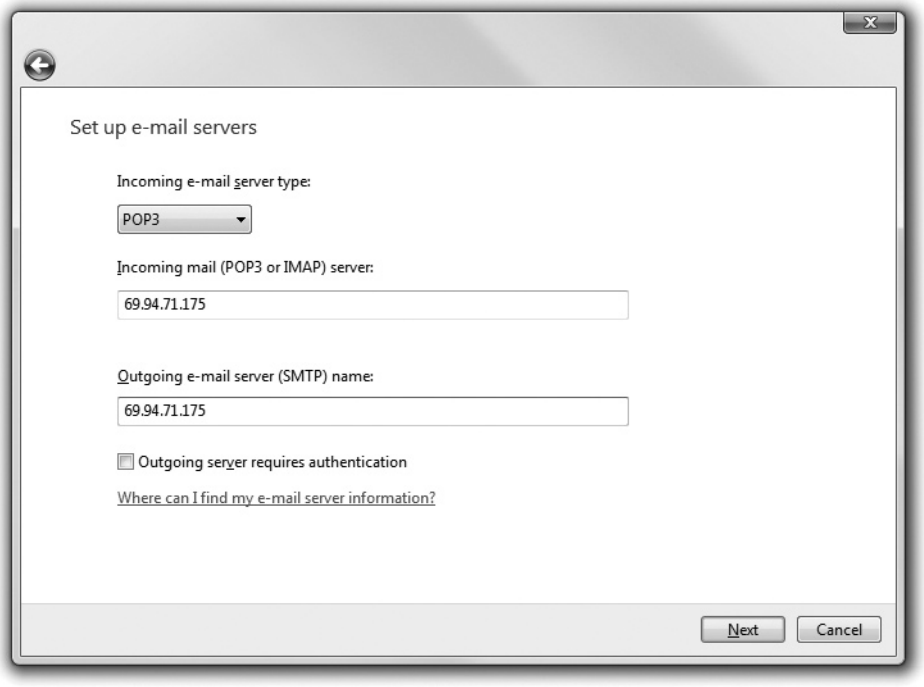


Figure 25-41 Entering IP addresses into POP3 and SMTP settings

NOTE Many people use Web-based e-mail, such as Yahoo! Mail or Gmail from Google, to handle all of their e-mail needs. Web-based mail offers the convenience of having access to your e-mail from any Internet-connected computer. The benefit to using a standalone program is that most offer a lot more control over what you can do with your e-mail, such as flagging messages for later review. Web-based mail services, especially Gmail, are catching up, though, and might surpass traditional e-mail programs in features and popularity.

Newsgroups

Newsgroups are one of the oldest services available on the Internet. To access a newsgroup, you must use a newsreader program. A number of third-party newsreaders exist, such as the popular Forté Free Agent, but Microsoft Outlook Express is the most common of all newsreaders (not surprising since it comes free with most versions of Windows). To access a newsgroup, you must know the name of a news server. *News servers* run the *Network News Transfer Protocol* (*NNTP*). You can also use public news servers, but these are extremely slow. Your ISP will tell you the name of the news server and provide you with a user name and password if you need one (Figure 25-42).

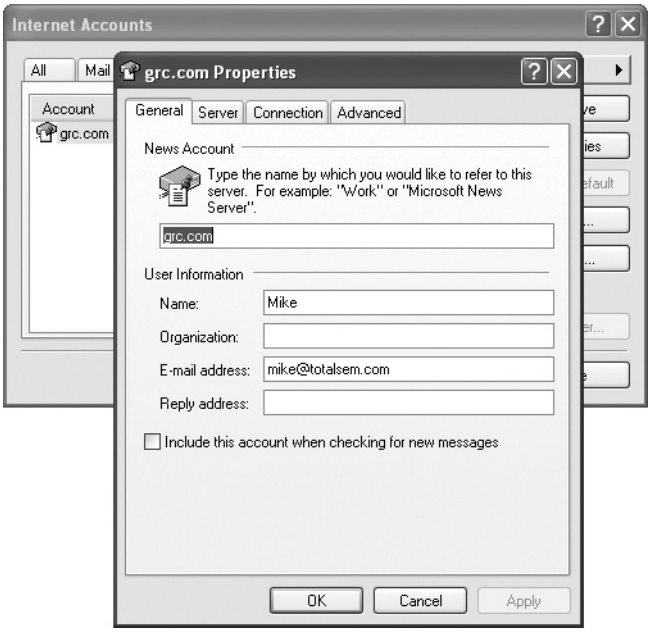


Figure 25-42 Configuring Outlook Express for a news server

File Transfer Protocol (FTP)

File transfer protocol (*FTP*), using ports 20 and 21, is a great way to share files between systems. FTP server software exists for most operating systems, so you can use FTP to transfer data between any two systems regardless of the operating system. To access an FTP site, you must use an FTP client such as FileZilla, although most Web browsers provide at least download support for FTP. Just type in the name of the FTP site. Figure 25-43 shows Firefox accessing ftp.kernel.org.

Although you can use a Web browser, all FTP sites require you to log on. Your Web browser will assume that you want to log in as "anonymous." If you want to log on as a specific user, you have to add your user name to the URL. (Instead of typing **ftp://ftp.example.com**, you would type **ftp://mikem@ftp.example.com**.) An anonymous logon works fine for most public FTP sites. Many techs prefer to use third-party programs such as FileZilla (Figure 25-44) for FTP access because these third-party applications can store user name and password settings. This enables you to access the FTP site more easily later. Keep in mind that FTP was developed during a more trusting time, and that whatever user name and password you send over the network is sent in clear text. Don't use the same password for an FTP site that you use for your domain logon at the office!

Telnet and SSH

Telnet is a terminal emulation program for TCP/IP networks that uses port 23 and enables you to connect to a server or fancy router and run commands on that machine as if you were sitting in front of it. This way, you can remotely administer a server and communicate with other servers on your network. As you can imagine, this is rather risky. If *you* can

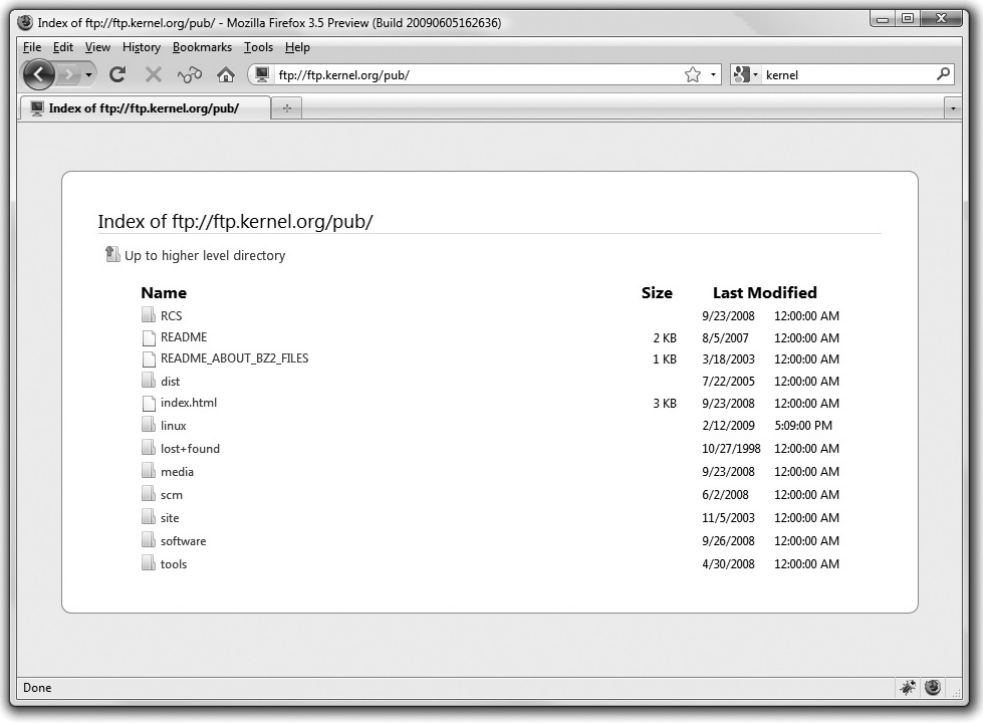


Figure 25-43 Accessing an FTP site in Firefox

remotely control a computer, what's to stop others from doing the same? Of course, Telnet does not allow just *anyone* to log on and wreak havoc with your network. You must enter a special user name and password to run Telnet. Unfortunately, Telnet shares FTP's bad habit of sending passwords and user names as clear text, so you should generally use it only within your own LAN.

If you need a remote terminal that works securely across the Internet, you need *Secure Shell* (*SSH*). In fact, today SSH has replaced Telnet in almost all places Telnet used to be popular. To the user, SSH works just like Telnet. Behind the scenes, SSH uses port 22, and the entire connection is encrypted, preventing any eavesdroppers from reading your data. SSH has one other trick up its sleeve: it can move files or any type of TCP/IP network traffic through its secure connection. In networking parlance, this is called *tunneling*, and it is the core of a technology called VPN, which I will discuss in more depth later in the chapter.

EXAM TIP The CompTIA A+ Certification exams test your knowledge of a few networking tools, such as Telnet, but only enough to let you support a Network+ tech or network administrator. If you need to run Telnet (or its more secure cousin, SSH), you will get the details from a network administrator. Implementation of Telnet falls well beyond CompTIA A+.

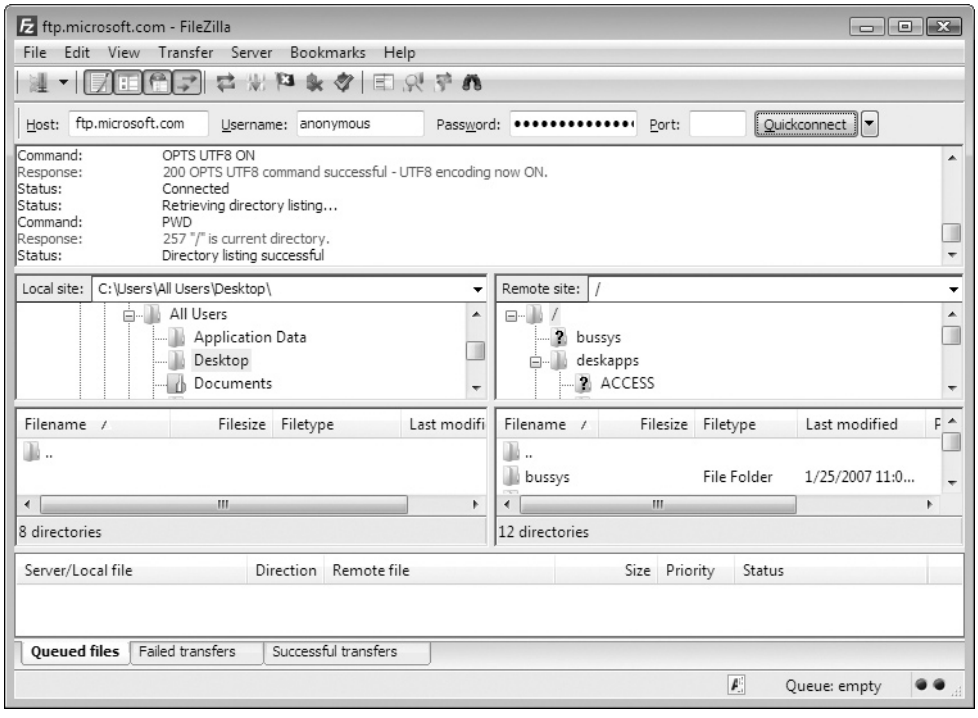


Figure 25-44 The FileZilla program

Voice over IP

You can use *Voice over IP* (*VoIP*) to make voice calls over your computer network. Why have two sets of wires, one for voice and one for data, going to every desk? Why not just use the extra capacity on the data network for your phone calls? That's exactly what VoIP does for you. VoIP works with every type of high-speed Internet connection, from DSL to cable to satellite.

VoIP doesn't refer to a single protocol but rather to a collection of protocols that make phone calls over the data network possible. Venders such as Skype and Vonage offer popular VoIP solutions, and many corporations use VoIP for their internal phone networks. A key to remember when installing and troubleshooting VoIP is that low network latency is more important than high network speed. *Latency* is the amount of time a packet takes to get to its destination and is measured in milliseconds. The higher the latency, the more problems, such as noticeable delays during your VoIP call.

A quick way to check your current latency is to use the ever-handy PING.

1. Run PING on some known source, such as www.microsoft.com or www.totalsem.com.
2. When the PING finishes, take note of the average round-trip time at the bottom of the screen. This is your current latency to that site.

Terminal Emulation

In Microsoft networking, we primarily share folders and printers. At times it would be convenient to be transported in front of another computer—to feel as if your hands were actually on its keyboard. This is called *terminal emulation*. Terminal emulation is old stuff; Telnet is one of the oldest TCP/IP applications, but the introduction of graphical user interfaces cost it much of its popularity. Today when techs talk about terminal emulation, they are usually referring to graphical terminal emulation programs.

Like so many other Windows applications, graphical terminal emulation originally came from third-party companies and was eventually absorbed into the Windows operating system. Although many third-party emulators are available, one of the most popular is the University of Cambridge's VNC. VNC is free and totally cross-platform, enabling you to run and control a Windows system remotely from your Macintosh system, for example. Figure 25-45 shows VNC in action.

Figure 25-45 VNC in action

NOTE All terminal emulation programs require separate server and client programs.

Windows 2000 Server (not Professional) was the first version of Windows to include a built-in terminal emulator called Windows Terminal Services. Terminal Services has a number of limitations: the server software runs only on Windows Server and

the client software runs only on Windows—although the client works on *every* version of Windows and is free. Figure 25-46 shows Windows Terminal Services running on a Windows 2000 computer.

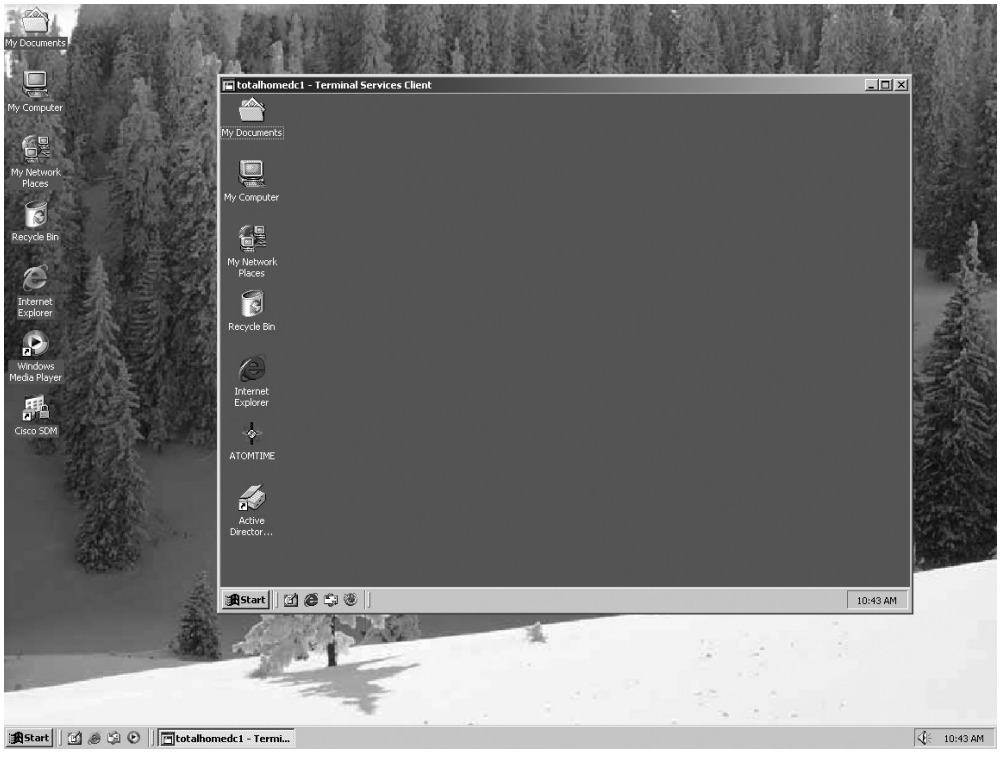


Figure 25-46 Old Terminal Services

Windows XP and Vista offer an alternative to VNC: Remote Desktop. *Remote Desktop* provides control over a remote server with the fully graphical interface. Your desktop *becomes* the server desktop (Figure 25-47). It's quite incredible—although it's only for Windows XP and later.

Wouldn't it be cool if, when called about a technical support issue, you could simply see what the client sees? (I'm not talking voyeur cam here.) When the client says that something doesn't work, it would be great if you could transfer yourself from your desk to your client's desk to see precisely what the client sees. This would dramatically cut down on the miscommunication that can make a tech's life so tedious. Windows Remote Assistance does just that. Based on the Shared Desktop feature that used to come with the popular MSN Messenger program, *Remote Assistance* enables you to give anyone control of your desktop. If a user has a problem, that user can request support directly from you. Upon receiving the support request e-mail, you can then log in to the user's system and, with permission, take the driver's seat. Figure 25-48 shows Remote Assistance in action.

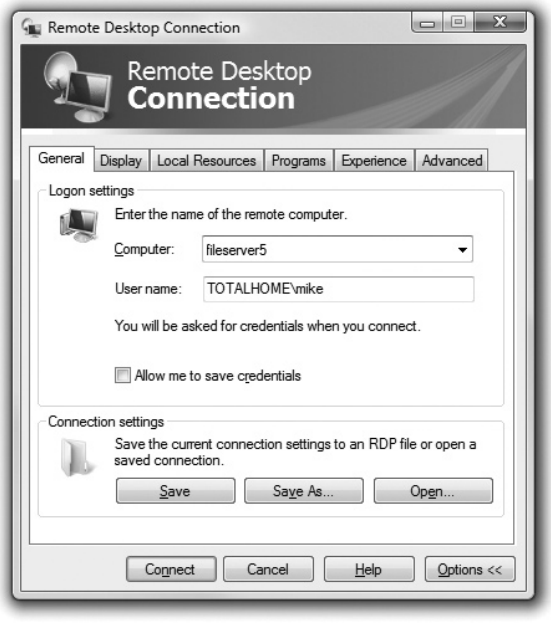


Figure 25-47 Windows Vista Remote Desktop Connection dialog box

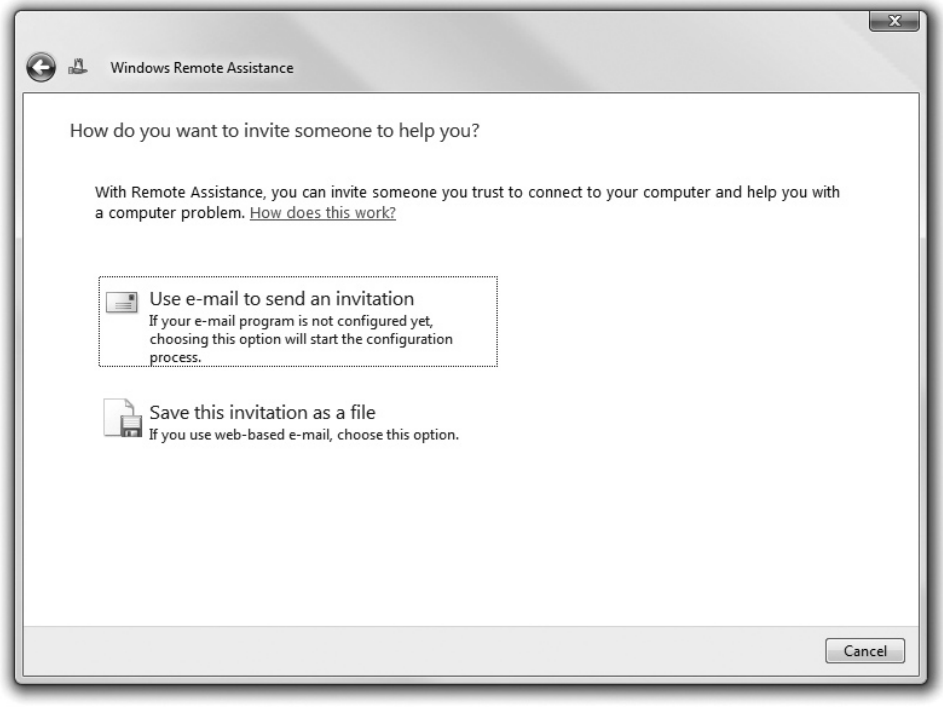


Figure 25-48 Remote Assistance in action

With Remote Assistance, you can do anything you would do from the actual computer. You can troubleshoot some hardware configuration or driver problem. You can install drivers, roll back drivers, download new ones, and so forth. You're in command of the remote machine as long as the client allows you to be. The client sees everything you do, by the way, and can stop you cold if you get out of line or do something that makes the client nervous! Remote Assistance can help you teach someone how to use a particular application. You can log on to a user's PC and fire up Outlook, for example, and then walk through the steps to configure it while the user watches. The user can then take over the machine and walk through the steps while you watch, chatting with one another the whole time. Sweet!

The new graphical terminal emulators provide everything you need to access one system from another. They are common, especially now that Microsoft provides free terminal emulators. Whatever type of emulator you use, remember that you will always need both a server and a client program. The server goes on the system you want to access and the client goes on the system you use to access the server. On many solutions, the server and client software are integrated into a single product.

Virtual Private Networks

Remote connections have been around for a long time, long before the Internet existed. The biggest drawback about remote connections was the cost to connect. If you were on one side of the continent and had to connect to your LAN on the other side of the continent, the only connection option was a telephone. Or, if you needed to connect two LANs across the continent, you ended up paying outrageous monthly charges for a private connection. The introduction of the Internet gave people wishing to connect to their home networks a very cheap connection option, but with one problem: the whole Internet is open to the public. People wanted to stop using dial-up and expensive private connections and use the Internet instead, but they wanted to do it securely.

Those clever network engineers worked long and hard and came up with several solutions to this problem. Standards have been created that use encrypted tunnels between a computer (or a remote network) to create a private network through the Internet (Figure 25-49), resulting in what is called a *Virtual Private Network* (*VPN*).

An encrypted tunnel requires endpoints—the ends of the tunnel where the data is encrypted and decrypted. In the SSH tunnel you've seen thus far, the client for the application sits on one end and the server sits on the other. VPNs do the same thing. Either some software running on a computer or, in some cases, a dedicated box must act as an endpoint for a VPN (Figure 25-50).

To make VPNs work requires a protocol that uses one of the many tunneling protocols available and adds the capability to ask for an IP address from a local DHCP server to give the tunnel an IP address that matches the subnet of the local LAN. The connection keeps the IP address to connect to the Internet, but the tunnel endpoints must act like NICs (Figure 25-51). Let's look at one of the protocols, PPTP.

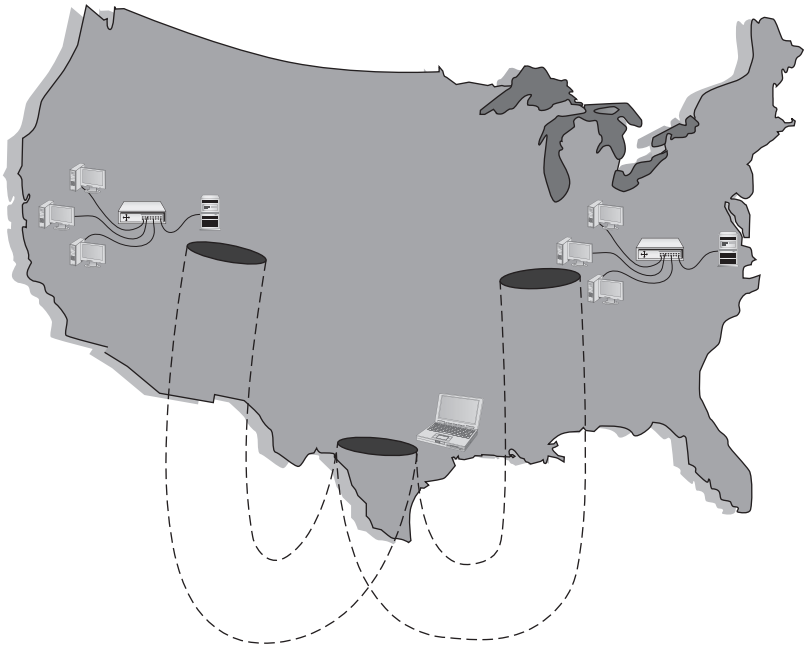


Figure 25-49
VPN connecting computers across the United States

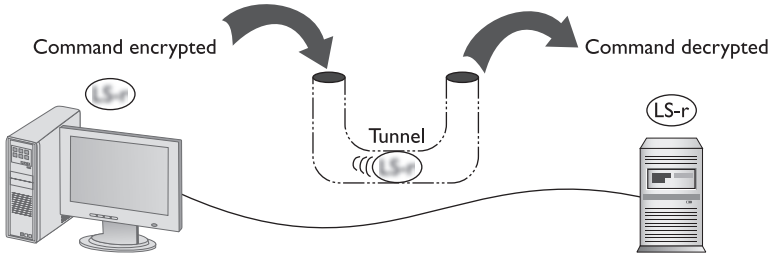


Figure 25-50
Typical tunnel

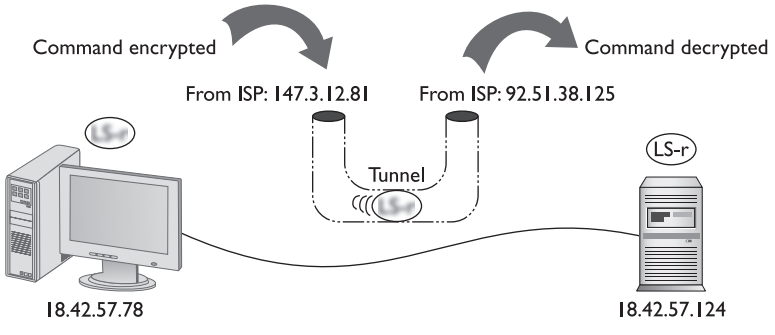


Figure 25-51
Endpoints must have their own IP addresses.

PPTP VPNs

So how do we make IP addresses appear out of thin air? Microsoft got the ball rolling with the *Point-to-Point Tunneling Protocol* (*PPTP*), an advanced version of a protocol used for dial-up Internet called PPP that handles all of this right out of the box. The only trick is the endpoints. In Microsoft's view, a VPN is intended for individual clients (think employees on the road) to connect back to the office network, so Microsoft places the PPTP endpoints on the client and a special remote access server program called Routing and Remote Access Service (RRAS), originally only available on Windows Server, on the server (see Figure 25-52).

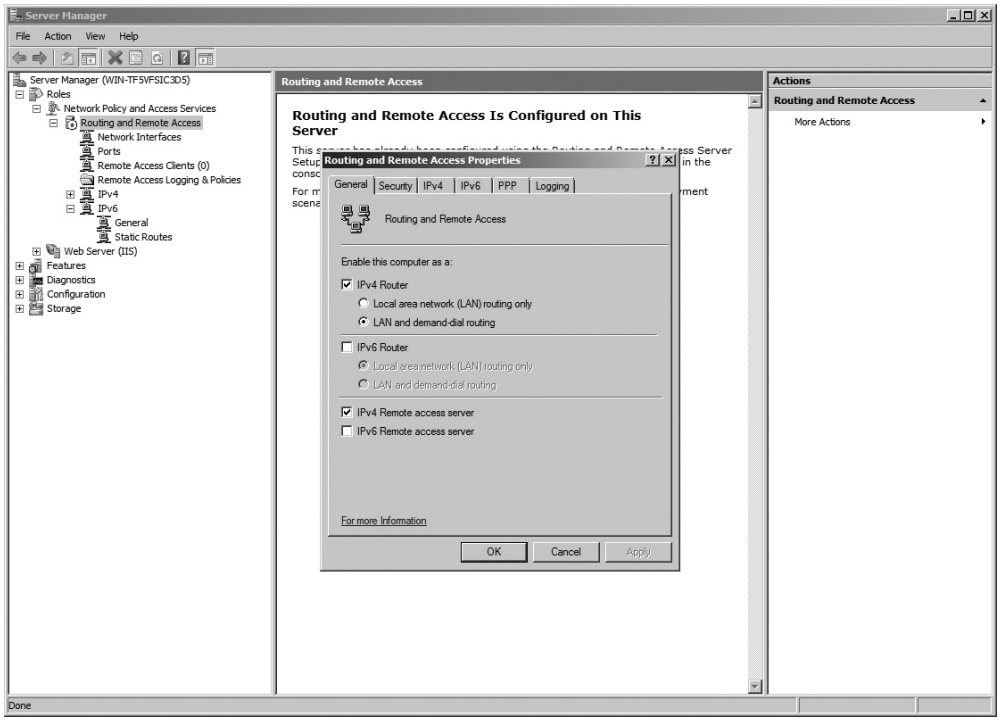


Figure 25-52 RRAS in action

On the Windows client side, you right-click on My Network Places and click on Create a New Connection (Windows 2000–XP) or right-click on Network and select *Set up a connection or network* (Windows Vista) from the Network and Sharing Center. This presents you with a dialog where you can enter all your VPN server information. Your network administrator will most likely provide this to you. The result is a virtual network card that, like any other NIC, gets an IP address from the DHCP server back at the office (Figure 25-53).

Figure 25-53 VPN connection in Windows

EXAM TIP A system connected to a VPN looks as though it's on the local network but performs much slower than if the system were connected directly back at the office.

When your computer connects to the RRAS server on the private network, PPTP creates a secure tunnel through the Internet back to the private LAN. Your client takes on an IP address of that network, as if your computer were plugged into the LAN back at the office. Even your Internet traffic will go through your office first. If you open your Web browser, your client will go across the Internet to the office LAN and then use the LAN's Internet connection! Because of this, Web browsing is very slow over a VPN.

Beyond A+

The areas covered by the CompTIA A+ Certification exams do a great job on the more common issues of dealing with the Internet, but a few hot topics (although beyond the scope of the CompTIA A+ exams) are so common and important that you need to know them: online gaming, chatting, and file sharing.

Online Gaming

One of the more exciting and certainly more fun aspects of the Internet is online gaming. Competing online against a real person or people makes for some pleasant gaming. Enjoying classics such as Hearts and Backgammon with another human can be challenging and fun. Another popular genre of online gaming is the "first-person shooters" format. These games place you in a small world with up to 32 other players. A great example is Valve Software's Counter-Strike: Source (Figure 25-54).

No discussion of online gaming is complete without talking about the most amazing game type of all: the massively multiplayer online role-playing game (MMORPG).

Figure 25-54 Counter-Strike: Source

Imagine being an elfin wizard, joined by a band of friends, all going on adventures together in worlds so large that it would take a real 24-hour day to journey across them! Imagine that in this same world, 2,000 to 3,000 other players, as well as thousands of game-controlled characters, are participating! Plenty of MMORPGs are out there, but the most popular today is World of Warcraft (Figure 25-55).

Each of these games employs good old TCP/IP to send information, using ports reserved by the game. For instance, the Quake series of games uses port 26000, while DirectX uses ports 47624 and 2300–2400.

Chatting

If there's one thing we human beings love to do, it's chat. The Internet provides a multitude of ways to do so, whether by typing or actual talking. Keep in mind that chatting occurs in real time. As fast as you can type or talk, whoever is at the other end hears or sees what you have to say. To chat, however, you need some form of chat software. The oldest family of chat programs is based on the Internet Relay Chat (IRC) protocol, and the single most common IRC chat program is probably mIRC. IRC protocols allow for a number of other little extras as well, such as being able to share files.

Figure 25-55 My editor playing World of Warcraft

Today, companies such as AOL, Yahoo!, and Microsoft have made their own chat programs that not only provide text chat but also add features such as voice and video, turning your PC into a virtual replacement for your telephone! Figure 25-56 shows the popular Microsoft Windows Live Messenger software.

File Sharing

The last extra Internet function to discuss is also probably the most controversial: file sharing. File sharing basically consists of a whole bunch of computers with one program loaded, such as Napster or Kazaa. The file-sharing program enables each of the computers running that program to offer files to share, such as MP3 music files and MPEG movies. Once all of the file-sharing computers log on to the Internet, any of them can download any file offered by any other in the group.

File sharing through such *distributed* sharing software becomes almost anonymous and free—and that's the problem. You can share *anything*, even copyright-protected music, movies, and more. The music industry in particular has come out swinging to try to stop file-sharing practices. As a result, the music industry is working on a way to shut down those persons who share lots of files. But software developers have countered, creating Internet protocols such as BitTorrent to handle the distribution and make the file sharers much more difficult to find and punish. Figure 25-57 shows one of the

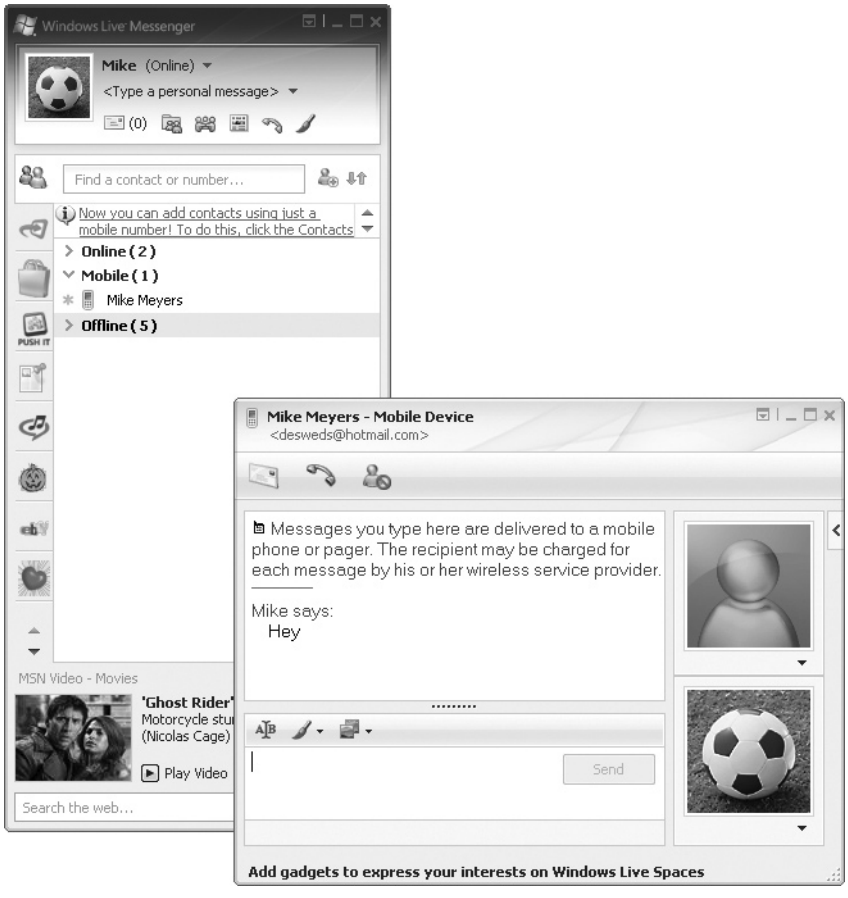


Figure 25-56 Windows Live Messenger in action

more popular BitTorrent protocol programs called µTorrent (the µ is the symbol for "micro," so you pronounce it "micro torrent"). BitTorrent has many legitimate uses as well—its protocol is extremely efficient for the distribution of large files and has become the method of choice for distributing Linux distributions and large open-source applications such as Apache and OpenOffice.

These example programs just scratch the surface of the many applications that use the Internet. One of the more amazing aspects of TCP/IP is that its basic design is around 30 years old. We use TCP/IP in ways completely outside the original concept of its designers, yet TCP/IP continues to show its power and flexibility. Pretty amazing!

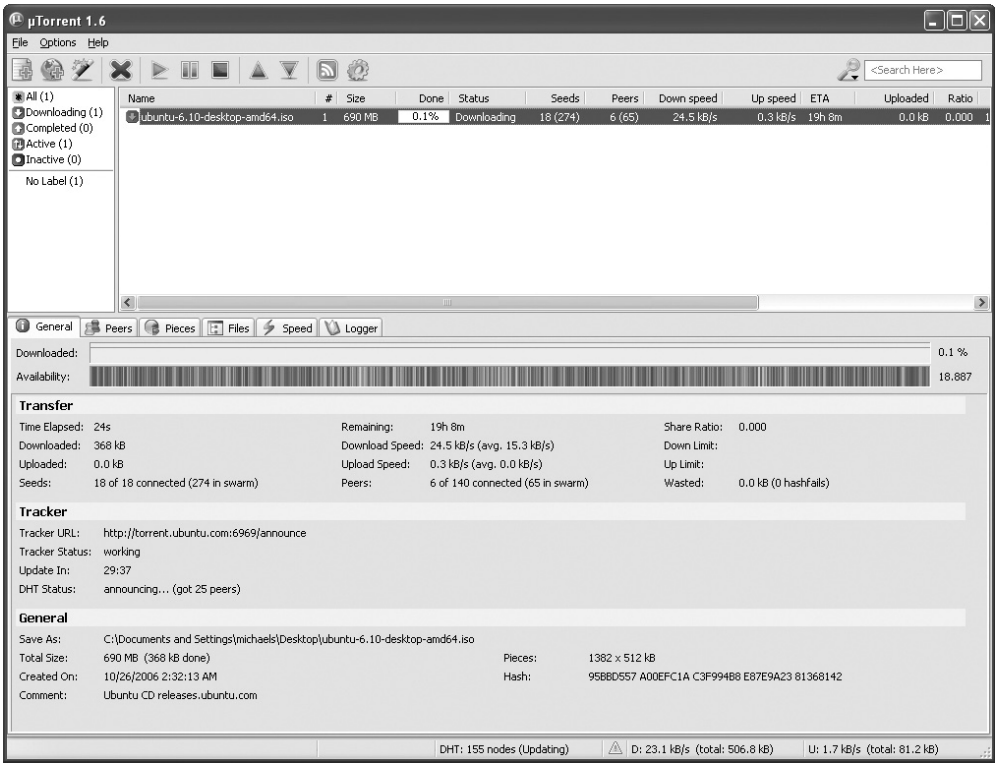


Figure 25-57 µTorrent

Chapter Review Questions

1. Of the following four Internet connection options, which typically offers the *slowest* connection speed?
   - **A.** Cable
   - **B.** Dial-up
   - **C.** DSL
   - **D.** Satellite
2. Which of the following technologies use dial-up connections? (Select two.)
   - **A.** Cable modem
   - **B.** DSL receiver
   - **C.** ISDN TA
   - **D.** Modem

3. What advantages does dial-up have over DSL?
   - **A.** Dial-up is faster than DSL
   - **B.** You can be farther than 18,000 feet from a main phone service switching center.
   - **C.** You can get a second phone lines to use just for dial-up.
   - **D.** None. Dial-up has no advantages over DSL.
4. Which protocol can you use to send e-mail?
   - **A.** IMAP
   - **B.** POP3
   - **C.** PPP
   - **D.** SMTP
5. Which protocols can you use to receive e-mail? (Select two.)
   - **A.** IMAP
   - **B.** POP3
   - **C.** PPP
   - **D.** SMTP
6. What advantage does satellite have over cable for connecting to the Internet?
   - **A.** Satellite is faster than cable.
   - **B.** Cable degrades in stormy weather; satellite does not.
   - **C.** Satellite requires you to be within 18,000 feet of a central switch.
   - **D.** Cable is limited to areas with cable installed; satellite is not.
7. Which Microsoft technology enables you to share a single Internet connection with multiple computers?
   - **A.** Internet Connection Sharing
   - **B.** My Network Places
   - **C.** Remote Access
   - **D.** Remote Desktop
8. What command often enables you to diagnose TCP/IP errors such as connection problems?
   - **A.** FTP
   - **B.** PING
   - **C.** POP3
   - **D.** VoIP

9. At what layer of the OSI seven-layer model do proxy servers operate?
   - **A.** Layer 1, Physical
   - **B.** Layer 2, Data Link
   - **C.** Layer 6, Presentation
   - **D.** Layer 7, Application
10. Which of the following programs enable you to access and work on a remote computer from your local computer? (Select two.)
   - **A.** FTP
   - **B.** Internet Connection Sharing
   - **C.** Remote Desktop
   - **D.** Telnet

Answers

1. **B.** Dial-up connections are robust and widely available, but slower than the newer connection types.
2. **C, D.** ISDN terminal adapters and traditional modems use dial-up for connecting to the Internet.
3. **B.** DSL has a fairly short limit of 18,000 feet from a main switch, leaving people in rural areas (in the United States, at least) out of luck. Dial-up just requires a phone line.
4. **D.** You can use SMTP to send e-mail messages.
5. **A, B.** You can use either IMAP or POP3 to receive e-mail messages.
6. **D.** Clearly, satellite cuts you loose from the wires!
7. **A.** Internet Connection Sharing enables you to share a single Internet connection with multiple computers.
8. **B.** You can often use the PING command to diagnose TCP/IP problems.
9. **D.** Proxy servers operate at Layer 7, the Application layer.
10. **C, D.** Both Telnet and Remote Desktop enable you to access and work on a remote computer. The latter is just prettier!