

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...a 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). The "Beyond A+" section is beefier than that of other chapters because, although the CompTIA A+ certification exams don't require it, every tech needs to know how to assist clients with some of the *niceties* of the Internet. Let's get started!

Historical/Conceptual

Understanding the Internet

The Internet enables users to 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 when he or she 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. In order 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. However, 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 22-1 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 22-2). Polly happily reads the message and life is great. The Internet functions as planned.

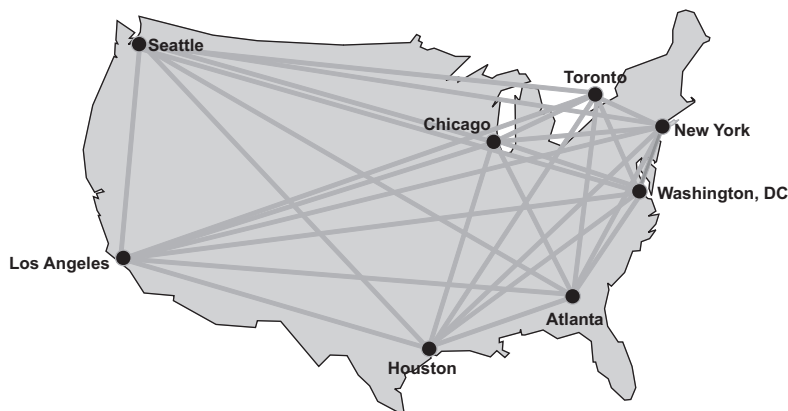


Figure 22-1 Internet Tier 1 connections

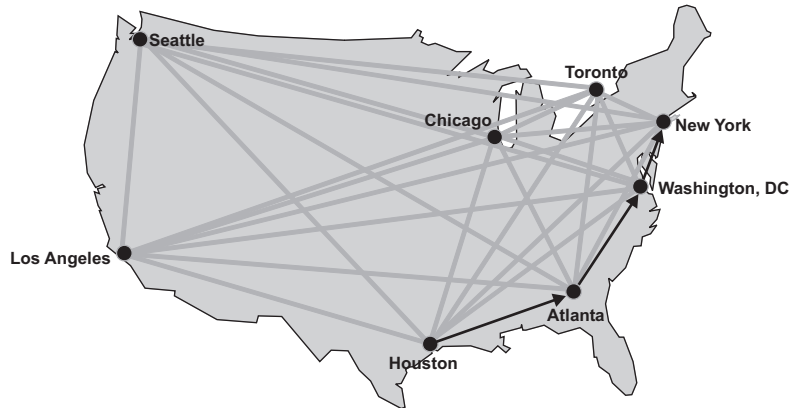


Figure 22-2 Message traveling from Houston to NYC

But what happens if the entire southeastern United States experiences a huge power outage and Internet backbones in every state from Virginia to Florida goes 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, then University of Toronto, and then SUNY (Figure 22-3). It's all in a day's work for the highly redundant and adaptable Internet. At this point in the game (early 2007), the Internet simply cannot go down fully—barring, of course, a catastrophe of Biblical proportions.

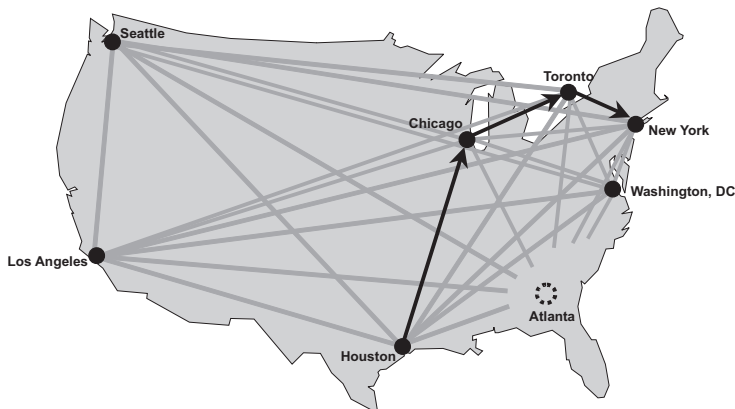


Figure 22-3 Rerouted message from Houston to NYC

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 21 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 Transport 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 out 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 together 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 catch words, only serving to confuse already bewildered consumers.

ISPs come in all sizes. America Online (AOL) has a huge pipe into the Internet, enabling its millions of customers (in the U.S. alone) to connect from their local machines and surf the Web. Contrast AOL with Unisono Net, an ISP in San Miguel de Allende, Mexico (Figure 22-4). Billed as the “Best ISP in San Miguel,” it services only a small (but delightful) community and the busy tourist crowd. Functionally, though, Unisono Net does the same thing AOL does, just without all the bells, whistles, and mountains of free CD-ROMs!

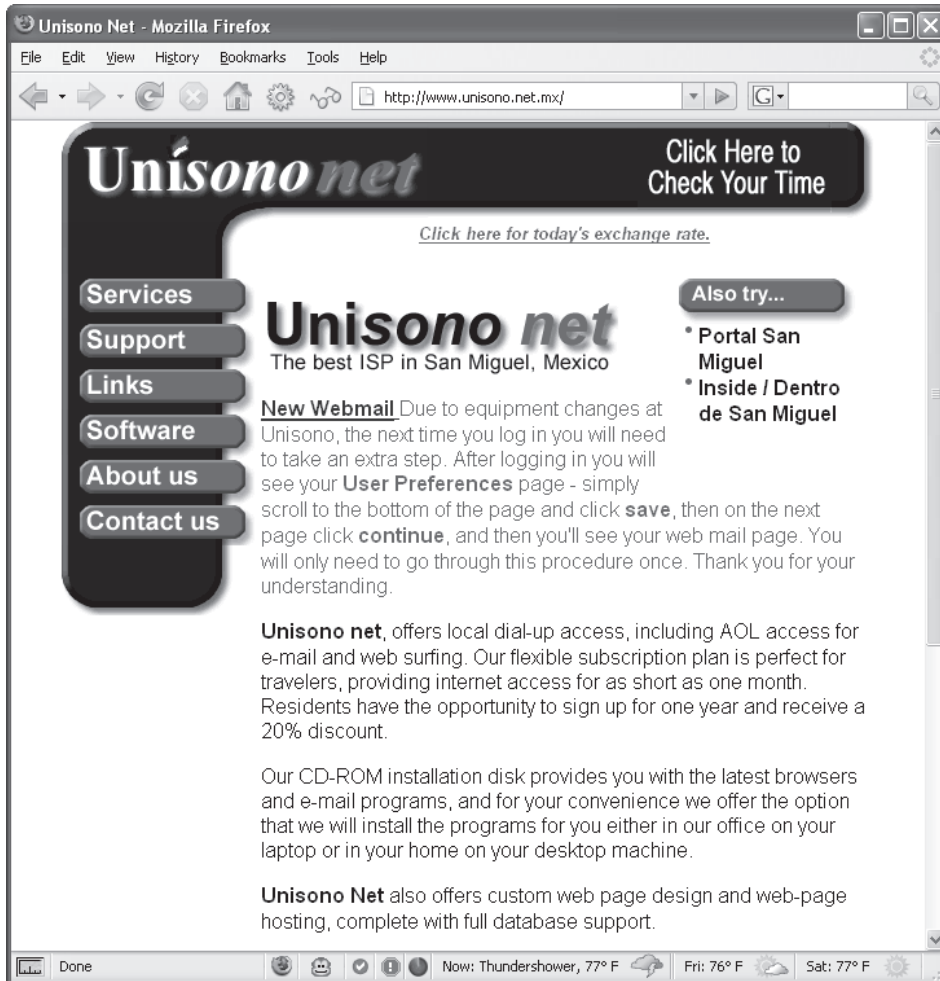


Figure 22-4 Unisono Net homepage

Connection Concepts

Connecting to an ISP requires two things to work perfectly: hardware for connectivity, such as a modem and a working telephone 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 22-5 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.

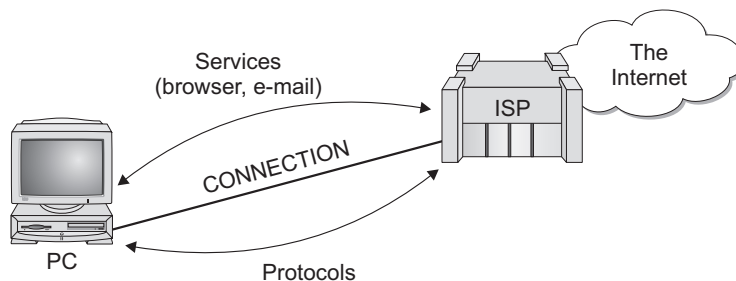


Figure 22-5 Simplified Internet connectivity

Essentials

Connecting to the Internet

PCs commonly connect to an ISP using one of seven technologies: 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 21. Satellite is the odd man out here; it may use either a modem or a NIC, depending on the particular configuration you have, although most folks will use a modem. 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 22-6). 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.

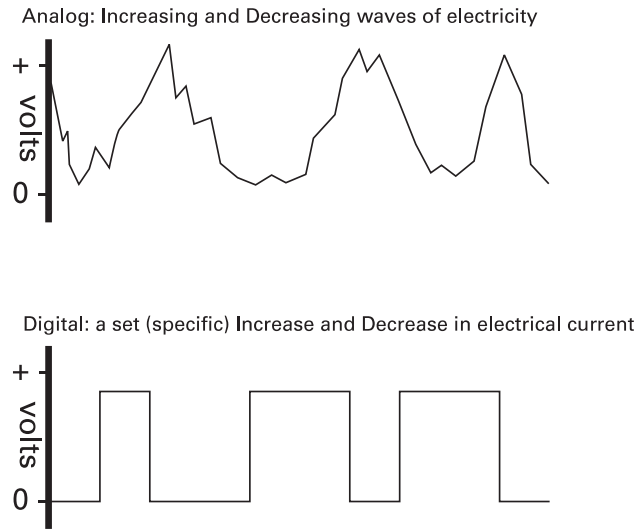


Figure 22-6 Analog signals used by a telephone line versus digital signals used by the computer

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 22-7). Modems also take digital signals from the PC and convert them into analog signals for the outgoing telephone line.

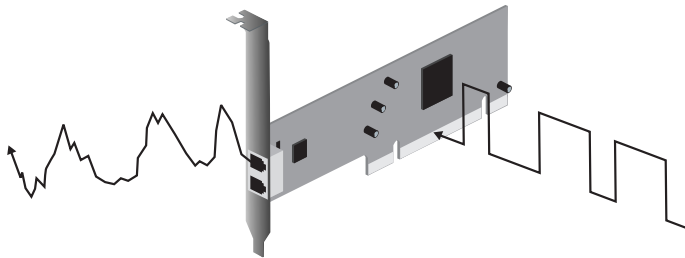


Figure 22-7 Modem converting analog signal to digital signal

A modem does what's 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 22-8). 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 22-9).

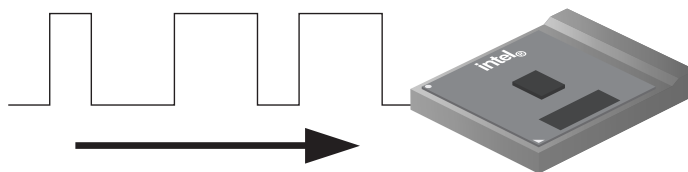


Figure 22-8 CPUs can't read serial data.

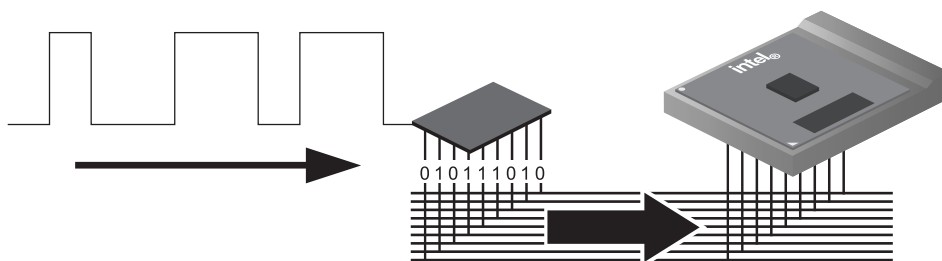


Figure 22-9 The UART chip converts serial data to parallel data.

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 22-10). Internal modems can handle both jobs because they have their own UART built in (Figure 22-11). Table 22-1 shows the UART chips that have been used in PCs.

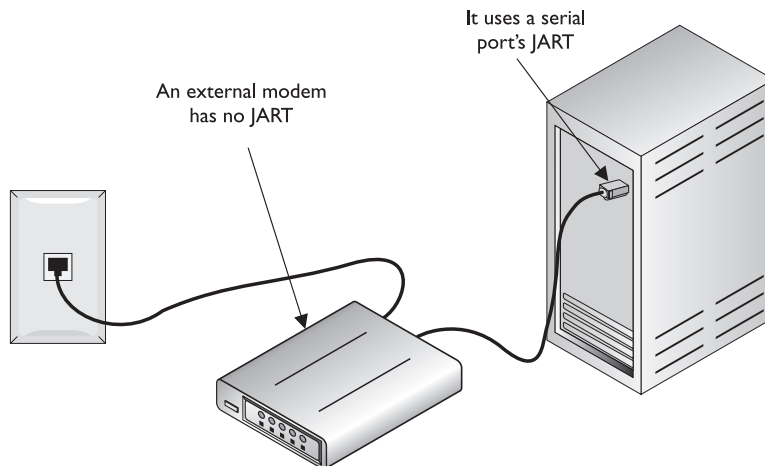


Figure 22-10 An external modem uses a PC's serial port.

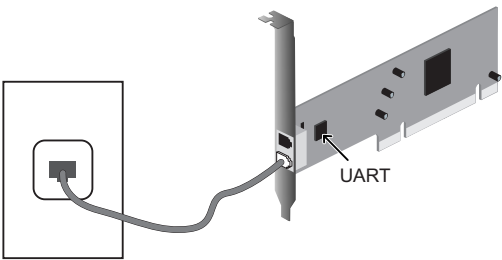


Figure 22-11 An internal modem has UART built in.

Chip	Description
8250	This is the original chip selected by IBM for use in the PC. It had several bugs, but IBM worked around them with built-in routines written in the PC and XT ROM BIOS.
8250A	This chip was developed to fix the bugs in the 8250, but the fix meant it did not work properly with the PC and XT BIOS, although it does work with the AT BIOS. This chip does not work adequately at speeds at or above 9600 bits per second (bps).
8250B	This chip was developed to fix the bugs in the previous chips, but still came with the interrupt enable bug contained in the 8250 chip. This made it compatible with the PC/XT BIOS, and possibly also with the AT BIOS. It retains the problems with rates above 9600 bps.
16450	This chip was initially picked by IBM for its AT systems. It should be seen as the bare minimum for its OS/2 systems; otherwise, the serial ports will not function properly. This chip has a higher throughput than the previous chips and has an added scratch register to aid in speed. The only drawback is that it cannot be used with the PC/XT BIOS due to the interrupt bug being fixed.
16550	This chip was an improvement over the 16450, but it cannot be used for First In First Out (FIFO) buffering modes. It did enable programmers to use multiple DMA channels, however. This chip is not recommended for standard high-speed communication use and should be replaced by the 16550A, even though it has a higher throughput.
16550A	This chip has 16 built-in FIFO registers for receiving and transmitting. It will increase your throughput without loss of characters at higher rates of speed, due to the added registers. This is the only UART installed on today's systems.

Table 22-1 UARTs

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: $2,400 \times 14 = 33.6$ 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 bps so often for so long that the terms have become functionally synonymous.

Modern Modem Standards: V.90 vs. 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-T), the current top standards are V.90 and V.92. Both standards offer 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.



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

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 22-12). What will they think up next?

Modem Connections: PCI, PCI Express, and USB Modems connect to the PC in two basic ways: internally or externally. 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 22-13). On AMD's motherboards this is called an ACR (Advanced Communication Riser) slot, while Intel motherboards use the extremely similar CNR (Communication and Networking Riser) slot. Finally, and least expensive of all, many current motherboards dispense with expansion cards entirely and come with the modem integrated into the motherboard.



Figure 22-12 Some of the many features touted by the manufacturer of the SupraMax modem

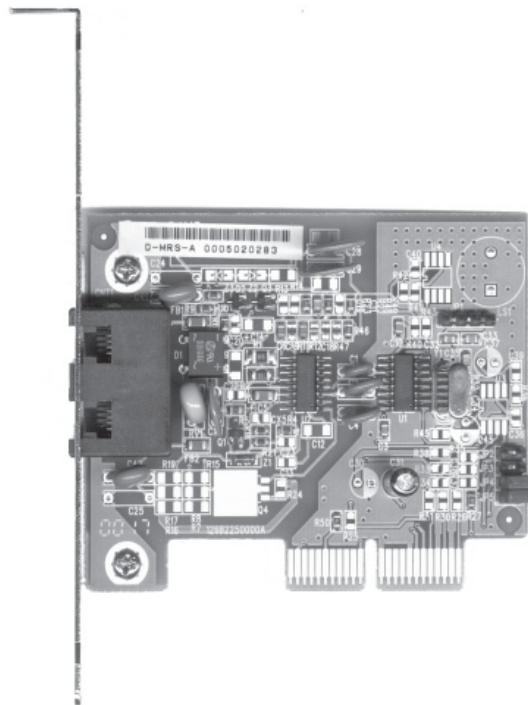


Figure 22-13 A CNR modem

External modems connect to the PC through an available serial port (the old way) or USB port (Figure 22-14). Many PCs come with two 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. Virtually all computers today have two or more USB ports in addition to serial ports.

Figure 22-14
A USB modem



If you have the option, choose a USB modem, especially one with a volume control knob. The very low speeds of data communication over a modem make the physical type of the connection unimportant. Even the slowest interface—the aging serial interface—can more than adequately handle 56 Kbps data transfers. 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 (Figure 22-15), and then choose *Set up or change your Internet connection* from the Pick a task menu (Figure 22-16). The Internet Properties dialog box opens with the Connections tab displayed. All your work will proceed from here (Figure 22-17).

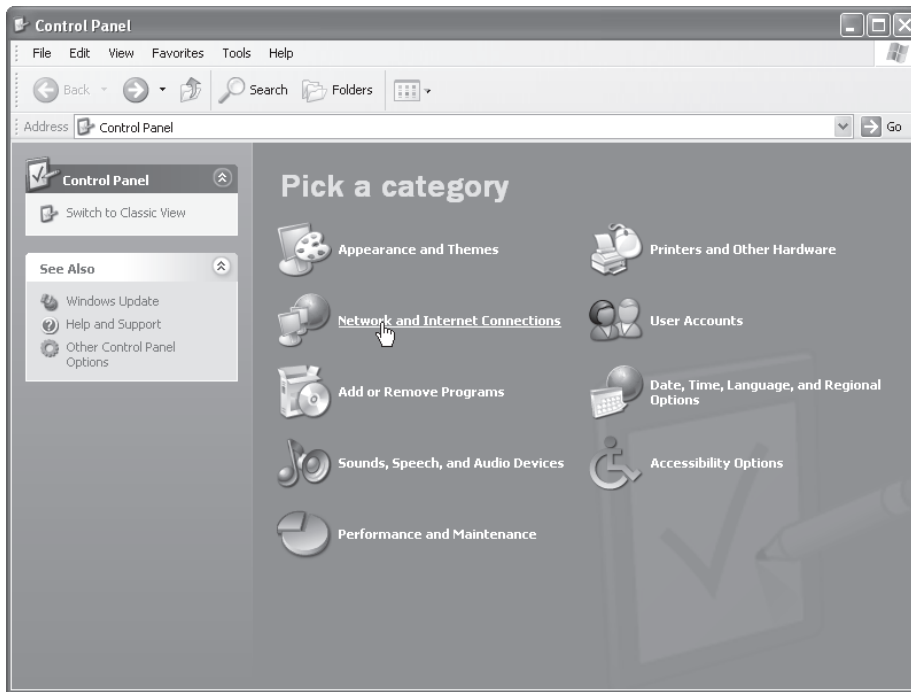


Figure 22-15 Opening the Network and Internet Connections applet

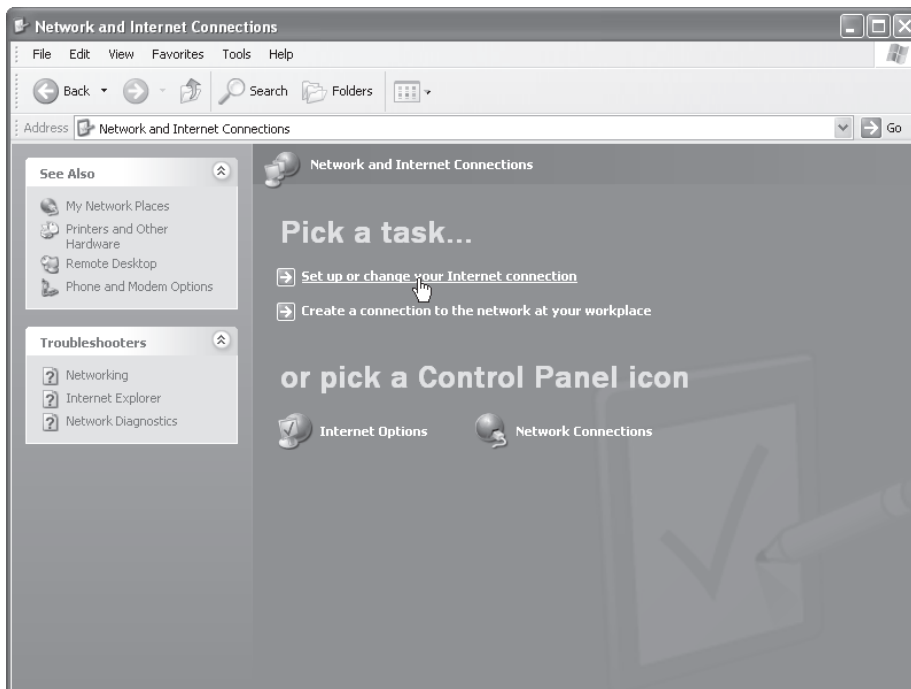
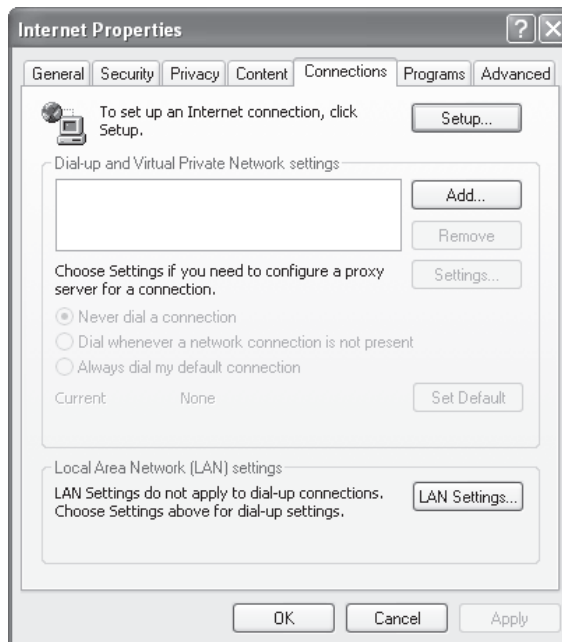


Figure 22-16 Picking a task ... set up or change?

Figure 22-17
The Connections
tab in the Internet
Properties dialog box

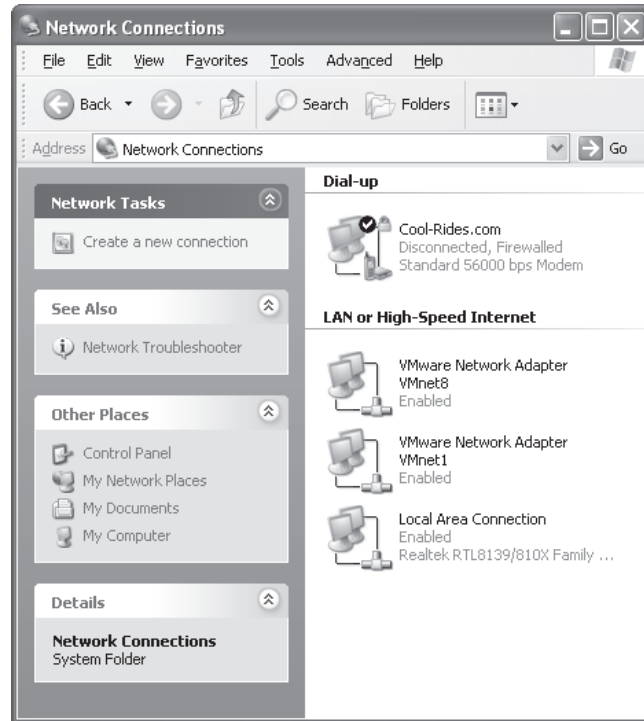


Click the Setup button to run the New Connection Wizard, and then work through the screens (Figure 22-18). At this point, you're going to need information provided by your ISP to configure your connection properly. When you finish the configuration, you'll see a new Connect To option on the Start menu if your system is set up that way. If not, open up Network Connections and your new dial-up connection will be available. Figure 22-19 shows the option to connect to a fictitious ISP, Cool-Rides.com.

Figure 22-18
The New
Connection Wizard



Figure 22-19
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 will 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, 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 rarely used as dial-up connections—they are far more common on dedicated lines.

Digital Subscriber Line (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 U.S., but the typical upload speed is ~384 Kbps, while download speed comes in at a very sweet ~2+ 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 128, 256, or 384 Kbps) and faster download speed (usually 2 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 a NIC in the Internet-bound PC and drop off a *DSL receiver* (often called a DSL modem) (Figure 22-20). The receiver connects to the telephone line and the PC (Figure 22-21). The tech (or the user, if knowledgeable) then configures the TCP/IP protocol options for the NIC to match the settings demanded by the DSL provider, 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. This pretty much stops everybody but inner-city dwellers from having access to DSL service.

Figure 22-20
A DSL receiver

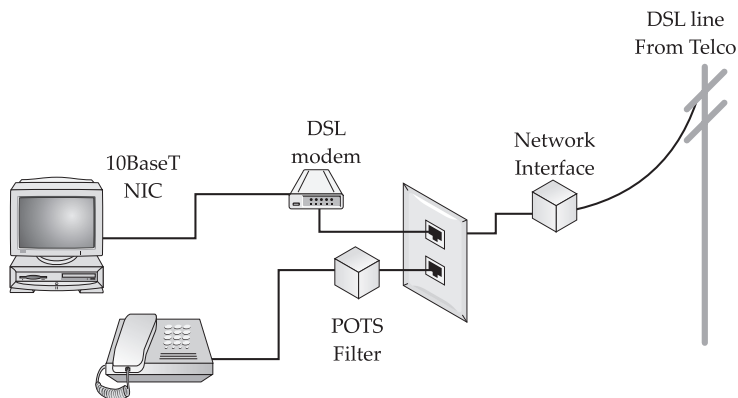


Figure 22-21 DSL connections

Cable

Cable offers a different approach to high-speed Internet access, using regular cable TV cables to serve up lightning-fast speeds. It offers comparable service to DSL with a 384 Kbps upload and 2+ Mbps download. Cable Internet connections are theoretically available anywhere you can get cable TV.

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 22-22 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.

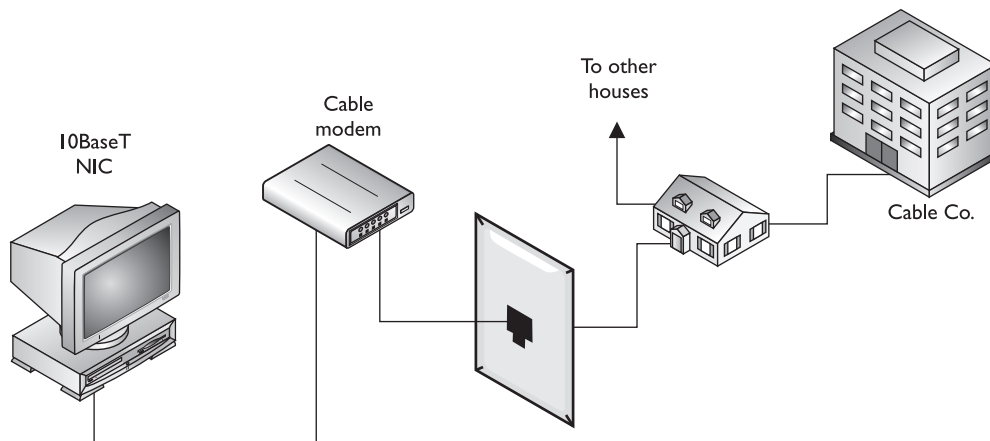


Figure 22-22 Cable connections

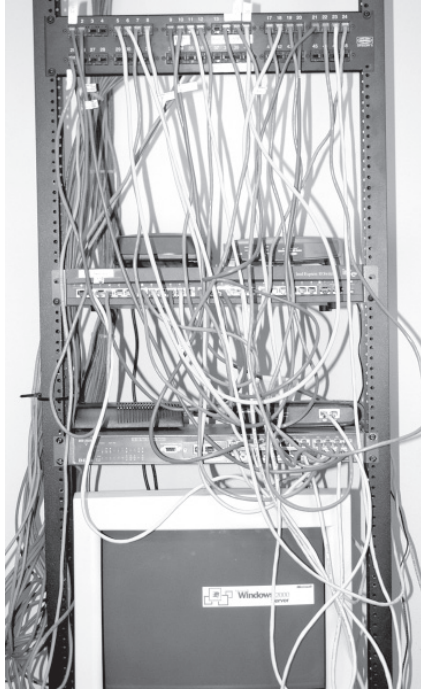


NOTE The term *modem* has been warped and changed beyond recognition in modern networking. Both DSL and cable fully-digital Internet connections use the term *modem* to describe the box that takes the incoming signals from the Internet and translates it into something the PC can understand.

LAN

Most businesses connect their internal local area network (LAN) to an ISP via some hardware solution that Network+ techs deal with. Figure 22-23 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 21, 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.

Figure 22-23
A wiring closet



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.

You spent a good deal of Chapter 21 working through wireless connectivity to a LAN, so I won't rehash any of that here. Suffice it to say that connecting to the Internet via wireless means that you must connect to a LAN that's wired to an ISP or connect to a cellular network. 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.



NOTE One form of wireless communication does not require local wires. *Wireless Broadband* relies on the ISP putting 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? Newer technology still requires the initial setup be done via modem, but the download and the upload go through the dish. 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 U.S.). 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.

Internet Connection Sharing

Windows 98 SE came out with a number of improvements over Windows 98, and one of the most popular was the inclusion of *Internet Connection Sharing (ICS)*. 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. Windows 2000 and Windows XP also provide this handy tool. Figure 22-24 shows a typical setup for ICS. Note the terminology used here. The PC that connects to the Internet and then shares via ICS that connection with 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.

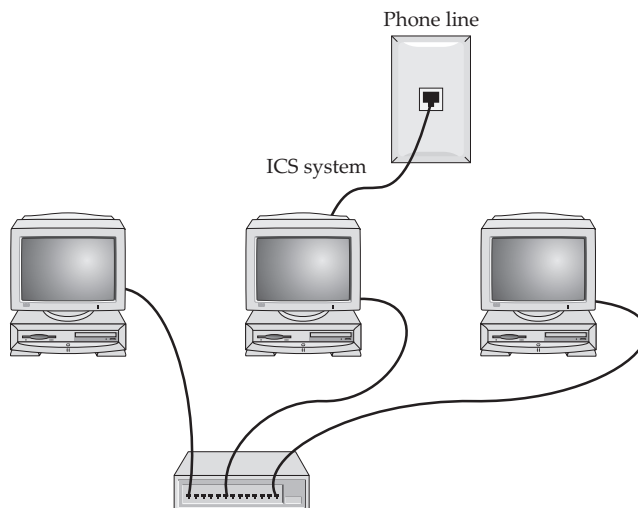
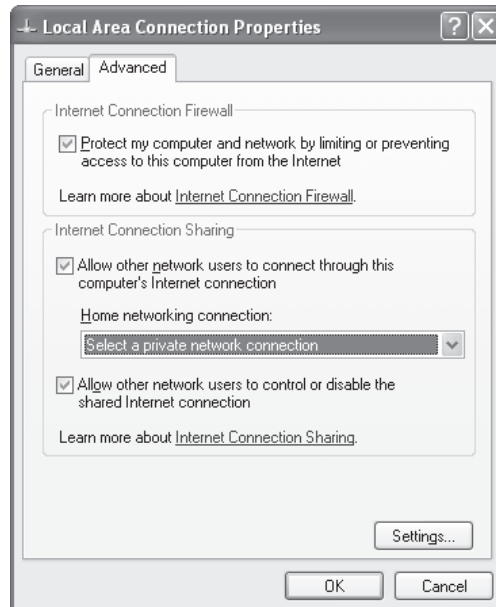


Figure 22-24 Typical ICS setup

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 will also have a NIC that plugs into a hub. Other PCs on the LAN likewise connect to the hub. 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 2000/XP is very simple. Open the properties dialog for My Network Places, and then access the properties of the connection you wish to share. Click the Sharing tab (Windows 2000) 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, Figure 22-25). Clients don't need any special configuration but should simply be set to DHCP for their IP address and other configurations.

Figure 22-25
Enabling Internet
Connection Sharing
in Windows XP



Several manufacturers offer robust, easy-to-configure hardware solutions that enable multiple computers to connect to a single Internet connection. These boxes require very little configuration and provide a level of firewall protection between the primary computer and the Internet. You'll find these boxes more commonly used with DSL and cable connections rather than any sort of dial-up.

Linksys makes a great little DSL/cable router, for example, that offers four 10/100 Ethernet ports for the LAN computers; plus, you can configure it so that to the outside world the router is the PC. It therefore acts as a firewall, protecting your internal network from probing or malicious users from the outside.

The Windows XP Internet Connection Firewall

Once you've established a connection to the Internet, you should start thinking about security. Windows 2000 requires you to use some third-party tool, such as a hardware firewall, but Windows XP offers the *Internet Connection Firewall (ICF)* built into the system. ICF basically stops all uninvited access from the Internet. ICF keeps track of when you initiate communication with a particular machine over your Internet connection and then allows communication back from that same machine. This works whether your connection is a single machine directly dialed into an ISP or a group of networked PCs connecting through an ICS host computer. ICF tracks the communication and blocks anything uninvited. You can implement ICF on the same screen as you would ICS (Figure 22-26).

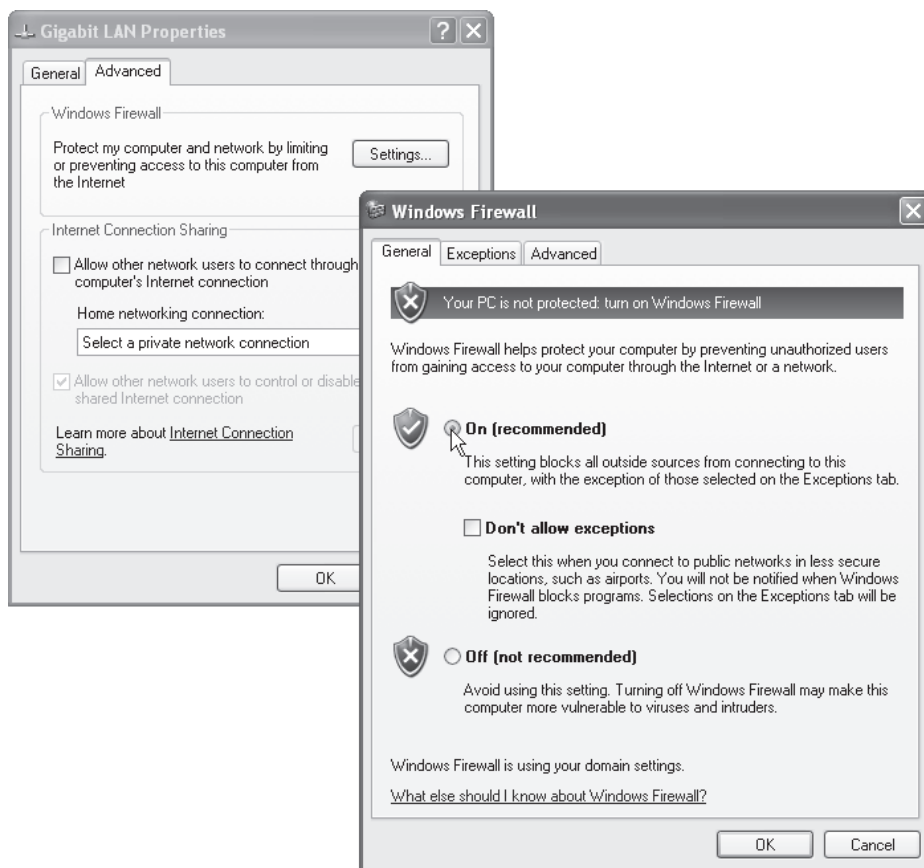


Figure 22-26 Implementing Internet Connection Firewall



NOTE ICF enables you to open up specific computers inside a LAN for specific tasks, such as running an FTP server.

When you're running a LAN, implement ICF only on the machine that directly connects to the Internet. If you enable ICF on other machines on the LAN, you can possibly create problems.

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
- E-mail
- Newsgroups
- FTP
- Telnet
- VoIP

Each of these services (sometimes referred to by the overused term *TCP/IP protocols*) requires a special application, and each of those applications has special settings. You'll look at all five services and learn how to configure them.

The World Wide Web

The Web provides a graphical face for the Internet. Servers running specialized software called *Web servers* provide Web sites and Web pages that you can access 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, but anywhere in the world. Figure 22-27 shows Internet Explorer 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.

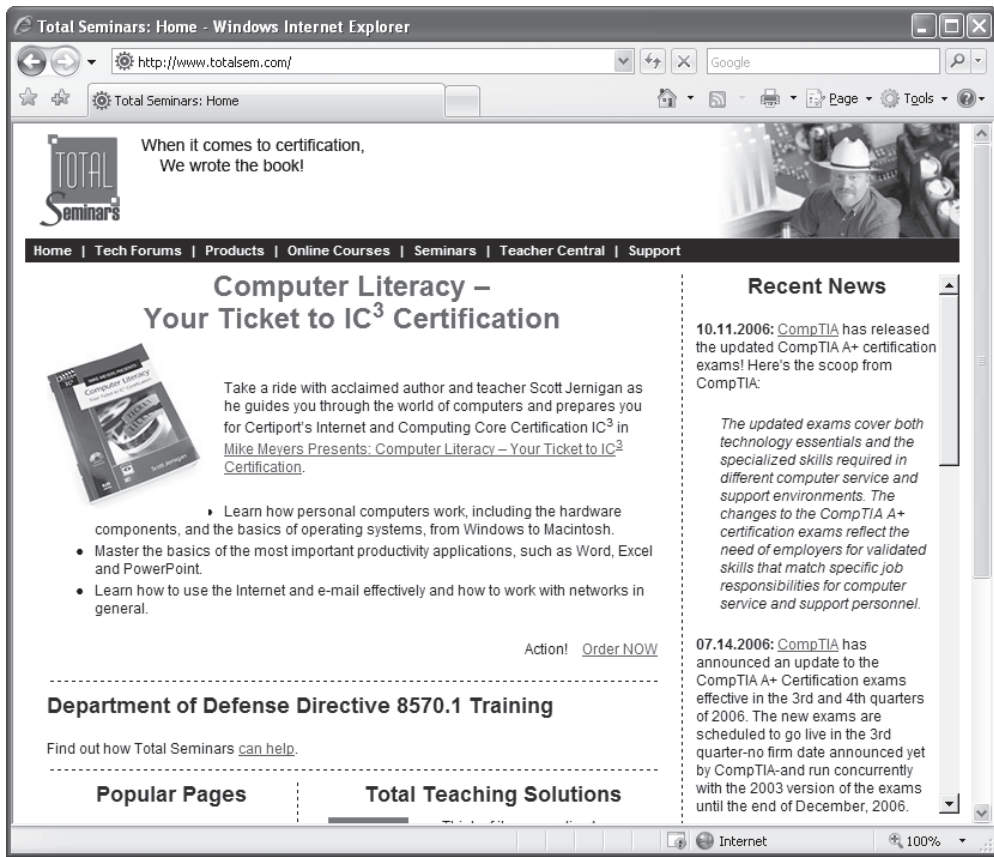


Figure 22-27 Internet Explorer showing a Web page

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.

The command-line tool *ping* may be your best friend for diagnosing TCP/IP errors. Ping always works; you don't need to log on to a server or even log on to a system. Simply type in a DNS name or an IP address. To run ping, get to a command prompt (Start | Run | type CMD | click OK) and type **ping** followed by a DNS name or IP address, like this:

```
c:\>ping www.whitehouse.gov
```

Then press the ENTER key. If the Web server is up, you'll get a reply to that effect.

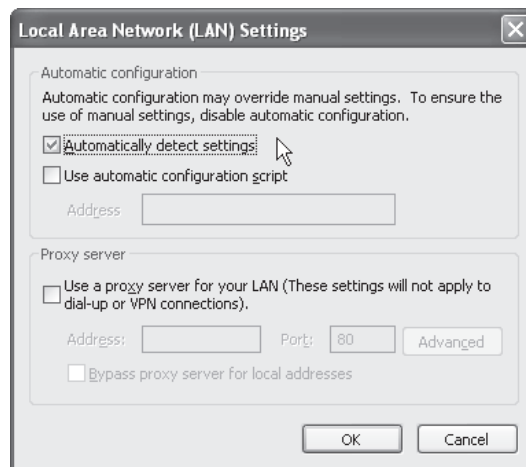
You can even ping yourself: just type **ping 127.0.0.1** (127.0.0.1 is known as the loopback address). If you ping an address and get the famous “Request timed out” message, the device you are trying to ping is not available. Be aware, however, that “Request timed out” messages are fairly common when you use ping on the Internet because many servers turn off the ping reply as a security measure.

Configuring the Browser

Web browsers are highly configurable. On most Web browsers, you can set the default font size, whether it will display graphics, and several other settings. Although all Web browsers support these settings, where you go to make these changes varies dramatically. If you are using the popular Internet Explorer that comes with Windows, configuration tools are found in the Internet Options Control Panel applet or under the Tools menu.

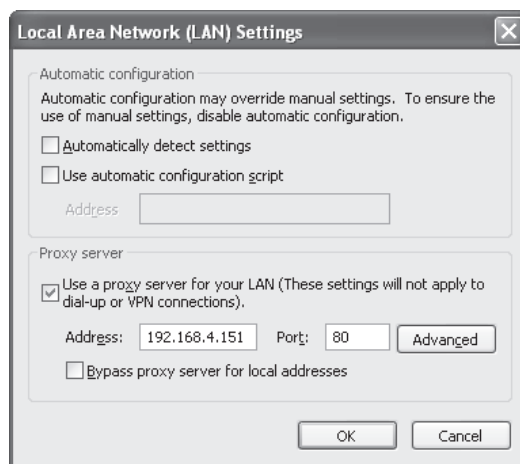
Proxy Server Many corporations use a *proxy server* to filter employee Internet access, and when you’re on their corporate network you will have to set your proxy settings within the Web browser (and any other Internet software you want to use). A *proxy server* is software that enables multiple connections to the Internet to go through one protected PC, much like how 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 21), 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 22-28).

Figure 22-28
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 for a proxy server by clicking the third radio button and simply typing it in (Figure 22-29). Your network administrator or a CompTIA Network+ tech 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 autoconfiguration 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 22-29
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 with names like Java and Active Server Pages. These programs make modern Web sites very 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, like in Figure 22-30), 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 22-31).

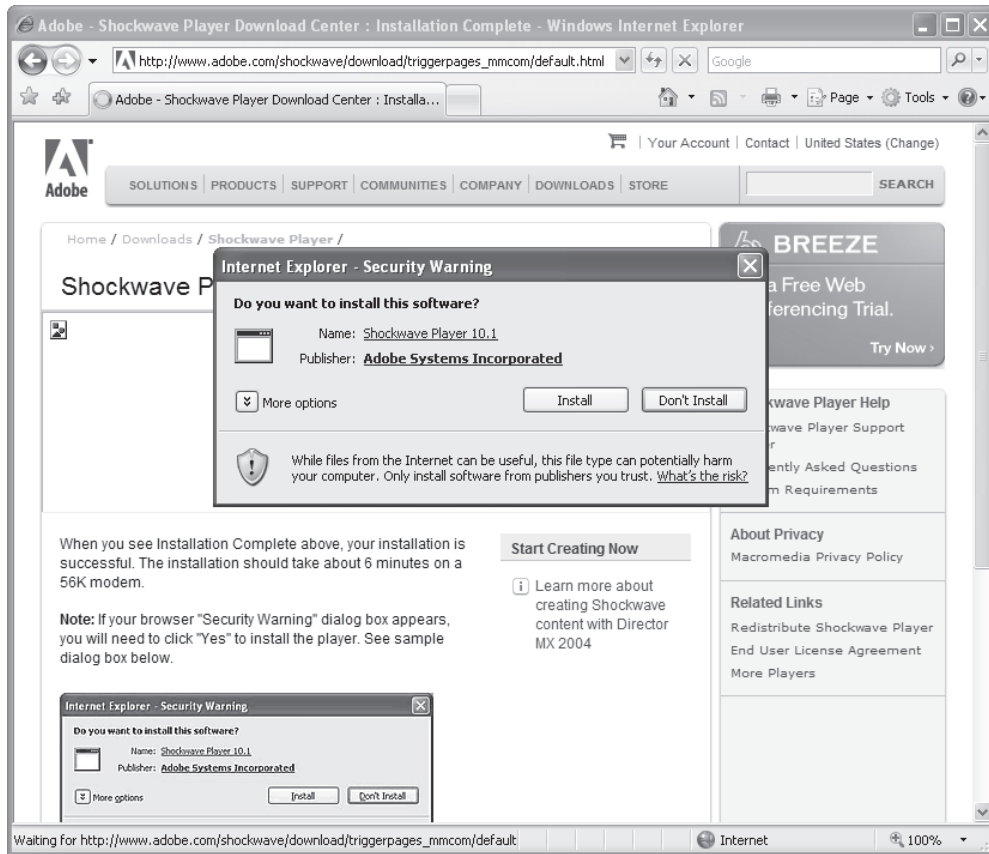
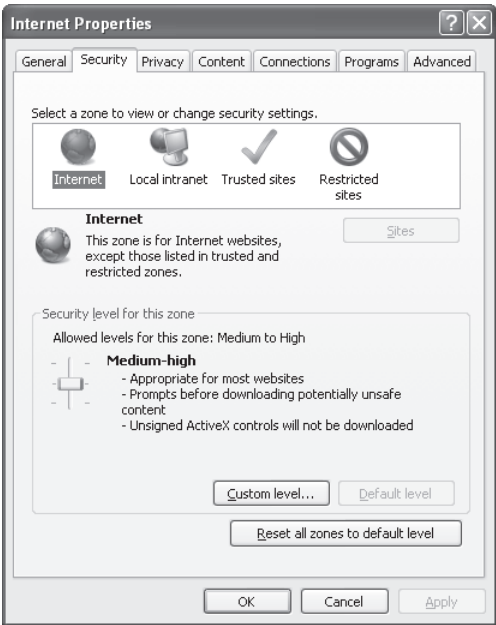


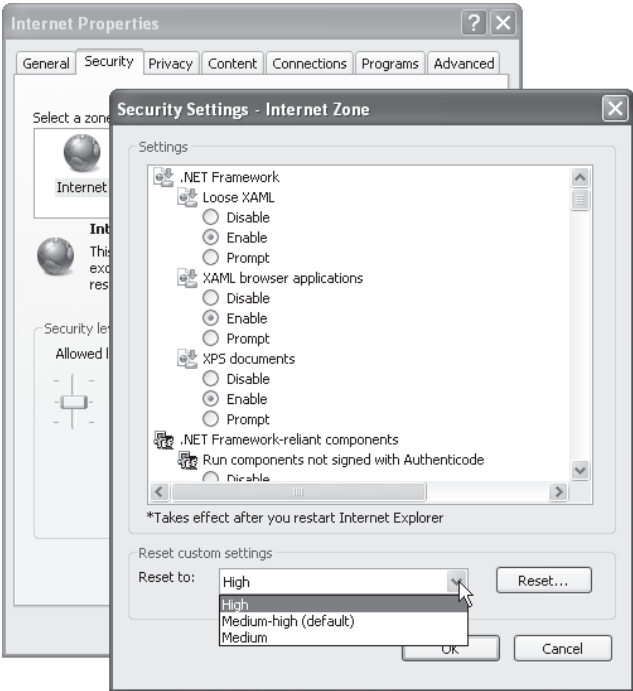
Figure 22-30 Warning message about running ActiveX

Figure 22-31
The Security tab in
the Internet Options
dialog box



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 22-32). 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 22-32.

Figure 22-32
Changing security
settings



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 of encrypting this information, the most common being *HTTP over Secure Sockets Layer (HTTPS)* Web sites. It's easy to tell if a Web site is using HTTPS because the Web address starts with *HTTPS*—instead of just *HTTP*, as shown in Figure 22-33. The Web browser also displays a lock symbol in the lower right-hand corner to remind you that you're using an encrypted connection.

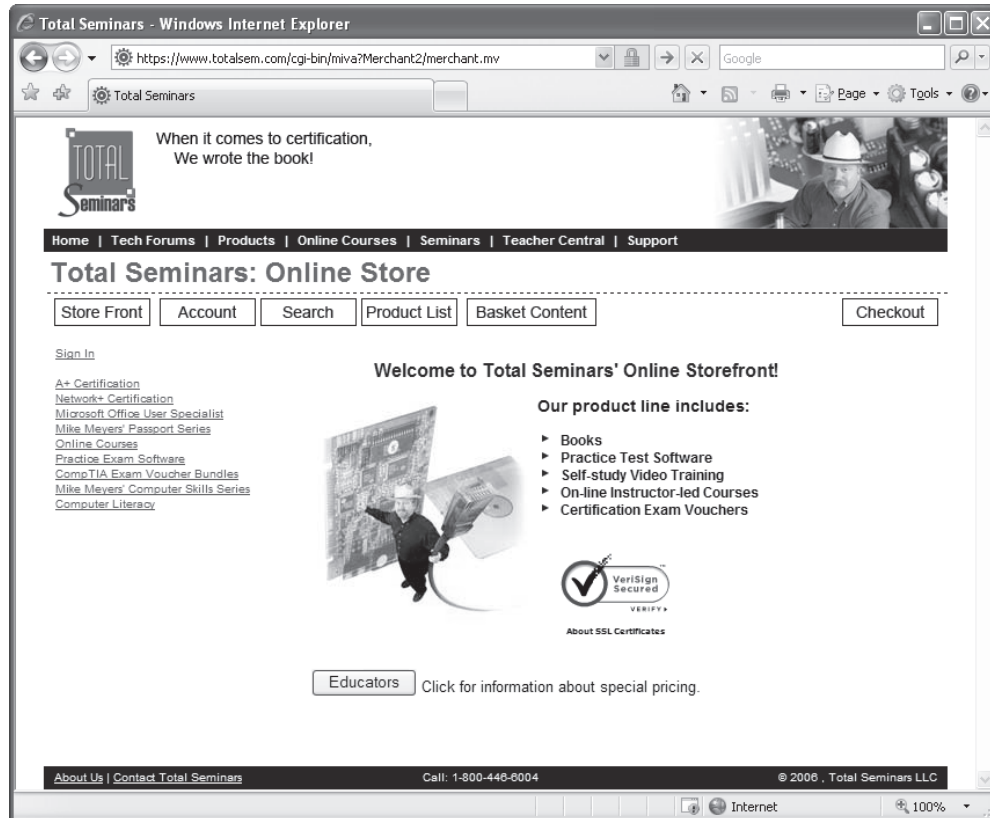


Figure 22-33 A secure Web page (check out the little lock in the lower-right corner)

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 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 23 for the scoop on Trojans and other viruses.

E-mail

You need an e-mail program to access e-mail. The two most popular are Microsoft's Outlook Express 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 22-34 shows e-mail information entered into the Outlook Express Internet Connection Wizard.

Figure 22-34
Adding an e-mail
account to Outlook
Express

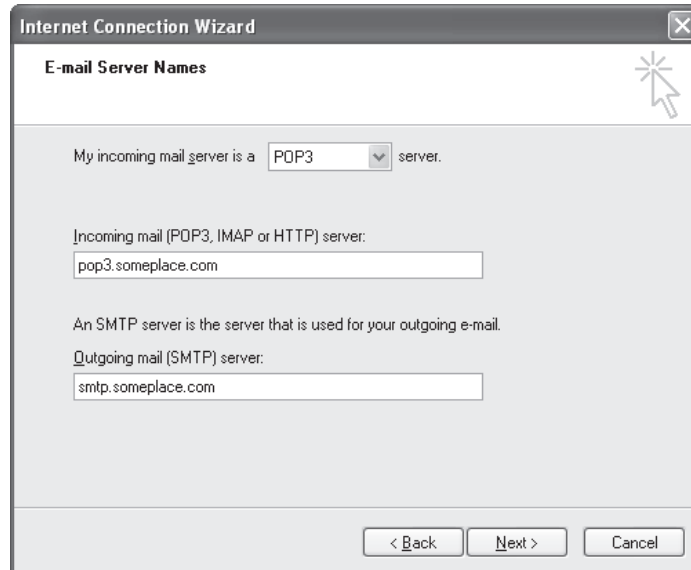
The screenshot shows a window titled "Internet Connection Wizard" with a close button (X) in the top right corner. The main heading is "Internet E-mail Address". Below this, a message states: "Your e-mail address is the address other people use to send e-mail messages to you." There is a text input field labeled "E-mail address:" containing the text "book3@totalsem.com". Below the input field, an example is provided: "For example: someone@microsoft.com". At the bottom of the window, there are three buttons: "< Back", "Next >", and "Cancel". A mouse cursor is pointing at a question mark icon in the top right corner of the dialog area.

The second thing you must add are the names of the *Post Office Protocol version 3* (POP3) or *Internet Message Access Protocol* (IMAP) 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.

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 22-35. All these settings should be provided to you by your ISP. If they are 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 22-35
Adding POP3 and
SMTP information
in Outlook Express



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 22-36. 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 22-37). If my mail starts to work, I know the DNS server is not working.

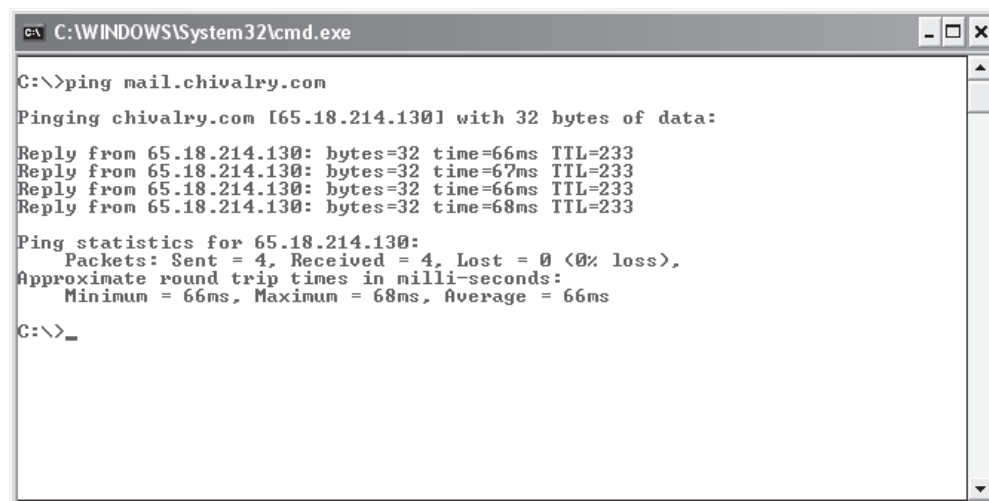
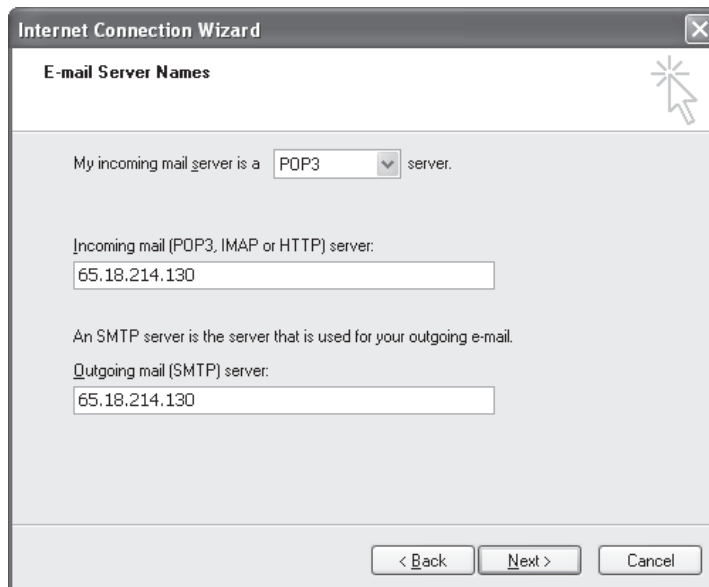


Figure 22-36 Using ping to determine the IP address

Figure 22-37
Entering IP addresses
into POP3 and SMTP
settings

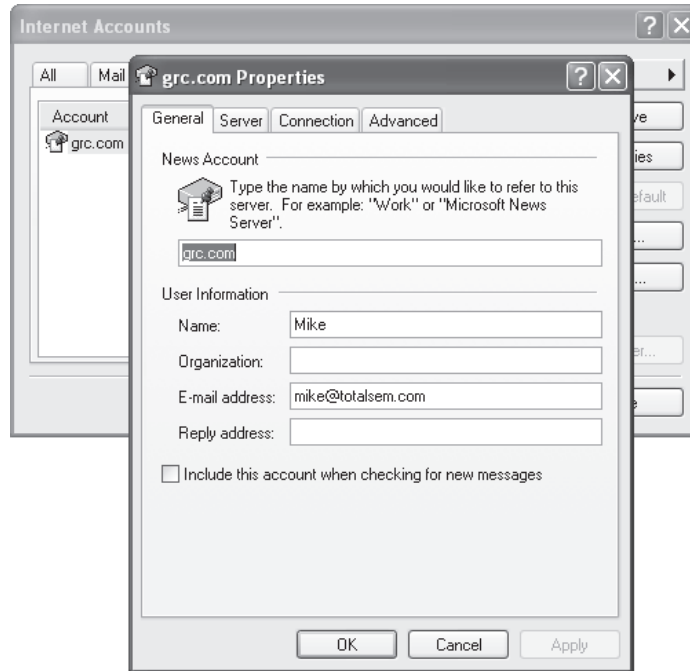


The screenshot shows a Windows-style dialog box titled "Internet Connection Wizard" with a close button (X) in the top right corner. The main heading inside is "E-mail Server Names". Below this, the text reads "My incoming mail server is a POP3 server." where "POP3" is in a dropdown menu. Underneath, it says "Incoming mail (POP3, IMAP or HTTP) server:" followed by a text input field containing "65.18.214.130". Further down, it says "An SMTP server is the server that is used for your outgoing e-mail." followed by "Outgoing mail (SMTP) server:" and another text input field also containing "65.18.214.130". At the bottom right, there are three buttons: "< Back", "Next >", and "Cancel". A mouse cursor is pointing at the top right corner of the dialog box.

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 necessary (Figure 22-38).

Figure 22-38
Configuring Outlook
Express for a news
server



File Transfer Protocol (FTP)

File Transfer Protocol (FTP) is also a great way to share files between systems. FTP server software exists for most operating systems, so FTP provides a great way 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 WS_FTP, although later versions of Internet Explorer and other Web browsers provide support for FTP. Just type in the name of the FTP site. Figure 22-39 shows Internet Explorer accessing <ftp.microsoft.com>.

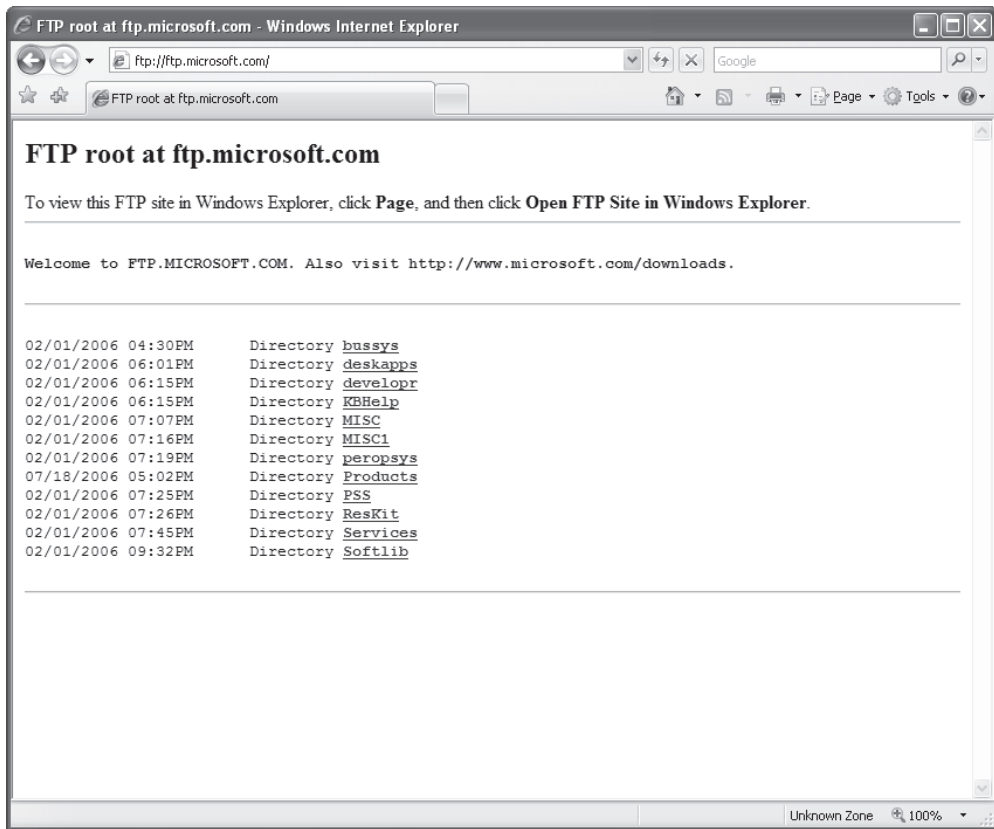


Figure 22-39 Accessing an FTP site in Internet Explorer

Even though 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 in `ftp://ftp.example.com`, you would type in `ftp://scottj@ftp.example.com`.) An anonymous logon works fine for most public FTP sites. Many techs prefer to use third-party programs such as WS_FTP (Figure 22-40) 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!

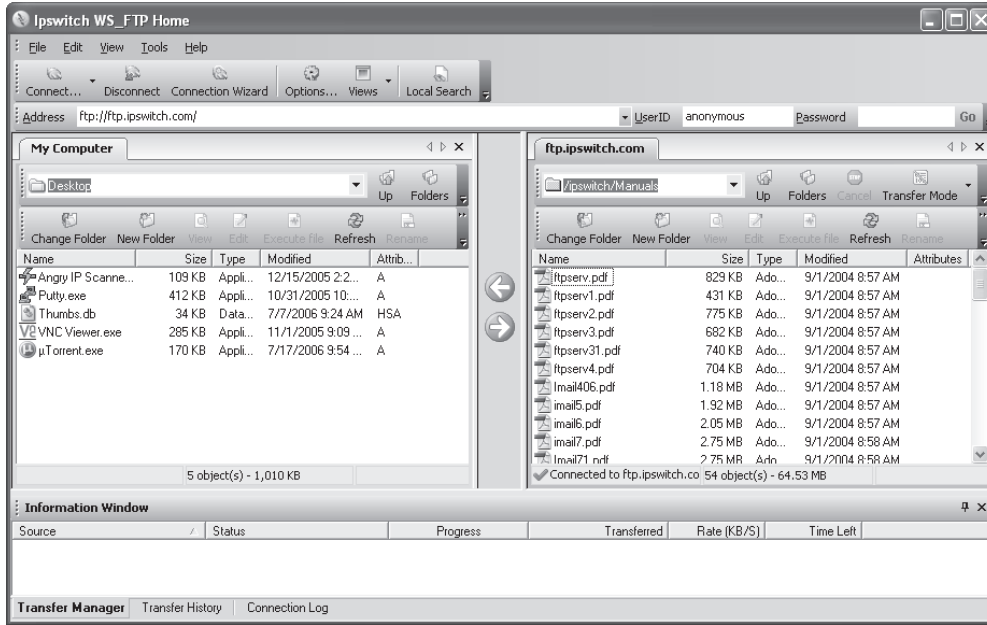


Figure 22-40 WS_FTP

Telnet

Telnet is a terminal emulation program for TCP/IP networks that enables you to connect to a server and run commands on that server 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 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, investigate more sophisticated tools such as SSH (Secure Shell).



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+.

Voice over IP

Voice over IP (VoIP) enables you 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 doesn't refer to a single protocol, but rather to a collection of protocols that make phone calls over the data network possible. Vendors such as Skype and Vonage offer popular VoIP solutions, and many corporations use VoIP for their internal phone networks.

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 types of Windows applications, graphical terminal emulation originally came from third-party companies and was eventually absorbed into the Windows operating system. While 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 22-41 shows VNC in action.



Figure 22-41 VNC



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 22-42 shows Windows Terminal Services running on a Windows 2000 computer.

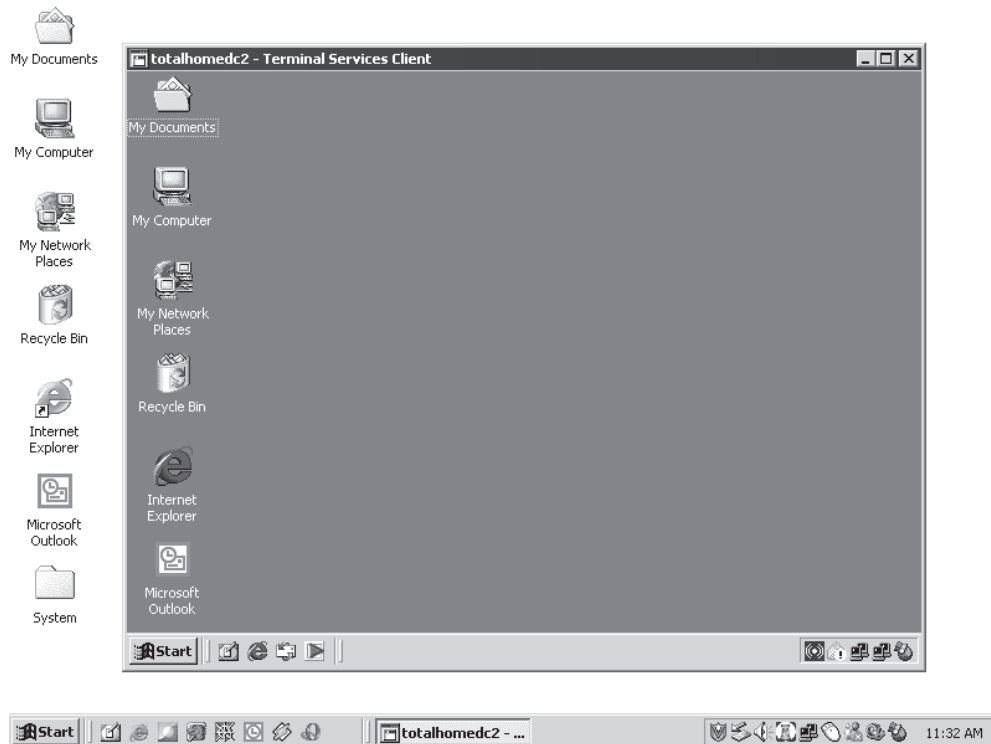
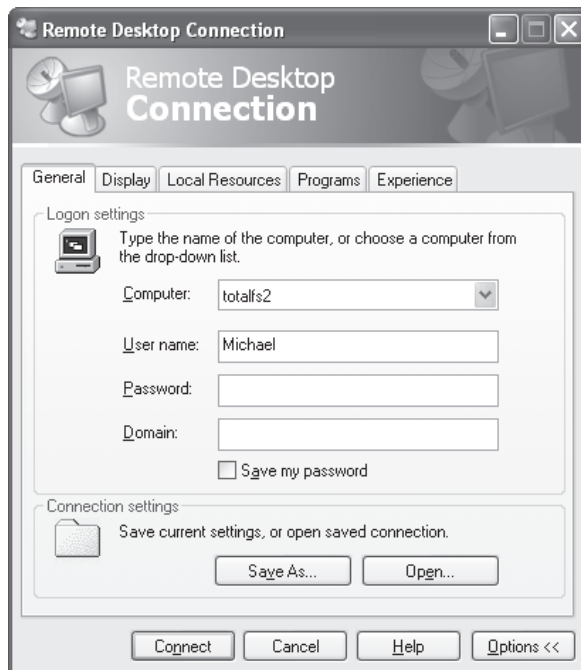


Figure 22-42 Terminal Services

Windows XP offers 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 22-43). It's quite incredible—although it's only for Windows XP.

Figure 22-43
Windows XP
Remote Desktop
Connection
dialog box



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 he or she sees. This would dramatically cut down on the miscommunication that can make a tech's life so tedious. Windows XP's Remote Assistance does just that. Based on the Shared Desktop feature that used to come with the popular MSN Messenger program, *Remote Assistance* allows you to give anyone control of your desktop. If a user has a problem, he or she can request support directly from you. Upon receiving the support request e-mail, you can then log into his or her system and, with permission, take the driver's seat. Figure 22-44 shows Remote Assistance in action.

Figure 22-44
Remote Assistance
in action

Remote Assistance - E-mail an Invitation

Set the invitation to expire

To lessen the chance that someone fraudulently gains access to your computer you can limit the time in which a recipient can accept a Remote Assistance invitation. Specify the duration that this invitation will remain open.

01 Hours

☒ **Require the recipient to use a password**

For security reasons, it is strongly recommended that you set a password that the recipient must use to connect to your computer. Do not use your network or Windows logon password.

Type password: Confirm password:

Important You must communicate the password to the recipient.

Send Invitation

Remote Assistance enables you to 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 him or her nervous! Remote Assistance can help you teach someone how to use a particular application. You can log onto 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 to access and the client goes on the system you use to access the server. On many solutions, the server and the client software are integrated into a single product.

Beyond A+

While the areas covered by the CompTIA A+ Certification exams do a great job on the more common issues of dealing with the Internet, 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 amazing games—classics like Hearts and Backgammon. Entire Web sites are devoted to helping you find playing partners and thereby enjoy thousands of different games (Figure 22-45). 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 22-46).

Figure 22-45
Folks playing
games online

• Ghost Recon	33 players
• Ghost Recon Demo	0 players
• Ghost Recon: Desert Siege	0 players
• Giants: Citizen Kabuto	12 players
• Global Operations	96 players
• Global Operations Public Beta	0 players
• Gore	36 players
• Gore Demo	0 players
• Gruntz	0 players
• Gulf War: Operation Desert Hammer	1 players
• Gunman Chronicles	4 players

H	
• Half-Life	58219 players
• Halo (Xbox)	102 players
• Harley Davidson: Race Around the World	0 players

Figure 22-46
Counter Strike:
Source



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). 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 22-47).

Figure 22-47
World of Warcraft



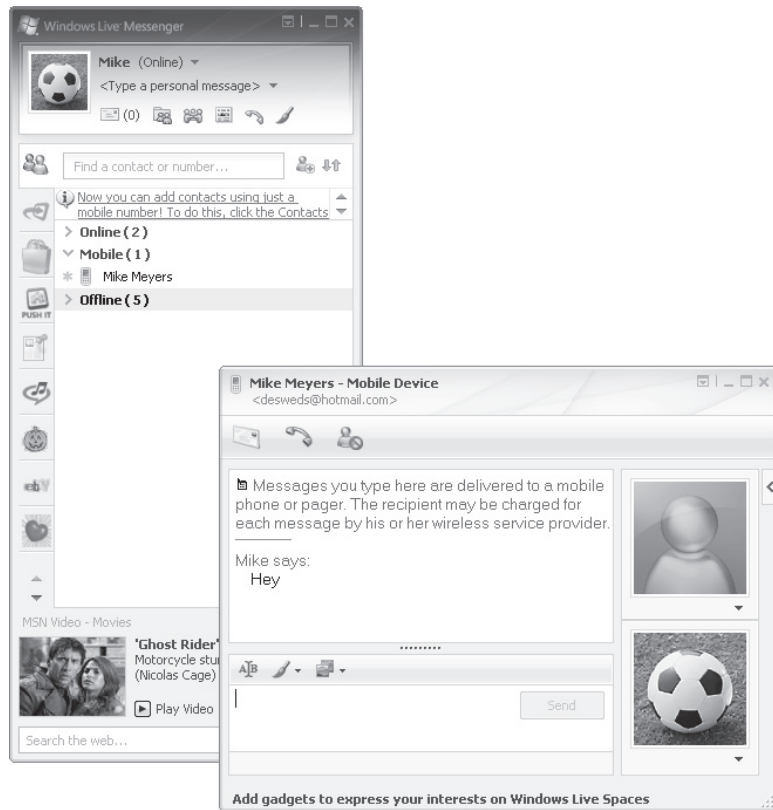
Each of these games employs good old TCP/IP to send information using special ports either reserved by the game itself or by DirectX. For instance, the Quake series of games uses port 26000, while DirectX uses ports 47624 and 2300–2400.

Chatting

If there's one thing we human beings love to do, it's chat. The Internet provides you with a multitude of ways to do so, whether it be by typing or actual talking. Keep in mind that chatting occurs in real time. As fast as you can type or talk, the other person or persons hear or see what you have to say. In order 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 the ability to share files.

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 22-48 shows the popular Microsoft Windows Live Messenger software.

Figure 22-48
Windows Live
Messenger in action



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 the file-sharing computers log onto 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 22-49 shows one of the more popular BitTorrent protocol programs called μ Torrent (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.

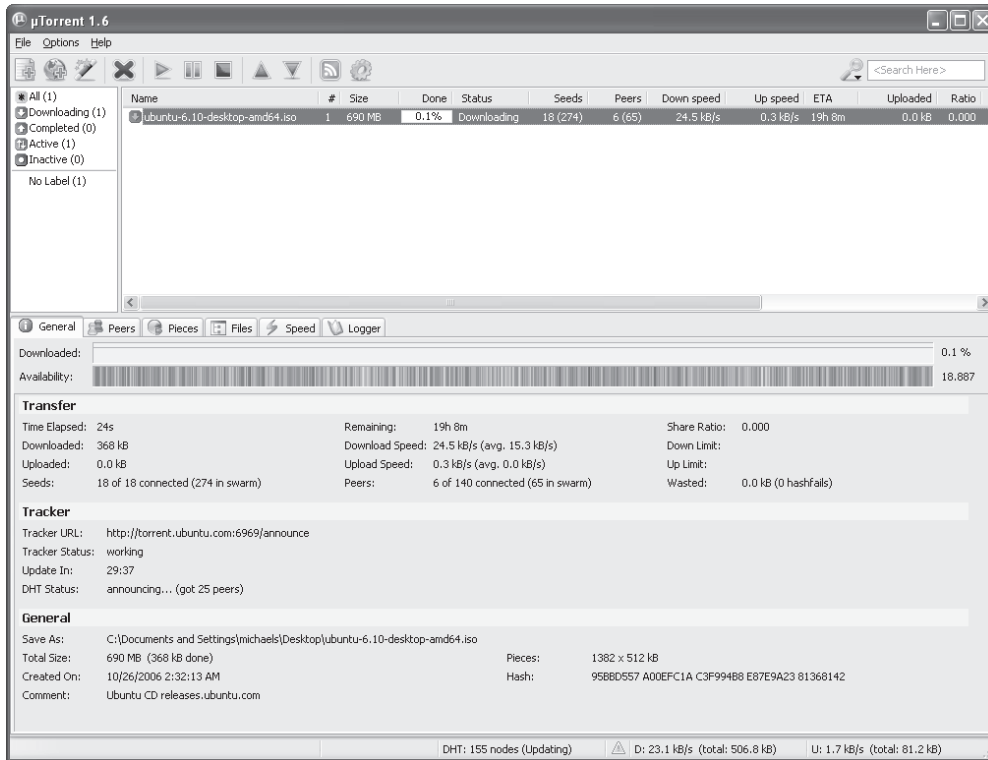


Figure 22-49 µTorrent

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!

Chapter Review Questions

1. Of the four Internet connection options listed below, 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 all that apply.)
 - 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 line 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 all that apply.)
 - 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 all that apply.)
- 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 U.S., 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. **A, D.** Both Telnet and Remote Desktop enable you to access and work on a remote computer. The latter is just prettier!