# 6 Networks: Internet, Intranets, and Extranets

In this chapter...


- Reality Check ***185***
- Inside the Internet ***185***
- Surfing the Net ***194***
- Internet Services ***204***
- Internet Security ***209***
- Intranets and Extranets ***215***
- Summary ***217***


**They Said It...**

*"The whole world is at my fingertips, if only I could type."*

Anonymous

There's no doubt that the Internet is changing our lives. The Internet is likely to be the first place you go when you're planning a trip, trying to avoid crowds at the malls, or researching your child's homework.

Much is written about how we use the Internet to buy goods, find information, or make a claim in the cyber gold rush. However, what is the Internet—really—and how does it work? What is an Intranet or an Extranet? In this chapter, I'll take you behind the scenes of the Internet, Intranets, and Extranets and explore how these magic marvels work. You'll learn about:

- the Internet
- a bit of Internet history
- the Internet backroom
- the international flavor
- a walk behind the scenes
- surfing the Net
- the Internet connection
- Internet addresses
- Internet protocols
- Internet services
- the World Wide Web
- Internet security
- Internet privacy
- Intranets and Extranets

## REALITY CHECK

It wasn't too long ago that a former intern at Salomon Brothers, an international investment banking firm, told colleagues he was leaving the company to sell books on the Internet. Everyone laughed quietly and joked that he'd be back in a year.

Selling books on the Internet was an outlandish idea, especially when you consider leaving a promising position on Wall Street. A year passed and he never returned. However, his former colleagues did hear from him again when he became the "Man of the Year" for *Time* magazine. His name is Jeff Bezos. His company is Amazon.com.

The Internet is a wide area network that links computers, servers, and other networking devices. However, Bezos' imagination, and that of a long list of other visionaries, has transformed network hardware into a revolutionary concept that changes the way we conduct business.

Within a few years, Bezos has taken on the giants of the book publishing industry to become one of the major booksellers around the world. He is leading the gold rush in which practically anyone who has a good business idea can turn it into a viable business venture by going online.

## INSIDE THE INTERNET

The Internet is a network of networks that is owned by no one and everyone. I agree this sounds more like legal mumbo jumbo, but this is a concise definition of the Internet. In previous chapters of this book you learned how cables, devices, and computers are linked to form a computer network called a local area network (LAN) (see Chapter 4).

A large LAN can be subdivided into smaller LANs called segments. In a sense, this is the same as the Internet except on a smaller scale. The Internet is a wide area network (see Chapter 5) of global proportions that is comprised of tens of thousands of segments.

Your company owns segments of your company's LAN. However, each segment on the Internet is independently owned by the organization that created the segment.

Let's say that the Internet is a co-op apartment building (Figure 6.1) in which apartments are network segments and the building itself is the Internet. Each resident owns his or her apartment, just like each organization owns its segment of the Internet.

Each apartment contains different items based on the apartment owner's wants. Some apartments may have a piano, others a monster TV, still others a professional kitchen. The organization that runs the co-op building does not tell each apartment owner what they can or cannot have in their apartment.

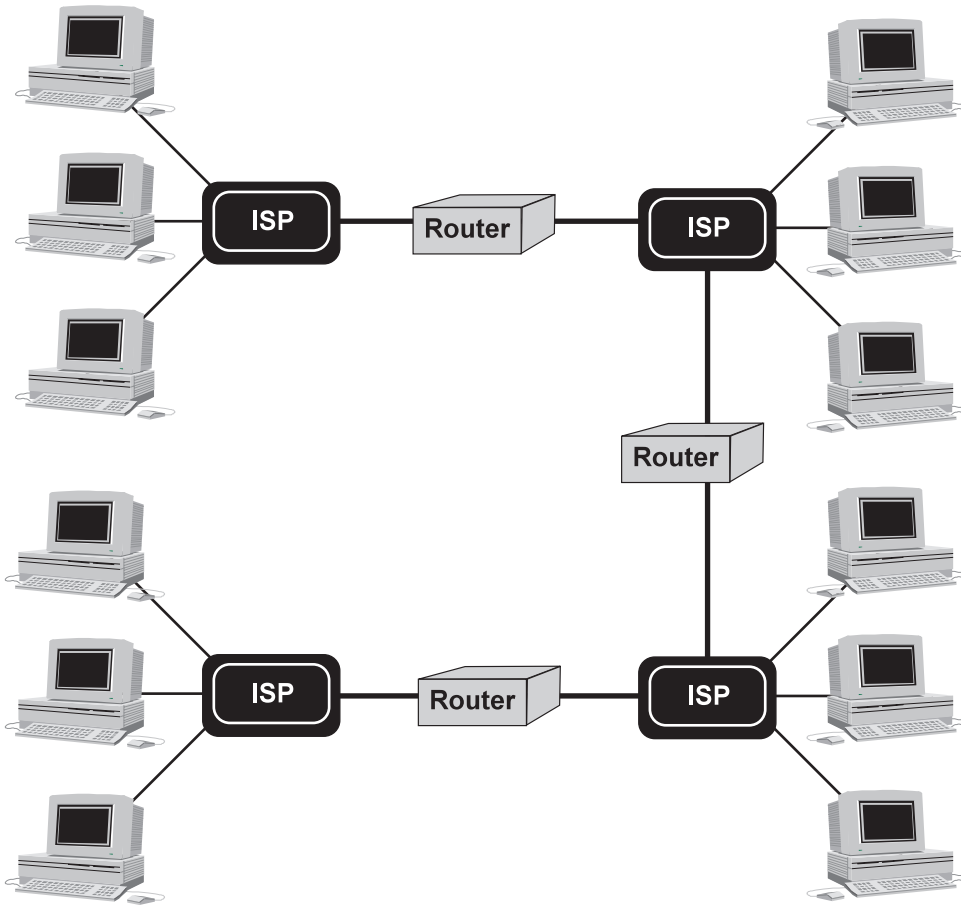


***Figure 6.1***
*The Internet is a network of networks. (Redrawn with permission from Prentice Hall. Comer, Douglas E. The Internet Book. Englewood Cliffs, NJ: Prentice Hall, 1997, p. 110.)*

The Internet works the same way, in that some segments will store games, others music, and still others e-commerce businesses The organization that oversees the Internet has no authority to control the material stored on any segment of it.

Visitors to the co-op apartment can wander the common hallways and knock on doors of any apartment. The apartment owner opens the door, then decides whether or not to allow the visitor into the apartment.

In Internet terms, you and I can log on the Internet and use the vast array of network cables to knock on the doors of Web sites. The owner of each Web site deter-

mines if we are allowed in to visit. The Internet cables, which are basically the telephone network, are like the hallways in a co-op apartment building, and the Web sites are located on segments of the Internet.

Once inside an apartment, the apartment owner grants us permission to freely roam the apartment or restricts us to certain rooms or activities, such as watching the monster TV, but not allowing us to change the channel. This is similar to restrictions found on some Web sites, where the Web site owner controls which Web pages you can access.

The co-op building is managed by a consortium of apartment owners whose job it is to establish rules for using the common areas of the building. For example, visitors must enter the co-op building using designated entrances. They must use the elevator to reach the desired floor. They must use the apartment number to identify the apartment they want to visit, and they must knock on the door of the apartment and wait to be invited into the apartment.

You probably surmise that the Internet also has rules developed by a consortium of segment owners. These rules are called *protocols* and they define the standards that must be followed for interacting with segments of the Internet.

For example, the entranceway to the Internet is through a portal usually supplied by an Internet Service Provider (ISP), which is discussed later in this chapter. After logging on the Internet, we use a Web site address to locate a segment of the Internet and we use our browser to knock on the door of the site.

The Web site follows Internet protocols and displays a page called a *home page*, which greets us similarly to how the apartment owner greets us at the door. Likewise, through our browser we follow certain protocols to interact with the Web site just as we follow certain mannerisms when interacting with apartment owner.

So the original statement that the Internet is a network of networks that is owned by no one and everyone is true. No one person owns the co-op apartment building, yet each apartment owner owns the co-op apartment building.

**Tech Talk**

**Home page: the first Web page that is displayed when you visit a Web site.**

## A Bit of History

For once, the federal government has done one thing correctly by giving birth to the Internet. The U.S. Department of Defense launched a project in 1969 to electronically connect government scientists at universities throughout the United States so they could easily, quickly, and securely share information.

This project, the Internet, made its way into the world in a "delivery room" tucked away in a corner of the University of California, Los Angeles. The delivery room was really a computer room and the Internet was known as ARPANET. (Who but the government would give their new offspring a name like ARPANET?) ARPANET is the acronym for Advanced Research Projects Agency Network.

An objective of ARPANET was to keep lines of communications flowing in the event of a nuclear attack. Today, this may seem less of an issue than in the days of the Cold War, when the U.S. Department of Defense thought such an attack was probable.

Engineers used technology developed in 1962 by the Rand Corporation, one of the pioneers in the computer industry, to ensure that data could be transmitted over the network even if a portion of the network became disabled. The technology is called *packet switching* (see Chapter 5).

**Tech Talk**

**Packet switching: the technique of dividing information into small pieces and placing each piece into an electronic envelope called a packet, which is transmitted over a network.**

Information that was transmitted over the ARPANET was stored in packets, which also contained the destination address, the sender's address, and error checking information. A packet was sent to the destination computer by traveling along one of multiple paths. If a path (transmission line) became inoperable, then a device called a switch, first created by the Bolt Beranek and Newman (BBN) company, rerouted the packet along a different path.

The dangers imposed by the Cold War dissipated by 1984 and so did ARPANET. However, with approximately 500 universities actively using ARPANET, it didn't make sense to disband it. Instead, ARPANET was renamed the Internet and three years later turned over to the National Science Foundation to administer.

Faculty, students, and computer hobbyists who managed to get onto the Internet soon found its services very useful. You're probably familiar with the Internet e-mail service; other Internet services, such as newsgroups, Telnet, and FTP might be unfamiliar.

**Tech Talk**

**Internet services: various methods that are available to exchange information over the Internet, such as e-mail, Telnet, FTP, and newsgroups.**

A *newsgroup*, sometimes called a bulletin board, is a place on the Internet where someone can post a notice, a question, or an answer to a posted question. Let's say a

student is tackling a technology problem and needs help. She can post the problem on a newsgroup and wait for another Internet user to post a solution. Newsgroups cover a variety of topics and still exist today, although commercial Web sites are taking over the role by offering interactive chat rooms.

As discussed later in this chapter, Telnet and FTP let you connect to a remote computer linked to the Internet. The Telnet service enables you to log on the remote computer and interact with it as if it was on your desk. The FTP service enables you to transfer files between your computer and the remote computer much like how you copy a file from a floppy disk to a hard disk. Both Telnet and FTP are also available today on the Internet.

Interacting with the Internet in its early days required good technical skills, since you had to log on the remote computer and locate the file that contained the desired information using commands. There was no one greeting you at the door with a home page.

The first major improvement to the Internet came in 1989 when the World Wide Web was created. The World Wide Web is a way information is organized on the Internet (see "The World Wide Web" on page 207).

The Internet and the early World Wide Web were text-based and lacked the graphical elements that Web pages have today. Anyone who wanted to surf the Internet in those days had to use special programs that required them to learn commands to interact with those programs. Commands were typed into the computer, primitive by today's standards in which we point and click our way through the Internet.

This system changed in 1993 when engineers that the University of Illinois developed Mosaic, the world's first browser for the World Wide Web. Internet users were no longer required to learn strange-sounding commands to find information on the Internet. Instead, they could point and click, then see information in a mixture of text and graphics.

## The Internet Backroom

Every organization has a "backroom" where the powerbrokers make decisions about how the organization will run. The co-op apartment building has the co-op board, composed of apartment owners who establish and enforce rules for operating the apartment building. The Internet, too, has a group that creates rules for it. Actually, there are several groups, each of which oversees an aspect of Internet operations.

In 1992, a nonprofit group called the Internet Society (ISOC) formed to develop policies to "govern" the Internet. (Govern is probably too strong a word to use to describe the ISOC's purpose.) The ISOC formally adopts standards recommended by leaders of a particular aspect of the Internet. Once adopted, hardware manufacturers

and software developers are responsible for making sure their products adhere to the standards. However, there is no Internet police force to catch violators. Instead, the desire to have their products work seamlessly with the Internet is the only motivation necessary to enforce the standards.

Internet Corporation for Assigned Names and Numbers (ICANN) handles policies that affect Internet addresses. ICANN is the successor of the Internet Assigned Numbers Authority (IANA), which was the original government agency selected to manage Internet addressing standards.

ICANN is a private international organization. This is the group that created .com, .net, .org, and other top-level domain names, which are discussed later in this chapter. The Internet Network Information Center (InterNIC) is the service run by Network Solutions, Inc. to register Internet names and addresses.

In addition to managing Internet addresses, there are two other aspects of the Internet operation that needed to be organized. These are hardware and software used to keep network traffic flowing, and the way information is accessed over the World Wide Web.

Traffic standards, as I like to call them, are created by the Internet Engineering Task Force. The IETF is a branch of the Internet Society and the Internet Operator's Providers Services (IOPS.ORG). The IETF focuses on standardizing the TCP/IP protocol, which is discussed later in this chapter. IOPS.ORG is a consortium of telecommunications carriers, such as AT&T, GTE, and MCI WorldCom, that set hardware standards to ensure that data is routed efficiently over the Internet.

**Tech Talk**

**TCP/IP: protocols used to transmit data over the Internet.**

The World Wide Web Consortium (W3C) sets standards for how information is shared on the World Wide Web by using a browser to link Web pages. The three leading members of the 150-member W3C are The MIT Laboratory for Computer Science, the French-based National Institute for Research in Computer Science and Automation, and Kieo University in Japan.

## The International Flavor

The Internet evolved from a computer network financed by the U.S. Department of Defense and has grown to encompass areas around the world that are serviced by a telephone network. This includes North and South America, Europe, Asia, Australia, and some African countries.

Compatibility among national telephone networks is the key to giving the Internet worldwide reach. The Post, Telegraph, and Telephone (PPT) agency within each country manages telephone networks in many European countries. For example, this enables the German telephone network to communicate seamlessly with the Italian telephone network.

On a more international scale, the International Telecommunications Union (ITU) is an organization of national telephone companies that adopt telecommunication standards which, if adhered to, ensure continuity among telephone networks around the world.

However, a dilemma arose when the ITU adopted the X.25 network protocol (see Chapter 5). The X.25 protocol is an older transmission protocol used for computer networks and is incompatible with TCP/IP, which is the protocol used to transmit data over the Internet.

By the mid-1990s, a group of universities and research labs formed a cooperative and created EBONE, which is the European Internet Backbone. Members of the cooperative pay a fee that goes toward leasing dedicated lines between the EBONE and the U.S. Internet.

EBONE is divided into three layers called levels (Figure 6.2). Each country is connected to the top level of EBONE. You can think of this as a network of countries. Each country has its own Internet network that connects regions within the country. Think of this as a network of regions inside a country. The lowest level of EBONE exists within each region and is used to link local Internet sites to the regional Internet. Regional Internet networks consist of a network of Internet sites.

## A Walk Behind the Scenes

Let's take a behind-the-scenes look at what happens when you the surf the Net. Your trip begins when your computer dials your ISP using a dial-up program. The dial-up program handles communication between your computer and the ISP's computer.

An ISP is an organization that sells connections to the Internet at a reasonable price. Anyone can become an ISP if they are willing to invest in hardware and communications lines. The objective of an ISP is to lease a dedicated T carrier-line from the telephone company for a monthly fee, then sell a portion of that time to people like you and me for a smaller monthly fee.

Before you made your first call with your computer, you needed to do a little "under the hood" tinkering to get the dial-up program working properly. This tinkering made sure your computer and the ISP's computer used the same communications protocol (see Chapter 4).

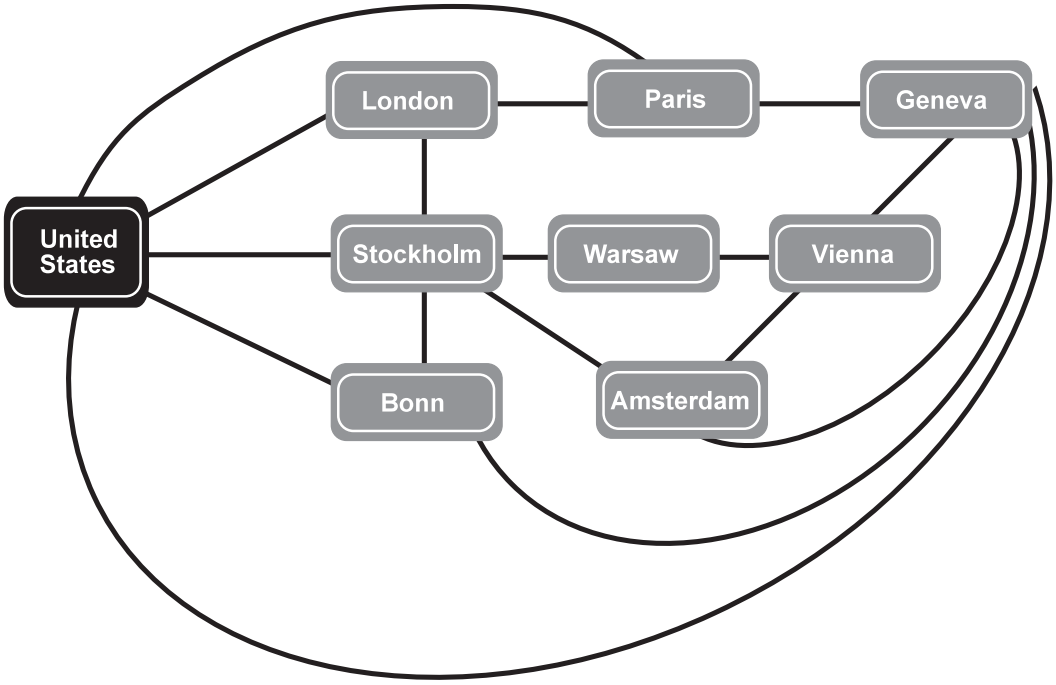


***Figure 6.2***
*EBONE is the European Internet backbone that links regional networks in several countries to the Internet backbone. (Redrawn with permission from Prentice Hall. Comer, Douglas E. The Internet Book. Englewood Cliffs, NJ: Prentice Hall, 1997, p. 77.)*

**Tech Talk**

**Internet service provider (ISP): an organization that provides inexpensive access to the Internet backbone.**

Once the dial-up software is configured (the technical term for tinkering under the hood), a click on the dial-up icon begins your trip. Your modem dials the ISP's telephone number, then waits for the ISP's computer to answer the call. Your ISP has rooms of modems that connect the telephone company's central office to its local area network using T carrier-line (Figure 6.3) (see also Chapter 5).

Your modem and the ISP's go through a handshaking procedure during which they say "hello" to each other and agree to the transmission speed. After these formalities, the ISP's computer requests your ID and password before giving you access to the ISP's local area network.

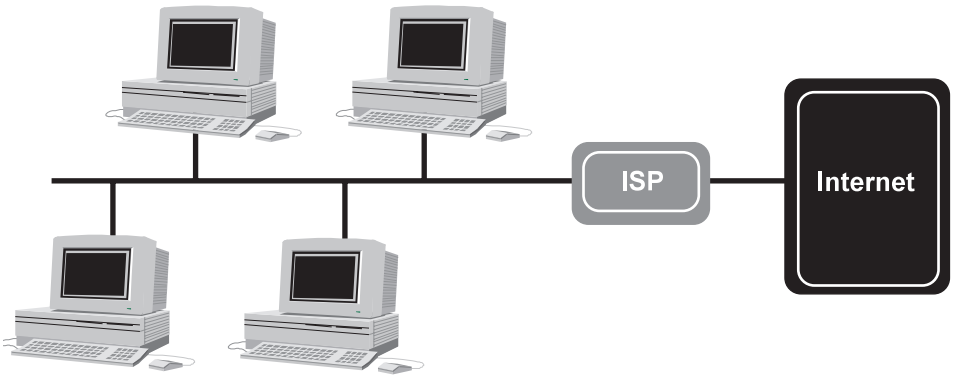


**Figure 6.3**
*An Internet service provider links computers to the Internet backbone. (Redrawn with permission from Prentice Hall. Dodd, Annabel Z. The Essential Guide to Telecommunications. Upper Saddle River, NJ: Prentice Hall, 2000, p. 308.)*

You can enter your ID and password into the dial-up software either when you set up the software or every time you connect to the ISP. The ID and the password are assigned to you when you sign up with the ISP.

The ISP's computer receives your ID and password, then compares them to data stored in its computer. If the data don't match, the ISP's computer transmits an error message to your computer prompting you to re-enter the information. Otherwise, the ISP's computer sends a message indicating that you have successfully connected to their network.

The ISP also assigns your computer a temporary Internet address called an IP address, which is discussed in detail later in this chapter. The IP address is similar to having your own "www…com" except your address is a number that is reassigned when you disconnect from the ISP.

**Tech Talk**

**IP address: Internet protocol address, which is the unique address assigned to every network device.**

The connection to the ISP is similar to being connected to your company's local area network. That is, the line of communication to the network is open and you need to run software on your computer that utilizes services on the LAN. After the connection is made, we click the browser icon and the ISP is transformed into our Internet portal.

**Tech Talk**

**Portal: the place where you enter the Internet.**

## SURFING THE NET

You can surf the Internet by entering the name of the Web site you want to visit into the browser, then pressing the Enter key or clicking highlighted text or a graph on the current Web page. In either case, the browser transmits the Web site name to the ISP's computer.

What you think of as a Web site's address is really just an alias because the IP address is the true address. For example, *www.amazon.com* is an alias for a specific IP address. We can remember the alias easier than trying to remember an IP address. (See the "Internet Address" section later in this chapter.)

The alias and the IP address are stored online in an Internet directory ( Figure 6.4), which is used to compare the alias a user enters into a browser with the IP address.

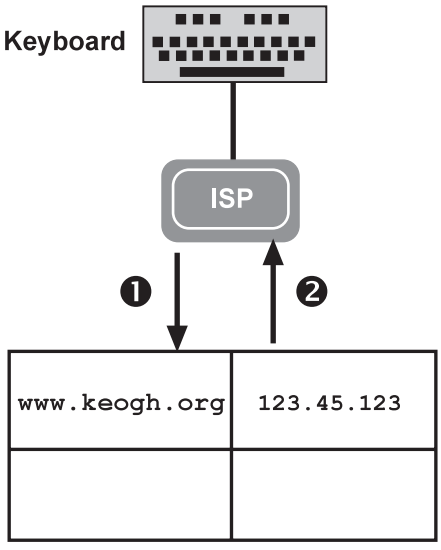


**Figure 6.4**
*A name of an Internet site is translated into a unique Internet address before connecting to the site.*

The Internet directory is a database stored at various central computers on the Internet and maintained by the Internet Network Information Center (see "The Internet Backroom" on page 189).

The ISP sends a request for the location to one of the databases and within a fraction of a second the Internet address is returned to the ISP. The ISP sends a message to the Internet address asking for a particular file, which is typically *index.html* unless your browser specified a different file name.

The *index.html* is the name of the file that contains the first Web page of a Web site, which is called the Web site's home page. This is the first Web page you see when visiting a Web site. A Web page consists of text that appears in the browser and includes instructions, called source code, that tell your browser how to display the text.

These instructions are written in one or a combination of Internet languages that include HTML, XML, and Java. Some of these instructions tell the browser to display text in bold or to align it left, right, or center. Other instructions direct your browser to request and display other files that contain graphics, video, or sound, for example.

**Tech Talk**

**Source code: the instructions that tell a browser how to display a Web page. You can see the source code by placing the cursor on the Web page, clicking the right mouse button, then selecting View Source from the pop-up menu.**
**Hypertext: text or a graphic that is associated with and linked to other text on a Web page or associated with another Web page.**

You've probably noticed that some text is highlighted on a Web page. These are called hypertext links because the text references other information and by clicking the hypertext, the browser displays the referenced information. Hypertext can reference information contained in the same file, called a bookmark, or reference information stored in a different file, which may be a different Web page.

When you click hypertext, the browser looks at the name associated with the hypertext and determines if it is a bookmark or another Web page. It knows the difference by the way the Web programmer encodes the instruction.

If the name is a bookmark, then the browser locates the bookmark on the Web page and displays the corresponding text and graphics. Otherwise, the browser looks up the Internet address of the Web page name, contacts that Web site, and requests the file.

Sometimes hypertext links to a different Web site, in which case the browser requests the *index.html* file for that site. Other times hypertext links to a specific file at a

Web site. For example, I visited the CNN/*Sports Illustrated* Web site and found hypertext linked to baseball. Baseball is another page on the CNN/*SportsIllustrated* site.

As you've noticed, surfing the Internet is really requesting that a file contained on a remote computer be copied to your computer. Your browser then follows instructions in the file to properly display text and graphics.

## JAVA™ PERKS UP A WEB PAGE

The office guru talks about Java™ in the coffee room at work—and her conversation has nothing to do with refreshments. Java is a programming language that consists of words that have special meaning to programmers and to your computer.

Programmers use programming languages to tell your computer how to do something, such as how to become a word processor. Java™ is one of many programming languages and is one that is used to give intelligence to Web pages.

For example, we've all seen scrolling text across a Web page. This is possible because a programmer writes a small Java™ program called an applet that instructs your computer about how to scroll text.

Engineers who created Java™ to work with a browser used a clever design to enable Java™ programs to run on any kind of computer, including PC, Mac, and UNIX computers. The design centers on using a Java™ engine.

Although the name conjures images of a device powering a rocket into space, the Java™ engine is much simpler to understand. It is a program designed for a particular computer. This means there is a Java™ engine for a PC and another for a Mac, and so on. The engine's job is to translate a Java™ program into instructions that a specific computer can understand.

Here's how it works. The programmer who created the Web page includes instructions written in the Java™ language as part of the page. Java™ instructions are clearly identified, so when the browser comes across them while reading HTML and XML instructions, it stops and runs the Java™ engine.

The Java™ engine picks up where the browser left off and translates the Java™ instruction embedded in the Web page and directs the computer to do something, such as scroll text at a particular location on the screen. Once the Java™ instructions are translated, the Java™ engine turns control back to the browser, which continues to read and follow the rest of the instructions on the Web page.

Java™ has an advantage over other programming languages because it is machine-independent. Programs written in other programming languages can run on specific computers, but not all computers.

For example, programs that run on a computer running Linux, an operating system used on many Internet servers, cannot run on a computer running Windows. Software manufacturers need to create a different version of their program for each type of computer. However, programs written in Java™ can run on any computer.

## The Internet Connection

The Internet is seen as the modern day gold rush in which everyone is trying to stake their claim to a site that might be sitting over a vein that will make them millionaires over night. Today's prospectors are staking claims to Web sites, but not too many years ago those looking to profit from the Internet sought their wealth by becoming Internet Service Providers.

An ISP gambles that there will be more subscribers to its service than the maximum number of transmissions per month. An example will help to clarify the idea.

Let's say the telephone company charges an ISP $500 a month for a T carrier-line that can carry 24 transmissions at the same time. The ISP charges its subscribers $20 per month and tries to get as many subscribers as possible to sign up for the service. The gamble is that not more than 24 subscribers will connect to the Internet at the same time.

The ISP needs at least 25 paid subscribers a month to cover the cost of the T carrier-line and a higher number of subscribers is necessary to cover other expenses. The ISP has hardware, software, maintenance support, customer relations, and other expenses needed to keep subscribers happy. At some point, the ISP is betting that these expenses will be covered by monthly subscription fees and return a profit.

I like to think of an ISP as a health club. The health club purchases expensive training equipment, then lets us have unlimited use of it in return for a monthly fee. The health club owner is betting that more people will pay the fee and not use the equipment than those who will pay the fee and use the facility.

Communications carriers, such as the telephone company and cable TV companies, soon realized that they too could easily become an ISP and possibly offer faster transmission than that provided by traditional ISPs. For example, some telephone companies offer DLS service (see Chapter 5) and some cable TV companies offer special modems that connect your computer to their cable.

Another objective of an ISP is to keep transmissions over the T carrier-line to the Internet backbone at a minimum. This reduces the chance that additional T carrier-lines will be needed to accommodate subscribers.

Imagine an ISP as a local area network of subscribers that has one pathway to the Internet superhighway, which is a T carrier-line. Let's say that many subscribers to the ISP visit Amazon.com.

Each time a subscriber selects Amazon.com, the ISP goes to a remote computer and looks up Amazon.com's Internet address. This ties up a channel on the T-carrier line. However, the ISP can eliminate these trips if it copies the Internet telephone book to a server on the ISP's local area network. This way, the ISP uses its own copy of the Internet telephone book to find Amazon.com's Internet address without using a channel on the T carrier-line.

The reduced traffic from the ISP to the Internet backbone frees the T carrier-line for other Internet transmissions, which could reduce the number of T carrier-lines that need to be leased from the telephone company.

The Internet backbone is the interconnection of networks managed by network services providers called Tier 1 providers. These providers include AT&T, Sprint, MCI WorldCom, GTE Internetwork, and UUNET.

**Tech Talk**

**Tier 1 provider: a telephone company that has a large network that connects IPSs and corporations directly to the Internet.**

Tier 1 providers each have their own large networks, which connect to ISPs and corporations that want direct access to the Internet. The National Science Foundation created four central points where Tier 1 providers exchange data. I think of these like regional post offices where information is redirected to the destination network. These central points are called public peering centers, and instead of letters being exchanged, such as is done in a regional post office, public peering centers exchange data packets (see Chapter 5). Private Tier 1 providers run each of the four centers.

However, the rapid growth of Internet traffic has far exceeded the capability of public peering centers to keep up with demand. Tier 1 providers are overcoming this obstacle to growth by creating private peering centers that perform similar duties to those the public peering centers perform (Figure 6.5).

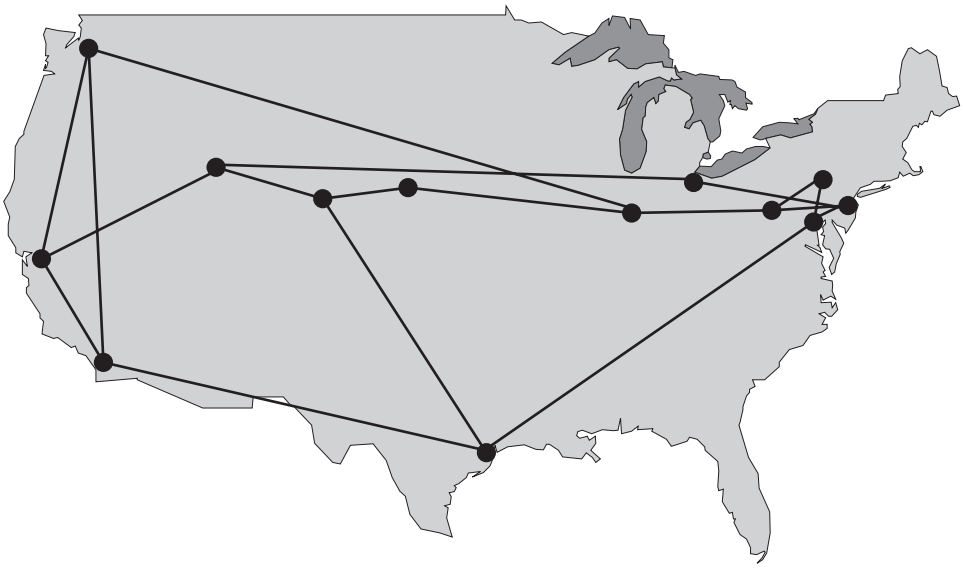

**Figure 6.5**
*Tier 1 Internet providers connect together centers around the country to exchange information. (Redrawn with permission from Prentice Hall. Comer, Douglas E. The Internet Book. Englewood Cliffs, NJ: Prentice Hall, 1997, p. 69.)*

## Internet Addresses

Some business Internet addresses are worth millions of dollars, but most are like mine, personal addresses that cost a few dollars a month to maintain rather than bringing in any revenue.

An Internet address is similar to a telephone number on the telephone network; the address uniquely identifies a particular computer that is connected to the Internet. The actual Internet address, also known as an IP address, looks something like this: 123.123.123.123.

This format of an IP address might appear strange to you especially if you are familiar with entering the name that is associated with the IP address rather than the address itself into your browser. For example, *www.keogh.org* is the Universal Resource Locator (URL) Internet name that is associated with my Web site. This is called the *domain name*. Frankly, I don't know my IP address, which is not a problem because my Internet Service Provider looks up the IP address whenever I connect to my Web site by typing *www.keogh.org*.

A domain name implies the nature of the organization that owns a computer. You recognize this as .com, .org, .net, .gov, .edu, and .mil. These indicate a commercial business, a nonprofit organization, a network, an educational institution, a government organization, and a military organization, respectively. These are referred to as top-level domain names.

A word of caution: Don't assume the top-level domain name actually reflects the type of organization that owns the computer. Anyone can register a .com, .org, or .net IP address by filling out an online form and paying a registration fee. For example, an address that ends with .org can be used for a commercial venture.

The IP address consists of a setting of bits called *octets,* such as 111.222.333.444. A bit is a binary digit (see Chapter 2), although I like to consider a bit like a switch that can be turned on or off, with on representing a 1 and off representing a 0.

The IP address identifies more than a computer linked to the Internet. It also identifies the network that contains the computer. Earlier in this chapter, you learned that the Internet is a network of networks. The first two sets of numbers in the IP address are called the *subnet* and identify the network that contains the computer. The next two sets of numbers identify the computer.

**Tech Talk**

**Subnet: the portion of an IP address that identifies a network.**

This is similar to your telephone number, in which the area code identifies your metropolitan region, the next three digits represent your exchange, and the last four digits represent your telephone. An IP address is associated with one or more URLs. This is called mapping. For example, *www.instituteofe-commerce.com* and *www.keogh.org* are mapped to the same IP address.

The first set of characters entered before the Web site name (www) identify the Internet service that you request. You'll notice that if you type *www.keogh.org* in your browser, it automatically places "http" in front of the name, which identifies the Internet service you want to use to transfer files over the Internet.

**Tech Talk**

**HTTP: HyperText Transfer Protocol, which is the Internet service used to transmit Web pages.**

An Internet service has nothing to do with the type of Web site you can visit. Instead, it describes a feature of the Internet that you want to use, such as e-mail, FTP (to transfer files), and HTTP (to enter the World Wide Web).

You are probably familiar with e-mail and HTTP more than with FTP because most of us rarely transfer files directly on the Internet. We usually let the browser handle file transfer behind the scenes. We'll explore FTP in detail later in this chapter.

## E-mail Address

The e-mail address is divided into two components that are separated by the @ sign. These are the name of the e-mail mailbox and the name of the computer that contains the mailbox. The name of the computer is called the domain name. The @ symbol was selected as the character to use for e-mail because it was unlikely that it would be used in a mailbox name or a domain name. In fact, @ cannot be used in a mailbox or a domain name.

The domain name is used by Internet devices, such as a router or a switch (see Chapter 4), to send mail to the proper computer, sometimes called the mail server (discussed in detail in Chapter 7). Once the mail arrives, the mail server uses the mailbox name to locate the proper mailbox on the server. If it is unable to find the mailbox, the e-mail is returned to the sender with a message stating that the mailbox is unknown. A mailbox is actually a directory on the mail server, similar to a folder on a computer's hard disk.

Internet Service Providers, especially those that host Web sites for other organizations, have a way to fool the system by assigning an IP address to a directory on their computer rather than to a computer.

Let's say that you want to have your own Web site and stake your claim to the billions of dollars that are expected to pour over the Internet. You can buy software that transforms your home computer to a Web server, then spend $500 a month plus an installation charge to connect your computer to the Internet backbone.

Or you can ask your Internet Service Provider to host your Web site for about $10 month plus setup charges. Don't expect to receive your own computer for that price. Instead, you'll receive a directory on the Internet Service Provider's computer.

You'll get to choose the name of your Web site, as long as it hasn't been reserved, and the Internet Service Provider will assign you an IP address that is associated with its computer. This IP address enables the Internet backbone routers and switches to find the computer on the Internet.

However, once a message arrives, the Internet Service Provider uses the IP address to locate your directory. This enables many of us to feed our dreams of making millions by owning a Web site, without spending thousands of dollars to set up a business.

The Internet is so hot that it is running out of IP addresses. There is a mathematical limit to the number of IP addresses that can be issued: 4,294,967,296. This is the number of bit combinations that can be represented by the bits used to store an IP address.

A similar situation is happening with telephone numbers. For example, each exchange (first three digits) can contain a maximum of 9,999 telephone numbers. And there can be a maximum of 999 exchanges for each area code, with a maximum of 999 area codes. My trusty calculator indicates that there can be 9,979,011,999 unique telephone numbers (9999*999*999).

Everyone overseeing the Internet realizes the seriousness of running out of IP addresses, and an effort has been launched to overcome this problem by creating a new version of the Internet Protocol.

## Internet Protocols

The Internet is like a highway of interconnecting networks and computers, and as with every highway there are rules of the road. On the Internet, these rules are called Internet protocols, which were discussed briefly in Chapter 5.

Another way to look at this is to think of information flowing around the Internet as stuffed into electronic envelopes called packets (see Chapter 5). You can stick any kind of information in any format within an envelope, as long as the envelope is the standard size and is addressed properly.

Internet protocols are called Transmission Control Protocol (TCP) and Internet Protocol (IP), which are commonly referred to as TCP/IP. Together, they form an Internet protocol suite, which is discussed in Chapter 5.

IP is the protocol that specifies how to send and receive packets, called datagrams, over the Internet. Software manufacturers build software that follows these rules to ensure that information is transmitted properly.

**Tech Talk**

**Datagram: a packet of information that is transmitted over the Internet.**

Each datagram contains the IP address of the destination computer and the computer that sent the datagram. Routers and other Internet devices use the IP address to determine the most efficient path for reaching the destination address.

While the IP protocol handles addressing and constructing a datagram, the TCP protocol handles how to deal with transmission problems. A superhighway is connected by many interchanges of on and off ramps that join to approach roads. The Internet also has interchanges called routers and switches (see Chapter 4).

A bottleneck can easily occur when too many datagrams try to move through the same router at the same time. Software in a router does what most of us do when we become overwhelmed with information—ignores it. This is unacceptable for the Internet, so engineers developed the TCP protocol to manage the connection between two computers and redirect discarded datagrams to lesser-used routers.

Here's how TCP works (Figure 6.6). A timer begins when a datagram is sent. If all goes well and the datagram is received, the destination computer sends an acknowledgement , which turns off the timer. However, if the time expires before the acknowledgement is received, TCP sends another copy of the datagram since it is assumed a router discarded the original one.

TCP has the intelligence to adjust the time limit between transmission and acknowledgement based on conditions on the Internet. For example, more time is given to receive a response during peak traffic periods or when the destination is far from the sender.

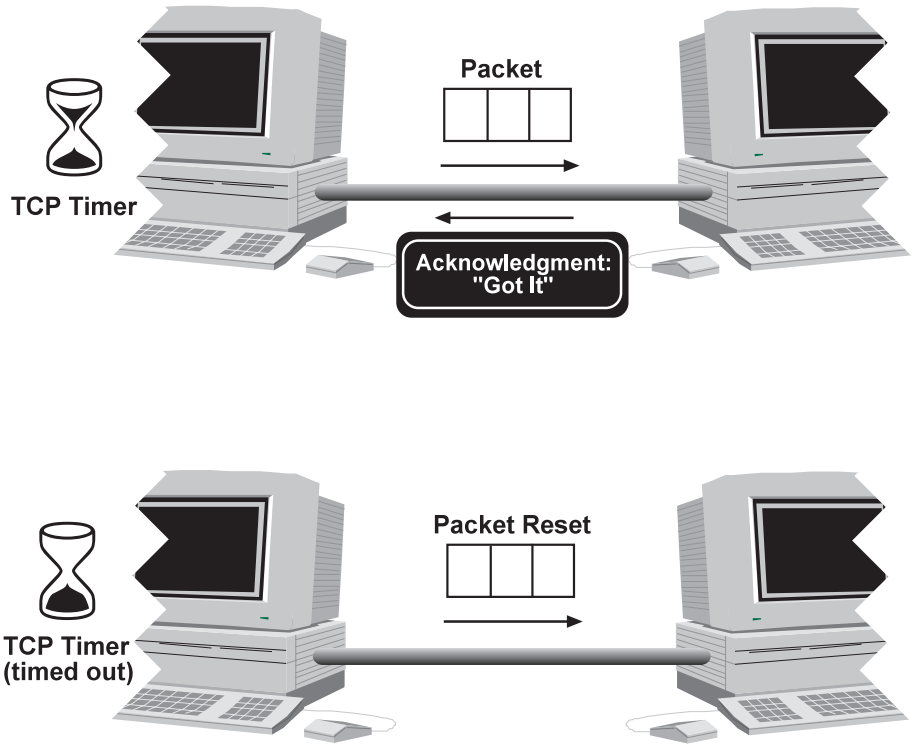


**Figure 6.6**
*TCP starts a timer when a packet is sent. If time expires before an acknowledgment is received, TCP resends the packet.*

## INTERNET SERVICES

It is difficult to accept that there was a time when Amazon.com and Yahoo.com didn't exist. There wasn't any place on the World Wide Web to buy discounted merchandise. In fact, there was a time when there wasn't a World Wide Web, but instead a bare-bones Internet.

The Internet was designed to accommodate communication among researchers and scientists at universities and research institutions. The people who used it were happy with less fancy communications than we have become accustomed to on today's Internet. Any improvement over communicating by telephone, fax, or "snail" mail was seen as a triumph.

As mentioned earlier in this chapter, the Internet is a network of networks that consists of cables, routers, switches, and computers, along with software that obey Internet protocols to exchange information.

Engineers who helped build the Internet had to develop ways to package data transmissions that was efficient and easy to use. The packaging I'm referring to isn't data packets or datagrams, but Internet services.

I like to think of an Internet service as a consumer product much like services we use to transfer things from one place to another. I can transfer a few words that describe my new house by calling our friend. I can supply her with a play-by-play commentary on how I bought the house by transferring my thoughts in a letter and sending it by snail mail. If I really want to be eccentric, I can hire a moving company to tow the entire house to my friend's front door.

The Internet has services similar to the ones I just described except they are identified by formal names such as Telnet, e-mail, and FTP. Of course, I cannot overlook the World Wide Web.

### Telnet

The Telnet service is similar to a telephone call; words we enter on our computer are sent directly to a remote computer. Like a telephone call, those words are not stored but, instead, displayed on the remote computer's screen.

In the early years of computers, before the Windows operating system or Macintosh computers hit the market, anyone who wanted to use a computer had to enter commands at an operating system prompt known as a command prompt. There weren't any fancy icons or lists of programs. Instead, everyone needed to learn commands that enabled him or her to control the computer.

For example, the command `dir` displayed the files and directories of the computer much like Windows Explorer does for a PC. You can still use commands if you display the MS-DOS Prompt window by clicking the Start button and then the Programs option in Windows.

The Telnet service enabled anyone who could connect to the Internet to take control of another computer that is also connected to it. Of course, the person who owned the remote computer had to grant access permission by issuing a login ID and password.

For example, I can access a computer at Columbia University, where I teach, by dialing my Internet Service Provider, then using telnet to dial the IP address of the computer at Columbia University. Once the computer "answers" the call, it sends my computer a log-in prompt, which are words that tell me to enter my ID and password. I enter this information on my computer, and it is transmitted to the Columbia University computer when I press the Enter key.

The Columbia University computer searches its password file to determine if my ID and password are valid. If they're not, a message is sent refusing me access to the computer. If the password and ID match, then an operating system prompt similar to the command prompt is sent to my computer. Then I can enter commands as if I was sitting in front of the Columbia University computer.

## E-mail

Electronic mail, better known as e-mail, was born in 1972 when Ray Tomlinson, an engineer at Bolt Beranek and Newman Company (BBN) and one of the pioneers of the original Internet, needed a way to communicate with other engineers who were connected to the Internet. Tomlinson is the father of the @ sign in e-mail addresses.

E-mail enables you to use store-forward technology to electronically write your thoughts into a file and then copy the file to a remote computer, where another person can read it.

**Tech Talk**

**Store-forward technology: a method of saving information to a file and then sending the file to a remote computer, where the file is stored until someone is available to read it.**

What makes e-mail special is that the file can be addressed to a particular person at a particular computer connected to the Internet. This is possible because of the e-mail rules of the road called Simple Mail Transfer Protocols (SMTP), which are part of the TCP/IP protocol suite.

SMTP controls how e-mail is sent and received. However, SMTP is unable to handle attachments to e-mails. Engineers needed to develop a way to attach other files to an e-mail. This need gave birth to the Multipurpose Internet Mail Extension (MIME) standard, which specifies how attachments are to be associated with an e-mail.

Here's how MIME works. Keep in mind that an e-mail consists of a group of bits in which the first few bits identify the recipient and sender, followed by the e-mail message and bits that indicate the end of the e-mail.

Between the last bit of the e-mail message and the bit that identifies the end of the e-mail are bits that represent the attachment. The first few bits of the attachment identify the beginning of it and the type of file that is attached. The last bit of the attachment signifies the end of it.

Let's say that you attached a Microsoft Word file to an e-mail. The Word file is identified with the .doc file extension. This is the type of file. If you select a file with the .doc file extension, Windows assumes that Word is the program you need to read this file and starts Word automatically.

## Archie, Gopher, and FTP

The original Internet was created for scientists and engineers who needed to exchange ideas through e-mail, and scientific works in the form of research papers and other documents. However, scientific works posed a new challenge. How would scientists and engineers know a scientific work existed? And how could they receive a copy of it?

Think about this a minute and you can appreciate the enormity of the problem. Let's say that I accumulated statistical data that described how to stop insects from eating apples. I wrote a formal scientific paper and placed it on my computer, then I told all my colleagues to go to the Internet and use Telnet to log on my computer and look at my paper.

This works well except for two limitations. My colleagues must read the paper online and cannot get their own copy. They cannot even print it because they are remotely connected to my computer, so any print commands they enter cause the document to print at my site, not theirs. The other limitation is that other scientists and engineers couldn't access the paper because they didn't know it existed unless the author told them. Many times the author was unable to spread the word about the paper and, therefore, the paper wasn't widely read.

You may be thinking, "Why don't they simply visit my Web page?". That's possible today, but until the early 1990s, Web pages didn't exist. However, there were

three Internet services that were created to resolve these problems. These are Archie, Gopher, and the File Transfer Protocol (FTP).

The Archie and Gopher services were the forerunner of today's search engines. They enabled you to enter a keyword or phrase, and then Archie or Gopher searched the Internet for documents that matched the search criteria. The address of the remote computer that contained the document was returned as the results of the search.

The Archie Internet service was command driven, which meant anyone who used it needed to learn Archie commands to perform a search. The Gopher Internet service improved upon Archie by interacting with users through a menu instead of using commands.

Next, there needed to be a way to copy a document from a remote computer. Of course, e-mail could have been used for this purpose, but the scientist or engineer first needed to contact the author of the paper and ask that the document be sent as an attachment to the e-mail. This became cumbersome. The author didn't have time to respond to inquiries.

A better method was to use the FTP Internet service, which enabled the scientist or engineer to copy the file directly, without contacting anyone at the remote computer. The FTP Internet service required the person to connect to the remote computer and log in.

Obviously, the scientist or engineer didn't have an ID or password to gain access to the remote computer. However, owners of remote computers typically created a standard ID called "anonymous" and the password was the visitor's e-mail address. The password wasn't used to protect the site, but instead to record visitors. Everyone trusted other Internet users. Those were the days before computer viruses and cyber attacks.

After the scientist or engineer logged on the remote computer, he or she used FTP commands to locate the file that contained the document and to copy the file to his or her computer.

## The World Wide Web

Surfing the Internet before the Web browser was created was a nightmare because you needed to learn a vocabulary of commands for every Internet service before you could become proficient using the Internet.

The main objective of the Internet is to foster an easy way for people to communicate, without requiring them to learn and use an archaic language. Tim Berners-Lee, a scientist at the European Laboratory for Particle Physics, agreed and took things into his own hands. He created a new service for the Internet called the World Wide Web (WWW).

The WWW specifies rules for finding and displaying information that is stored on a computer connected to the Internet, independent of a computer language and computer. These rules are called the HyperText Transfer Protocol (HTTP). You probably recognize HTTP as the first four characters displayed on the address bar of your browser. At the heart of HTTP is the HyperText Markup Language (HTML).

**Tech Talk**

**HyperText Markup Language (HTML): a language that uses embedded tags to describe how a document is to be displayed in a browser and how it is to be linked to other documents.**

Let's say you visit my Web site, *www.keogh.org*, by entering the address in your browser. The browser looks up the IP address associated with my site and requests the *index.html* file. This is usually the file that contains the Web site home page. The Internet Service Provider who hosts my Web site sends a copy of the *index.html* file to your computer, where your browser opens the file.

Your browser assumes that the *index.html* file is written in HTML, then reads each line of the *index.html* file looking for HTML tags (Figure 6.7) that tell the browser how I want the text to be displayed on your screen.

```
<HTML>
<HEAD>
<TITLE>Test Page</TITLE>
</HEAD>
<BODY bgColor=#ffffcc link="#3333ff" vlink="#3333ff" alink="#3333ff">
<P><IMG src="test.gif" ></P>
</BODY>
</HTML>
```

***Figure 6.7***
*HTML uses tags to tell a browser how to display a Web page.*

If I want the person viewing my Web site to see a mixture of pictures and text, I would use an HTML tag to tell the browser where to insert a specific graphic. This tag contains the name of the file and the name of the computer that contains the file, which the browser uses to request the picture file from that computer.

If you visit my Web site, you'll notice that I have links to many other sites. These are called *hyperlinks*, which are HTML tags that tell the browser the name of

the file to request when someone clicks on the hyperlink. You recognize hyperlinks as colored text on the Web page or perhaps graphics that you can click on.

The hidden benefit of HTML is that any browser can read it on any computer. In contrast, a computer program can be run only on a specific computer platform. For example, WordPerfect is a word processing program that has versions for Windows and UNIX, which are different operating systems. You must have the proper version of WordPerfect for the operating system used on your computer. This is not the case with HTML documents since they can be viewed on any computer running a browser.

With the onset of electronic commerce and new technology, enhanced versions of HTML were developed. These include the Dynamic HyperText Markup Language (DHTML), Extensible Markup Language (XML), the Voice Extensible Markup Language (VXML), and SGML, which is the forerunner of XML.

DHTML is similar to HTML except the HTML code is generated by a program at the time a Web page is requested, rather than at the time the programmer creates it. For example, after you identify yourself by signing into a Web site, a program running on the site creates a personal greeting, which is displayed on the page. The Web pages that are not personalized are likely to be created once by a programmer and stored on the server waiting for your browser to ask for the page.

XML enables authors to create their own labels and fields, some of which have been standardized for electronic commerce. Let's say you have an e-commerce Web site that needs to exchange product information, such as prices, with other systems. You can create a product ID tag and a price tag that identifies information as the product identifier and the price of the product.

VXML enables you to Interact with the World Wide Web using voice over the telephone. For example, you can ask for a weather report and receive a briefing over the telephone from a computer that is connected to the Web.

## INTERNET SECURITY

The Internet is vulnerable to attack from people who seek to beat the system or cause cyber graffiti by leaving their name in a remote computer. There is an increased interest in protecting the Internet as more of our economy is conducted in cyber space.

There are many security issues involving the Internet because, as you've learned in this chapter, the Internet is comprised of many pieces, each of which must work together to provide successful transmission of information.

Let's identify points in a transmission where an attack can occur. The Internet is organized as a client/server network (see Chapter 7) in which at least one computer contains the information other computers want. The computer that contains the information is called a server and the computer requesting the information is called the client.

You and I are clients when we log on Amazon.com and browse its bookstore. Amazon.com uses a server to supply us with Web pages and eventually information that enables us to complete a transaction.

We begin our trip into cyber space by entering the name of the Web site that we want to visit, such as *www.amazon.com*. Our Internet Service Provider's computer looks up the actual IP address that is associated with *www.amazon.com*. Everyone assumes that the computer (a server) that contains the IP directory contains accurate information.

However, a cyber criminal could change the IP address associated with *www.amazon.com* in an IP directory. Keep in mind there are many copies of these "telephone books," so changing one may go undetected for some time.

A spoofing Web site operated by a cyber criminal can be substituted for the real IP address. Every request for your computer is passed to the spoofing site, which intercepts your request and forwards it to the real IP address. A sniffer program is used to search individual packets of data for confidential information, such as your credit card number. Next, *www.amazon.com* sends a response to your request to the spoofing Web site, which intercepts it before relaying it to your computer.

**Tech Talk**

**Spoofing: occurs when an illegitimate Web site pretends to be a specific legitimate Web site.**
**Sniffer program: software that examines datagrams transmitted over the Internet for confidential information.**

Information that is intercepted can be altered or left intact and used for illegal purposes without you or Amazon.com finding out until the cyber crime is detected. The most critical information in an e-commerce transaction is your credit card information. E-tailers, the name given to merchants on the Internet, protect credit card information by encrypting the data using a secured Web site. A cyber criminal still might intercept your credit card information, but the information is garbled and must be decoded with a special key.

Servers on the Internet are vulnerable to a frontal attack by cyber crooks trying to use various methods to gain access to IDs, passwords, and back doors that give them direct access to files located anywhere on the server.

**Tech Talk**

**Back door: an entrance to a server that bypasses ID and password security measures.**
**War dialing: the technique in which a program dials sequential telephone numbers trying to detect those that are attached to modems.**

For example, a cyber criminal might begin the attack by war dialing, in which programs are used to automatically dial thousands of telephone numbers trying to find those that are connected to modems. The idea is that where there is a modem, there must be a computer, which might contain interesting and confidential information.

Of course, the cyber criminal still needs an ID and a password to gain access to the server. Several techniques are used to overcome this obstacle. First, a password cracker can be used, which is software that tries to guess an ID and a password by attempting hundreds of combinations.

The good guys fight back by disconnecting the telephone call after three failed log-in attempts. Many times a call must be made to the administrator of the server to re-establish the ID. However, this too may not pose a problem because once the cyber criminal identifies the company that owns the server, he or she uses the social engineering tactic to gain access.

## Social Engineering

Social engineering is used by smooth-talkers to make unsuspecting company employees give out IDs and passwords. For example, someone might call an employee and pretend to be a technician working with the IS department and ask the person to verify his or her ID and password. Of course, the "technician" gives the wrong ID and password, which the employee corrects, and the "technician" promises to correct the company's records.

Then there are those diehards who will dumpster-dive for the chance that someone tossed information about IDs and passwords in the trash.

Companies take a defensive position to fight off attacks by creating a *firewall* between their servers and the Internet. A firewall acts similarly to a brick and mortar firewall; the firewall separates two structures, which are spaced to ideally prevent dangerous people from attacking the main structure. In cyber space, the main structure is comprised of the servers within an organization.

**Tech Talk**

**Firewall: a computer that filters every piece of information within the organization that is received from and sent to the Internet.**

Some employees like to call a firewall "Big Brother" because it refuses employees access to specific Web sites that someone in the organization feels are not suited for viewing during business hours.

However, the primary purpose of a firewall is to trap Trojan horses, logic bombs, and malicious applets from gaining access to corporate servers. These are programs that can wreak havoc on a server.

**Tech Talk**

**Trojan horse: a program that uses the same program name as a safe program, but contains instructions inside that could destroy files on the server.**
**Logic bomb: a program that is like a booby trap and sits quietly on the server until someone inadvertently triggers it. Once triggered, instructions in the logic bomb do a dirty deed on the server.**
**Malicious applet: a short program written in the Java programming language that is embedded into a Web page. The Web page seems like any Web page to you and me, but once it is opened, the Java applet can do all kinds of mischief, such as send erroneous e-mails or search for IDs and passwords stored on the computer.**

One of the latest vulnerabilities of the Internet is denial of service, which causes such a traffic jam at a particular Web site that legitimate visitors are turned away. This has happened to Yahoo!, eBay, and other high profile Web sites.

The objective of cyber criminals who use this tactic is not to steal anything, but instead to deprive a company of business. Actually, denial of service is probably the least technical cyber crime and the most difficult one to prevent.

Here's how it works. Cyber criminals target both the IP address of the server and the IP addresses of routers and switches (see Chapter 4) that redirect packets to that IP address. Once these IP addresses are known, the criminal writes a program to send packets of data to those addresses. Although these IP addresses have the hardware and software that can handle high-peak traffic periods, there is a point when these IP addresses become overwhelmed and cannot process any more packets.

Cyber criminals know there is such a limit, but probably cannot measure it. So, they covertly distribute the packet-sending program to various Web servers and computers connected to the Web. Typically, they target computers at universities, which are less stringently controlled than those in corporations. Each program is timed to send a constant stream of packets to those IP addresses at precisely the same time and for the same duration, such as an hour. The congestion of packets at these addresses blocks legitimate packets from being processed, which can cause a slowdown of traffic on the Internet.

## Internet Privacy

Privacy is a major concern of anyone who uses the Internet, especially when the media reports that information about us is collected covertly by some Web site operators. Many of us fail to realize that when we are connected to the Internet, another computer is connected to ours, theoretically making anything on our computer available to the remote computer.

You need to realize that when visiting a Web site, you are inviting the owner of the site to run software (i.e., the Web page) on your computer, yet you never know what that software is actually doing.

Some Web pages write small pieces of information to our hard disk called *cookies*. Cookies hold various kinds of information, such as the last time you visited the Web page or the credit card number you used to order merchandise from that Web site.

Many browsers warn you when a Web page is about to write a cookie to your hard disk and gives you the opportunity to reject the cookie. If you reject the cookie, the Web page might not be able to function properly. However, many Web surfers become annoyed by receiving constant cookie alerts and decide to turn off the alert feature on their browser. This leaves them totally vulnerable to cookies being written without their knowledge.

Cookies are not infallible because a cookie identifies the last person who used your computer to interact with the Web page. This can be misleading because the information may not pertain to the current visitor. I discovered this when I logged on Amazon.com and was greeted personally as Joanne, who is my daughter and the last person who ordered a book from that site.

Even if a Web page doesn't write cookies to your hard disk, it can still gather information about you without you knowing it by using hidden fields of information in the Web page.

**Tech Talk**

**Field: a specific kind of information, such as a credit card number.**

Let's say that you visited your favorite online merchant. As soon as you request its home page, the merchant knows which ISP you used and the city, state, and country of the ISP. Businesses and larger organizations, such as universities, are their own ISP, so just by visiting a Web site the owner of the site can identify the organization.

Every time you request a page from a Web site, your request and information about your Internet return address is recorded in a log file that can be analyzed by tracking software. This enables the Web site owner to know what pages you viewed, how long you viewed them, and the path used to move from page to page throughout the site.

For example, the home page is usually *index.html* and displays information that the Web site owner hopes draws you to other pages on the site. Tracking software reports to the owner which of those pages you visited and which you avoided.

You may say that this information isn't too important to you because your identity remains unknown to the Web site owner. This is correct until you supply information about your identity when you become a "member" of a Web site or when you buy something from that site.

Information that you provide is likely stored in a database along with information that tracks your visit to the Web site. Say that you become a member of a Web site that contains information about cars. As you surf through the site, you might spend a few minutes looking at a Lexus and another few minutes looking at a Mercedes Benz before leaving the site.

You don't give the visit a second thought; however, you've provided the Web site owner with information that can be sold to a third party. The owner knows your identity because you filled out an online membership form, which probably included your home address and your e-mail address. And you were probably asked to sign in to the site whenever you visit so you can take advantage of "special deals."

You might actually find good deals that aren't offered to nonmembers. However, by signing onto the Web site, its owner is able to relate you to a traffic pattern. The tracking software is likely to detect your interest in a Lexus and a Mercedes Benz because you spent more time looking at those Web pages than other pages.

When this information comes to the attention of the Web site owner, you can expect that your identity will be sold to merchants who are looking for customers seeking to buy a Lexus or a Mercedes Benz. Furthermore, your identity could be sold to merchants who sell other products to customers who own Lexus or Mercedes Benz cars.

There is a trend among online merchants to ask your permission to sell information about you to third parties. You might find such a request buried at the bottom of your membership form or online purchase request. Don't be surprised if the default setting gives permission to sell your information just in case you forget to make a selection. Some Web site owners are also enabling you to see and correct the *profile* that is built about you whenever you visit their Web sites.

**Tech Talk**

**Profile: information stored by a Web site owner that describes products you purchase and Web pages you visit frequently. Profiles are used to display products and other information that might be of interest to you.**

Corporations and other large organizations try to limit information inferred from a Web site log file by using a proxy server. A proxy server is a computer that is an in-

termediary between the Internet and servers within the organization. The identity of the server used to request a Web page is recorded in the Web site's log file. However, this information reflects the identity of the proxy server and not the actual server within the organization because the proxy server strips away the information of the actual server and replaces it with its own.

### HONESTY MAY NOT BE THE BEST POLICY

Web site owners may not have all the relative information they think they have about visitors to their Web site. Clever Web surfers create virtual identities that conceal their true identity. For example, they create a fictitious name, then open a free e-mail account using that name. Instead of providing a Web site with their personal information, they provide a fake profile.

This enables the surfer to join free Web sites and participate in discussions without fearing that the site owner will learn any real information about them. This sounds dubious, but so are Web site owners who collect information about you and sell it to advertisers without your permission.

There's nothing illegal about creating a virtual identity as long as you don't attempt to defraud the Web site owner. For example, you must give legitimate information when making a purchase, but by then you should be comfortable dealing with that Web site.

## INTRANETS AND EXTRANETS

Businesses are finding other uses for Internet technology besides communicating with anyone in the world. Two of those new uses are to use this technology to communicate within an organization and among business partners.

The term *Intranet* is used to describe Internet technology used on a local area network to provide e-mail, Web pages, and other communication methods to employees. Employees use the same browser used to access the Internet to access the company's Intranet. However, anyone who is not connected to the organization's local area network is unable to access the Intranet.

Intranets are used to distribute employee information, provide Web page-based forms that are completed online, and give authorized employees access to data stored in the organization's databases.

An Extranet (Figure 6.8) is frequently used to link business partners, such as suppliers, vendors, and trading partners, who conduct frequent business transactions with an organization. Let's say you provide office supplies to 100 businesses. Instead of the office staff quoting prices, checking availability, and tracking orders, every customer can do this by logging on your Extranet.

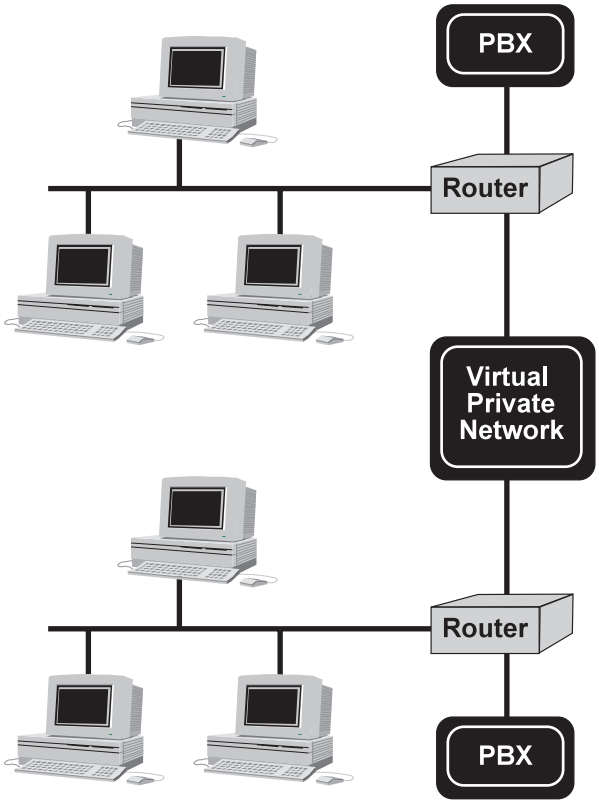


**Figure 6.8**
An Extranet connects business partners. (Redrawn with permission from Prentice Hall. Dodd, Annabel Z. The Essential Guide to Telecommunications. Upper Saddle River, NJ: Prentice Hall, 2000, p. 306.)

Typically, a customer uses the Internet address to visit your site, then uses an ID and a password to gain access to the Extranet Web pages. From that point, it is as if the customer is viewing a normal Web page.

An Extranet automates many of the normal business transactions that require human interaction but can easily be automated. Many inquiries require a sales assistant to look up the information in the company's computer system. The Extranet gives customers controlled access to that computer system.

Security is a critical concern to owners of Extranets since the owner is relying on the skills of the IS department to write a program that addresses all the facets dealing with a customer. The owner does not want incorrect information to be sent to the customer, nor does the owner want to frustrate the customer before he or she is able to talk to a person.

Extranets satisfy security concerns by using encryption, authorization, and integrity checks. Encryption mixes up data so it isn't easily read, as discussed previously in this chapter. Authorization requires the customer to use a unique ID and password to access the Extranet.

Integrity checks consist of logic written into a program to ensure that the interaction with the customer makes sense. For example, a small business that buys 10 reams of paper every month is unlikely to order 100 reams one month, so the Extranet ordering program would flag the order and bring it to the sales rep's attention.

## SUMMARY

The Internet is a network of networks that links computers called servers that contain Web pages and computers called clients that request to see Web pages. The entrance point to the Internet is typically through an Internet Service Provider (ISP), which is an organization that sells access to the Internet for a small monthly charge.

An ISP leases one or more T carrier-lines from the telephone company, which enables the ISP to transmit and receive information on the Internet. Depending on the type of T carrier-line, the ISP will have a minimum of 24 communications channels over which data can be communicated 24 hours, 7 days a week.

Every telephone company has its own telecommunication network that links ISPs and organizations that directly link their servers to the Internet without going through an ISP. Telephone companies exchange Internet data at regional centers called peering centers. There are four public peering centers and many private peering centers operated by telecommunications carriers.

Every device on the Internet has a unique Internet address, which is a set of numbers. An Internet address, also known as an IP address, is often identified by a Web site name that is associated with the IP address, such as *www.keogh.org*.

You and I can visit a Web site by dialing our ISP, then using software called a browser to request and display Web pages. After entering the Web site name, the browser sends the request to the ISP, which searches the Internet telephone book to locate the IP address associated with the Web site name.

Once the IP address is found, the ISP contacts the Web site and requests a page. The first page that is requested is the site's home page, unless your request specifies another page. The Web page is sent to your ISP from the Web site and is passed to your computer, where the browser reads and displays the page.

A Web page is written using HTML or an enhanced version of that language called XML. Programmers who build the Web page insert HTML and XML tags into the page that tell the browser how to display the page.

In addition to tags that specify the text format, there are tags that tell the browser what graphics to display and how to link to other Web pages. These tags are called hyperlinks. A hyperlink is typically highlighted text or a graphic that, when clicked on, tells the browser to request either another block of text on that Web page or to display another Web page.

Information travels over the Internet in small electronic envelopes called datagrams. The TCP/IP protocol suite controls datagram traffic on the Internet. The Internet Protocol (IP) describes how datagrams are constructed and transmitted. The Transmission Control Protocol (TCP) is used to manage the transmission.

TCP, for example, requires a timer to be activated when a datagram is transmitted. If an acknowledgement has not been received when time has expired, then the datagram is resent because TCP assumes the first one was lost or discarded during transmission.

The Internet groups the different ways to transfer information over the Internet into Internet services. Four popular services are Telnet, e-mail, FTP, and HTTP (World Wide Web). The Telnet service enables a person to directly interact with a remote computer. The e-mail service enables people linked to the Internet to exchange electronic mail. The FTP service is used to copy files to and from a remote computer. HTTP is the service used to exchange Web pages.

Security and privacy concerns are a serious threat to the viability of the Internet as a tool for electronic commerce. Cyber crooks can use a variety of methods to gain access to a server or prevent legitimate visitors from accessing a server. Organizations whose servers are connected to the Internet use various techniques to thwart such attacks by password-protecting sites and using firewalls and proxy servers.

Anyone who visits a Web site must be on alert that the owner of the site might be creating a visitor's profile, which identifies you and your interests, and might sell your profile to a third party.

Internet technology is also used within an organization and its business partners by creating an Intranet and Externet. An Intranet is an organization's private Internet that enables employees to share information and access corporate data. An Extranet is also a private Internet, but it is used to link business partners, such as key vendors, and to track orders, sales, and other information typically exchanged by business partners.

## Summary Questions

1. **What are the differences between a Tier 1 provider and an Internet Service Provider?**
2. **What are the business objectives of an Internet Service Provider?**
3. **How are peering centers used on the Internet?**
4. **How do cyber criminals deny service to a Web site?**
5. **What are the privacy issues regarding visiting a Web site?**
6. **What security measures can a Web site owner take to thwart a cyber attack?**
7. **How does a browser work?**
8. **What are the components of an e-mail address?**
9. **What services are offered on the Internet?**
10. **Why are Extranets beneficial to businesses?**