After reading this chapter, you will be able to:

- Discuss the origins of the Internet.
- Identify the key technology concepts behind the Internet.
- Describe the role of Internet protocols and utility programs.
- Explain the current structure of the Internet.
- Understand the limitations of today's Internet.
- Describe the potential capabilities of Internet II.
- Understand how the World Wide Web works.
- Describe how Internet and Web features and services support e-commerce.
Most people love the Web, but hate the wait. Studies have shown that most people won’t stay on a site if the page and its contents take more than eight seconds to load. That’s bad news for anyone seeking to use the Web for e-commerce.

Slow-loading Web pages sometimes result from poor design, but more often than not, the problem stems from the underlying infrastructure of the Internet. As you’ll learn in this chapter, the Internet was originally developed to carry text-based e-mail messages among a relatively small group of researchers, not bandwidth-hogging graphics, sound, and video files to millions of people.

Akamai Technologies is seeking to provide a solution by improving the “World Wide Wait” with existing Internet infrastructure technologies. Akamai (which means intelligent, clever, or “cool” in Hawaiian) was founded by Tom Leighton, an MIT professor of applied mathematics, and Daniel Lewin, an MIT grad student. Leighton and Lewin wondered: What if Web traffic could be monitored all over the world, just like traffic reporters monitor road traffic, and users seeking access to congested sites diverted on the fly to less busy Web servers (computers that “serve up” Web pages)? A simple idea in concept, but difficult to implement. It took three years to perfect mathematical algorithms that could perform such complex routing in real time.

Officially launched in August 1998, Akamai’s software constantly monitors the entire Internet, locating potential sluggish areas and devising faster routes for information to travel. Frequently used portions of a client’s Web site, or large files that would be difficult to send to users quickly, are stored on Akamai’s 8000 servers in over 50 countries around the world. Akamai’s software
determines which server is optimum for the user and then transmits the “Akamaized” content locally.

Akamai passed its most visible public test in October 1999, when it supported the Webcast of NetAid’s Concert against Hunger, which attracted millions of hits within a very short period of time. It also helped client Barnes & Noble cut the average wait time on its home page from four seconds at Christmas 1999 to 1.5 seconds by Christmas 2000, and assisted CNN.com in dealing with the sudden surge when millions of voters went looking for election day updates virtually simultaneously in November 2000.

Akamai makes money by selling its service to a wide range of clients, from Yahoo to Nasdaq to Martha Stewart Living. In 2000, it had revenues of approximately $90 million. However, Akamai is not alone in providing enhanced Web site performance. Its closest competitor is Inktomi, which uses a similar technology. The field is also likely to continue to attract further entrants. As one analyst notes, the Web has yet to approach performance standards that were once commonplace in the days of mainframe computers, and “until typical performance gets down to the subsecond range, anyone who can improve performance would have a good business.”
The Akamai story illustrates how much the Internet as it currently exists (what we call Internet I) and the World Wide Web are strained by the extraordinary growth in Web traffic over the last few years, as millions of people sign on to a small number of high-traffic sites such as Barnesandnoble.com, Amazon.com, and others. But equally important, the Akamai case also illustrates how important it is for a business to understand how the Internet and related technologies work. Implementing key Web business strategies such as personalization, customization, market segmentation, and price discrimination all require that business people understand Web technology. Looking forward five years to the emerging Internet II of 2006, the business strategies of the future will require a firm understanding of these new technologies.

This chapter examines the Internet and World Wide Web of today and tomorrow, how it evolved, how it works, and how the present and future infrastructure of the Internet and the Web enables e-commerce.

### 3.1 THE INTERNET: TECHNOLOGY BACKGROUND

What is the Internet? Where did it come from, and how did it support the growth of the World Wide Web? What are the Internet's most important operating principles?

As noted in Chapter 1, the Internet is an interconnected network of thousands of networks and millions of computers (sometimes called host computers or just hosts) linking businesses, educational institutions, government agencies, and individuals together. The Internet provides around 400 million people around the world (and over 170 million people in the United States) with services such as e-mail, newsgroups, shopping, research, instant messaging, music, videos, and news. No one organization controls the Internet or how it functions, nor is it owned by anybody, yet it has provided the infrastructure for a transformation in commerce, scientific research, and culture. The word Internet is derived from the word internetwork or the connecting together of two or more computer networks. The World Wide Web, or Web for short, is one of the Internet's most popular services, providing access to over one billion Web pages, which are documents created in a programming language called HTML and which can contain text, graphics, audio, video, and other objects, as well as "hyperlinks" that permit a user to jump easily from one page to another.

**THE EVOLUTION OF THE INTERNET 1961–2000**

Internet 1 — today's Internet — has evolved over the last forty years. In this sense, the Internet is not "new"; it did not happen yesterday. Although journalists and pundits talk glibly about "Internet" time — suggesting a fast-paced, nearly instant, worldwide global change mechanism, in fact, it has taken forty years of hard work to arrive at today's Internet.
The history of the Internet can be segmented into three phases (see Figure 3.1). In the first phase, the Innovation Phase, from 1961 to 1974, the fundamental building blocks of the Internet were conceptualized and then realized in actual hardware and software. The basic building blocks are: packet-switching hardware, client/server computing, and a communications protocol called TCP/IP (all described more fully below). The original purpose of the Internet, when it was conceived in the late 1960s, was to link together large mainframe computers on college campuses. This kind of one-to-one communication between campuses was previously only possible through the telephone system or postal mail.

In the second phase, the Institutional Phase, from 1975 to 1995, large institutions such as the Department of Defense and the National Science Foundation provided funding and legitimization for the fledging invention called the Internet. Once the concept of the Internet had been proven in several government-supported demonstration projects, the Department of Defense contributed a million dollars to develop the concepts and demonstration projects into a robust military communications system that could withstand nuclear war. This effort created what was then called ARPANET (Advanced Research Projects Agency Network). In 1986, the National Science Foundation assumed responsibility for the development of a civilian Internet (then called NSFNet) and began a ten-year-long $200 million expansion program.

In the third phase, the Commercialization Phase, from 1995–2001, government
agencies encouraged private corporations to take over and expand both the Internet backbone and local service to ordinary citizens — families and individuals across America and the world who were not students on campuses. By 2000, the Internet’s use had expanded well beyond military installations and research universities. The E-commerce I period begins — arguably — in 1994 with the first effort to advertise and market on the Web.

See Figure 3.2 for a closer look at the development of the Internet from 1961 on.

### FIGURE 3.2 DEVELOPMENT OF THE INTERNET: TIMELINE

<table>
<thead>
<tr>
<th>YEAR</th>
<th>EVENT</th>
<th>SIGNIFICANCE</th>
</tr>
</thead>
<tbody>
<tr>
<td>1961</td>
<td>Lawrence Roberts (MIT) connects a computer in Cambridge to a computer in California using a low-speed data line.</td>
<td>This is the first demonstration of a wide area network using telephone circuits. It demonstrated that computers could retrieve data and run programs remotely (and that the phone system was too noisy and slow for this purpose).</td>
</tr>
<tr>
<td>1962</td>
<td>J.C.R. Licklider (MIT) writes memos calling for a “Galactic Network” of computers.</td>
<td>The vision of a global computer network is born.</td>
</tr>
<tr>
<td>1963</td>
<td>Licklider heads up Department of Defense (DOD) ARPA network development.</td>
<td>This is the beginning of military interest and funding. ARPA becomes the largest funder of early Internet efforts.</td>
</tr>
<tr>
<td>1966</td>
<td>Lawrence Roberts convinces ARPA to fund development of ARPANET using packet switching.</td>
<td>The first effort begins to build a global packet switched wide-area network.</td>
</tr>
<tr>
<td>1968</td>
<td>ARPA requests quotes from various companies to build packet switches.</td>
<td>The concept of packet switching moves toward physical reality.</td>
</tr>
<tr>
<td>1969</td>
<td>The first packet switches are installed at UCLA and Stanford by Bolt, Beranek and Newman (BBN), a defense contractor.</td>
<td>The communications technology hardware of the Internet is born — the first “Inter Network.” The questions now are: How could this new technology be used? And for what purpose?</td>
</tr>
</tbody>
</table>

---

*a wide area network* is a network that connects computers and other devices over distances longer than 1,000 meters. Early “local” networks connected dumb terminals in the same building (less than 1,000 meters) to centralized mainframe computers. These early networks essentially sent keyboard and display commands back and forth from the terminals to the mainframe computers. The new wide area networks proposed in the 1960s were much more powerful: These new networks promised to permit remote computers to transfer entire files, send e-mail messages, and execute programs on a local computer.

bARPA refers to the Advanced Research Projects Agency of the United States Department of Defense. ARPA is essentially the research and development unit within the Department of Defense; it invests in promising new technologies that could have military significance.
<table>
<thead>
<tr>
<th>YEAR</th>
<th>EVENT</th>
<th>SIGNIFICANCE</th>
</tr>
</thead>
<tbody>
<tr>
<td>1972</td>
<td>E-mail is invented by Ray Tomlinson of BBN. The first ARPANET application is demonstrated at ICICC conference. Roberts writes the first e-mail utility program permitting listing, forwarding, and responding to e-mails.</td>
<td>The first “killer app” of the Internet is born.</td>
</tr>
<tr>
<td>1973</td>
<td>Bob Metcalfe (XeroxPARC Lab) invents Ethernet and local area networks.</td>
<td>Client/server computing is invented. Ethernet permitted the development of local area networks and client/server computing in which thousands of fully functional desktop computers could be connected into a short distance (&lt;1,000 meters) network to share files, run applications, and send messages. Although the Apple and IBM personal computers had not yet been invented, at XeroxPARC the first powerful desktop computers were created in the late 1960s. Xerox’s Ethernet StarNetwork connected these early desktop machines into a functioning office network that could share files, programs, and send messages. TCP/IP invented. The conceptual foundation for a single common communications protocol that could potentially connect any of thousands of disparate local area networks and computers, and a common addressing scheme for all computers connected to the network, is born. These developments made possible “peer-to-peer” “open” networking. Prior to this, computers could only communicate if they shared a common proprietary network architecture, e.g., IBM’s System Network Architecture. With TCP/IP, computers and networks could work together regardless of their local operating systems or network protocols.</td>
</tr>
<tr>
<td>1974</td>
<td>“Open architecture” networking and TCP/IP concepts are presented in a paper by Vint Cerf (Stanford) and Bob Kahn (BBN).</td>
<td></td>
</tr>
</tbody>
</table>

**INSTITUTIONAL PHASE 1980–1993**

<table>
<thead>
<tr>
<th>YEAR</th>
<th>EVENT</th>
<th>SIGNIFICANCE</th>
</tr>
</thead>
<tbody>
<tr>
<td>1980</td>
<td>TCP/IP is officially adopted as the DOD standard communications protocol</td>
<td>The single largest computing organization in the world adopts TCP/IP and packet-switched network technology. Altair, Apple, and IBM personal desktop computers are invented. These computers become the foundation for today’s Internet, affording millions of people access to the Internet and the Web. The idea of a “civilian” Internet is born.</td>
</tr>
<tr>
<td>1980</td>
<td>Personal computers are invented.</td>
<td></td>
</tr>
<tr>
<td>1983</td>
<td>ARPA creates a separate military network (MILNET) and ARPANET contains only civilian university traffic.</td>
<td>Telnet permits remote computers to link into a local computer and operate programs. FTP permits easy file transfers on the Internet. These services join e-mail as new “killer apps.”</td>
</tr>
<tr>
<td>1983</td>
<td>Telnet and File Transfer Protocol (FTP) services are deployed.</td>
<td></td>
</tr>
</tbody>
</table>
"Backbone" refers to the U.S. domestic trunk lines that carry the heavy data traffic across the nation, from one metropolitan area to another. Universities are given responsibility for developing their own campus networks that must be connected to the national backbone.

---

### Figure 3.2 Development of the Internet: Timeline (continued)

<table>
<thead>
<tr>
<th>Year</th>
<th>Event</th>
<th>Significance</th>
</tr>
</thead>
<tbody>
<tr>
<td>1984</td>
<td>Apple Computer releases the HyperCard program as part of its graphical user interface operating system called Macintosh.</td>
<td>The concept of &quot;hyperlinked&quot; documents and records that permit the user to jump from one page or record to another is commercially introduced.</td>
</tr>
<tr>
<td>1986</td>
<td>The National Science Foundation (NSF) adopts the Internet as its interuniversity network.</td>
<td>NSF begins $200 million program to develop a university network. It requires all universities receiving NSF funds to make access available campus-wide.</td>
</tr>
<tr>
<td>1988</td>
<td>NSF encourages development of private long-haul backbone communication carriers to privatize the Internet.</td>
<td>Private firms such as PSI and UUNet form to handle commercial Internet traffic.</td>
</tr>
<tr>
<td>1989</td>
<td>Tim Berners-Lee at the CERN physics lab in Switzerland proposes a worldwide network of hyperlinked documents based on a common markup language called HTML — HyperText Markup Language.</td>
<td>The concept of an Internet-supported service called the World Wide Web is born. The Web would be constructed from &quot;pages&quot; created in a common markup language, with &quot;hyperlinks&quot; that permitted easy access among the pages. The idea does not catch on rapidly and most Internet users rely on cumbersome FTP and Gopher protocols to find documents.</td>
</tr>
<tr>
<td>1990</td>
<td>NSF plans and assumes responsibility for a civilian Internet backbone and creates NSFNET. ARPANET is decommissioned.</td>
<td>The concept of a &quot;civilian&quot; Internet open to all is realized through non-military funding by NSF.</td>
</tr>
<tr>
<td>1990</td>
<td>The Internet backbone grows.</td>
<td>By 1990, the backbone had grown from six nodes connected at 56 Kbps to 21 nodes connected at 45 Mbps. 50,000 networks were now connected on all continents, with 29,000 in the United States alone.</td>
</tr>
<tr>
<td>1993</td>
<td>The first graphical Web browser called Mosaic is invented by Mark Andreesen and others at the National Center for Supercomputing at the University of Illinois.</td>
<td>Mosaic makes it very easy for ordinary users to connect to HTML documents anywhere on the Web. The browser-enabled Web takes off.</td>
</tr>
<tr>
<td>1994</td>
<td>NSF report plans the development of a &quot;information superhighway supporting universities, business and civilians.&quot;</td>
<td>Congress and the President’s Office propose the creation of a national information superhighway to support research, education, commercial, and private interests.</td>
</tr>
</tbody>
</table>
## Figure 3.2 Development of the Internet: Timeline (continued)

<table>
<thead>
<tr>
<th>Year</th>
<th>Event</th>
<th>Significance</th>
</tr>
</thead>
<tbody>
<tr>
<td>1995</td>
<td>NSF privatizes the backbone, and commercial carriers take over backbone operation.</td>
<td>The fully commercial civilian Internet is born. Major long-haul networks such as ATT, Sprint, GTE, UU Net, and MCI take over operation of the backbone. Network Solutions (a private firm) is given a monopoly to assign Internet addresses.</td>
</tr>
<tr>
<td>1996</td>
<td>Internet2 Consortium formed</td>
<td>Thirty-four government agencies, universities, and business firms plan the development of an Internet 100 to 1,000 times faster than the existing Internet I.</td>
</tr>
<tr>
<td>1998</td>
<td>The U.S. federal government encourages the founding of Internet Corporation for Assigning Numbers and Names (ICANN).</td>
<td>Governance over domain names and addresses passes to a private nonprofit international organization.</td>
</tr>
</tbody>
</table>


### The Internet: Key Technology Concepts

In 1995, the Federal Networking Council (FNC) took the step of passing a resolution formally defining the term Internet. (See Figure 3.3)

Based on that definition, the Internet means a network that uses the IP addressing scheme, supports the Transmission Control Protocol (TCP), and makes services available to users much like a telephone system makes voice and data services available to the public.

### Figure 3.3 Resolution of the Federal Networking Council

"The Federal Networking Council (FNC) agrees that the following language reflects our definition of the term "Internet."

"Internet" refers to the global information system that—

(i) is logically linked together by a globally unique address space based on the Internet Protocol (IP) or its subsequent extensions/follow-ons;

(ii) is able to support communications using the Transmission Control Protocol/Internet Protocol (TCP/IP) suite or its subsequent extensions/follow-ons, and/or other IP-compatible protocols; and

(iii) provides, uses or makes accessible, either publicly or privately, high level services layered on the communications and related infrastructure described herein."

Last modified on October 30, 1995.
Behind this formal definition are three extremely important concepts that are the basis for understanding the Internet: packet switching, the TCP/IP communications protocol, and client/server computing. Although the Internet has evolved and changed dramatically in the last 30 years, these three concepts are at the core of how the Internet functions today and are the foundation for Internet II.

Packet Switching. Packet switching is a method of slicing digital messages into parcels called “packets,” sending the packets along different communication paths as they become available, and then reassembling the packets once they arrive at their destination (see Figure 3.4). Prior to the development of packet switching, early computer networks used leased, dedicated telephone circuits to communicate with terminals and other computers. In circuit-switched networks such as the telephone system, a complete point-to-point circuit is put together, and then communication can proceed. However, these “dedicated” circuit-switching techniques were expensive and wasted available communications capacity—the circuit would be maintained regardless of whether any data was being sent. For nearly 70% of the time, a dedicated voice circuit is not being fully used because of pauses between words and delays in assembling the circuit segments, both of which increased the length of time required to find and connect circuits. A better technology was needed.

The first book on packet switching was written by Leonard Kleinrock in 1964 (Kleinrock, 1964), and the technique was further developed by others in the defense research labs of both the United States and England. With packet switching, the communications capacity of a network can be increased by a factor of 100 or more. The communications capacity of a digital network is measured in terms of bits per second.¹ Imagine if the gas mileage of your car went from 15 miles per gallon to 1,500 miles per gallon—all without changing too much of the car!

In packet-switched networks, messages are first broken down into packets. Appended to each packet are digital codes that indicate a source address (the origination point) and a destination address, as well as sequencing information and error-control information for the packet. Rather than being sent directly to the destination address, in a packet network, the packets travel from computer to computer until they reach their destination. These computers are called routers. Routers are special-purpose computers that interconnect the thousands of different computer networks that make up the Internet and route packets along to their ultimate destination as they travel. To ensure that packets take the best available path toward their destination, the routers use computer programs called routing algorithms.

Packet switching does not require a dedicated circuit but can make use of any spare capacity that is available on any of several hundred circuits. Packet switching

¹A bit is a binary digit, 0 or 1. A string of eight bits constitutes a byte. A home telephone modem connects to the Internet usually at 56 Kbps (56,000 bits per second). Mbps refers to millions of bits per second.
makes nearly full use of almost all available communication lines and capacity. Moreover, if some lines are disabled or too busy, the packets can be sent on any available line that eventually leads to the destination point.

TCP/IP answered the problem of what to do with packets on the Internet and how to handle them. TCP refers to the Transmission Control Protocol (TCP). IP refers to the Internet Protocol (IP). A protocol is a set of rules for formatting, ordering, compressing, and error-checking messages. It may also specify the speed of transmission and means by which devices on the network will indicate they have stopped sending and/or receiving messages. Protocols can be implemented in either hardware or software. TCP/IP is implemented in Web software called server software (described below). TCP is the agreed upon protocol for transmitting data packets over the Web. TCP establishes the connections among sending and receiving Web computers, handles the assembly of packets at the point of transmission, and their reassembly at the receiving end.
TCP/IP is divided into four separate layers, with each layer handling a different aspect of the communication problem (see Figure 3.5). The Network Interface Layer is responsible for placing packets on and receiving them from the network medium, which could be a Local Area Network (Ethernet) or Token Ring Network, or other network technology. TCP/IP is independent from any local network technology and can adapt to changes in the local level. The Internet Layer is responsible for addressing, packaging, and routing messages on the Internet. The Transport Layer is responsible for providing communication with the application by acknowledging and sequencing the packets to and from the application. The Application Layer provides a wide range of services including Telnet, FTP, SMTP, HTTP, and many others.
variety of applications with the ability to access the services of the lower layers. Some of the best known applications are HyperText Transfer Protocol (HTTP), File Transfer Protocol (FTP), and Simple Mail Transfer Protocol (SMTP), all of which we will discuss later in this chapter.

**IP Addresses.** TCP handles the packetizing and routing of Internet messages. IP provides the Internet's addressing scheme. Every computer connected to the Internet must be assigned an address — otherwise it cannot send or receive TCP packets. For instance, when you sign onto the Internet using a dial-up telephone modem, your computer is assigned a temporary address by your Internet Service Provider.

Internet addresses, known as **IP addresses**, are 32-bit numbers that appear as a series of four separate numbers marked off by periods, such as 201.61.186.227. Each of the four numbers can range from 0–255. This “dotted quad” addressing scheme contains up to 4 billion addresses (2 to the 32nd power). The leftmost number typically indicates the network address of the computer, while remaining numbers help to identify the specific computer within the group that is sending (or receiving ) a message.

The current version of IP is called Version 4, or IPv4. Because many large corporate and government domains have been given millions of IP addresses each (to accommodate their current and future work forces), and with all the new networks and new Internet-enabled devices requiring unique IP addresses being attached to the Internet, a new version of the IP protocol, called IPv6 is being adopted. This scheme contains 128-bit addresses, or about one quadrillion (10 to the 15th power) (National Research Council, 2000).

Figure 3.6 illustrates how TCP/IP and packet switching work together to send data over the Internet.

**Domain Names and URLs.** Most people cannot remember 32-bit numbers. IP addresses can be represented by a natural language convention called **domain names.** The **domain name system (DNS)** allows expressions such as cnet.com to stand for numeric IP addresses (cnet.com's numeric IP is 216.200.247.134). **Uniform resource locators (URLs),** which are the addresses used by Web browsers to identify the location of content on the Web, also use domain names as part of the URL. A typical URL contains the protocol to be used when accessing the address, followed by its location. For instance, the URL http://www.azimuth-interactive.com/flash_test refers to the IP address 208.148.84.1 with the domain name "azimuth-interactive.com" and the protocol being used to access the address, Hypertext Transfer Protocol (HTTP). A resource called "flash_test" is located on the server directory path /flash_test. A URL can have from two to four parts, for example name1.name2.

---

2You can check the IP address of any domain name on the Internet. In Windows, bring up the DOS program or use Start/Run/command to start the DOS prompt. Type “Ping <Domain Name>”. You will receive the IP address in return.
The Internet uses packet-switched networks and the TCP/IP communications protocol to send, route, and assemble messages. Messages are broken into packets, and packets from the same message can travel along different routes.

Table 3.1 summarizes the important components of the Internet addressing scheme.

<table>
<thead>
<tr>
<th>TABLE 3.1</th>
<th>PIECES OF THE INTERNET PUZZLE: NAMES AND ADDRESSES</th>
</tr>
</thead>
<tbody>
<tr>
<td>IP addresses</td>
<td>Every computer connected to the Internet must have a unique address number called an Internet Protocol address. Even computers using a modem are assigned a temporary IP address.</td>
</tr>
<tr>
<td>Domain names</td>
<td>The DNS (domain name system) allows expressions such as aw.com (Addison Wesley’s Web site) to stand for numeric IP locations.</td>
</tr>
<tr>
<td>DNS servers</td>
<td>DNS servers are databases that keep track of IP addresses and domain names on the Internet.</td>
</tr>
<tr>
<td>Root servers</td>
<td>Root servers are central directories that list all domain names currently in use. DNS servers consult root servers to look up unfamiliar domain names when routing traffic.</td>
</tr>
<tr>
<td>ICANN</td>
<td>The Internet Corporation for Assigned Numbers and Names (ICANN) was established in 1998 to set the rules for domain names and IP addresses and also to coordinate the operation of root servers. It took over from private firms such as NetSolutions.com.</td>
</tr>
</tbody>
</table>
Client/Server Computing. While packet switching exploded the available communications capacity and TCP/IP provided the communications rules and regulations, it took a revolution in computing to bring about today’s Internet and the Web. That revolution is called client/server computing and without it, the Web—in all its richness—would not exist. In fact, the Internet is a giant example of client/server computing in which over 70 million host server computers store Web pages and other content that can be easily accessed by nearly a million local area networks and hundreds of millions of client machines worldwide (Computer Industry Almanac Inc., 2001.)

Client/server computing is a model of computing in which very powerful personal computers called clients are connected together in a network together with one or more server computers. These clients are sufficiently powerful to accomplish complex tasks such as displaying rich graphics, storing large files, and processing graphics and sound files, all on a local desktop or handheld device. Servers are networked computers dedicated to common functions that the client machines on the network need, such as storing files, software applications, utility programs such as Web connections, and printers. (See Figure 3.7.)

To appreciate what client/server computing makes possible, you must understand what preceded it. In the mainframe computing environment of the 1960s and 1970s, computing power was very expensive and limited. For instance, the largest commercial mainframes of the late 1960s had 128k of RAM and 10 megabyte disk drives, and occupied hundreds of square feet. There was insufficient computing capacity to support graphics or color in text documents, let alone sound files or hyperlinked documents and databases.

With the development of personal computers and local area networks during the late 1970s and early 1980s, client/server computing became possible. Client/server
computing has many advantages over centralized mainframe computing. For instance, it is easy to expand capacity by adding servers and clients. Also, client/server networks are less vulnerable than centralized computing architectures. If one server goes down, backup or mirror servers can pick up the slack; if a client machine is inoperable, the rest of the network continues operating. Moreover, processing load is balanced over many powerful smaller machines rather than being concentrated in a single huge machine that performs processing for everyone. Both software and hardware in client/server environments can be built more simply and economically.

Today there are about 450 million PCs in existence worldwide (Computer Industry Almanac Inc., 2001). Most of these PCs can display and process graphics, sound files, and colored text. They have memories up to 512MB, 20 gigabyte hard drives, and occupy about two square feet. These personal “supercomputers,” when tied together in local area networks or into large wide area networks such as the Web, make it possible for millions of people to enjoy “rich” Web documents and experiences. Soon these capabilities will move to handheld devices such as the Palms and HP Jornada, and wireless cell phones (much “thinner clients”). In the process, more computer processing will be performed by central servers (reminiscent of mainframe computers of the past).

OTHER INTERNET PROTOCOLS AND UTILITY PROGRAMS

There are many other Internet protocols that provide services to users in the form of Internet applications that run on Internet clients and servers. These Internet services are based on universally accepted protocols — or standards — that are available to everyone who uses the Internet. They are not owned by any one organization but are services that were developed over many years and given to all Internet users.

HTTP: Hypertext Documents. HTTP (short for HyperText Transfer Protocol) is the Internet protocol used for transferring Web pages (described in the following section). The HTTP protocol runs in the Application Layer of the TCP/IP model shown in Figure 3.5. An HTTP session begins when a client’s browser requests a Web page from a remote Internet server. When the server responds by sending the page requested, the HTTP session for that object ends. Because Web pages may have many objects on them — graphics, sound or video files, frames, and so forth — each object must be requested by a separate HTTP message.

SMTP, POP, and IMAP: Sending E-mail. E-mail is one of the oldest, most important, and frequently used Internet services. SMTP (Simple Mail Transfer Protocol) is the Internet protocol used to send mail to a server. POP (Post Office Protocol) is used by the client to retrieve mail from an Internet server. You can see how your browser handles SMTP and POP by looking in your browser’s Preferences or Tools section, where the mail settings are defined. You can set POP to retrieve e-mail mes-
IMAP (Internet Message Access Protocol) is a more current e-mail protocol supported by many servers and all browsers. IMAP allows users to search, organize, and filter their mail prior to downloading it from the server.

FTP: Transferring Files. FTP (File Transfer Protocol) is one of the original Internet services. It is a part of the TCP/IP protocol and permits users to transfer files from the server to their client machine, and vice versa. The files can be documents, programs, or large database files. FTP is the fastest and most convenient way to transfer files larger than 1 megabyte, which many mail servers will not accept. (See Figure 3.8.)

SSL: Security. SSL (Secure Sockets Layer) is a protocol that operates between the Transport and Application Layers of TCP/IP and secures communications between the client and the server. SSL helps secure e-commerce communications and payments through a variety of techniques such as message encryption and digital signatures that we will discuss further in Chapter 5.

An FTP session using the Windows operating system. Users can click on a file in the Remote System’s FTP directory and transfer the file to a directory in the local system. FTP is especially good for moving large files or programs.
Telnet: Running Remote. Telnet is a terminal emulation program that runs in TCP/IP. You can run Telnet from your client machine. When you do so, your client emulates a mainframe computer terminal. (The industry standard terminals defined in the days of mainframe computing are VT-52, VT-100, and IBM 3250.) You can then attach yourself to a computer on the Internet that supports Telnet and run programs or download files from that computer. Telnet was the first “remote work” program that permitted users to work on a computer from a remote location.

Finger: Finding People. You can find out who is logged onto a remote network by using Telnet to connect to a server, and then typing “finger” at the prompt. Finger is a utility program supported by UNIX computers. When supported by remote computers, finger can tell you who is logged in, how long they have been attached, and their user name. Obviously there are security issues involved with supporting finger, and most Internet host computers do not support finger today.

Ping: Testing the Address. You can “ping” a host computer to check the connection between your client and the server (see Figure 3.9). The ping (Packet InterNet Groper) program will also tell you the time it takes for the server to respond, giving you some idea about the speed of the server and the Internet at that moment. You can run ping from the DOS prompt on a personal computer with a Windows operating system by typing: Ping <domain name>. We will discuss ping further in Chapter 5, because one way to slow down or even crash a domain computer is to send it millions of ping requests.

Tracert: Checking Routes. Tracert is one of a several route-tracing utilities that allow you to follow the path of a message you send from your client to a remote computer on the Internet. Figure 3.10 shows the result of route tracking a message sent to a

FIGURE 3.9 THE RESULT OF A PING

A ping is used to verify an address and test the speed of the round trip from your client to a host and back.
CHAPTER 3 The Internet and World Wide Web

VisualRoute and other tracing programs provide some insight into how the Internet uses packet switching. This particular message traveled from a computer in Dulles, Virginia to Croton-on-Hudson, New York.

By 2001, there were approximately 400 million Internet users worldwide, up from 100 million users at year-end 1997. That figure is projected to continue to grow to close to 800 million by 2003 (Computer Industry Almanac Inc., 2001; Global Reach, 2001). One would think that with such incredible growth, the Internet would be overloaded. However, this has not been true for several reasons. First, client/server computing is highly extensible: By simply adding servers and clients, the population of Internet users can grow indefinitely. Second, the Internet architecture is built in layers so that each layer can change without disturbing developments in other layers. For instance,
The technology used to move messages through the Internet can go through radical changes to make service faster without being disruptive to your desktop applications running on the Internet.

Figure 3.11 illustrates the "hourglass" architecture of the Internet. The Internet can be viewed conceptually as having four layers: the network technology substrate, trans-
Today’s Internet has a multi-tiered open network architecture featuring a national backbone, regional hubs, “campus” networks, and local client machines.

Middleware
the “glue” that ties the applications to the communications networks, and includes such services as security, authentication, addresses, and storage repositories.

Backbone
high-bandwidth fiber optic cable that transports data across the Internet.

Network Service Provider (NSP)
owns and controls one of the major networks comprising the Internet’s backbone.

Today’s Internet has a multi-tiered open network architecture featuring a national backbone, regional hubs, “campus” networks, and local client machines.

Middleware
the “glue” that ties the applications to the communications networks, and includes such services as security, authentication, addresses, and storage repositories.

Backbone
high-bandwidth fiber optic cable that transports data across the Internet.

Network Service Provider (NSP)
owns and controls one of the major networks comprising the Internet’s backbone.

The network technology substrate is composed of telecommunications networks and protocols. The transport layer houses the TCP/IP protocol. The applications layer contains client applications such as the World Wide Web, e-mail, and audio or video playback. Middleware is the glue that ties the applications to the communications networks, and includes such services as security, authentication, addresses, and storage repositories. Users work with applications (such as e-mail) and rarely become aware of middleware that operates in the background. Because all layers use TCP/IP and other common standards linking all four layers, it is possible for there to be significant changes in the network layer without forcing changes in the applications layer.

The network layer is described below.

THE INTERNET BACKBONE
Figure 3.12 illustrates the main physical elements of today’s Internet. The Internet’s backbone is formed by Network Service Providers (NSPs), which own and control…

3Recall that the TCP/IP communications protocol also has layers, not to be confused with the Internet architecture layers.
TABLE 3.2  MAJOR U.S INTERNET BACKBONE OWNERS

<table>
<thead>
<tr>
<th>AT&amp;T</th>
<th>Qwest</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cable &amp; Wireless</td>
<td>Level 3</td>
</tr>
<tr>
<td>Genuity</td>
<td>Williams</td>
</tr>
<tr>
<td>MCI Worldcom</td>
<td>Global Crossing</td>
</tr>
<tr>
<td>Sprint</td>
<td>Broadwing</td>
</tr>
</tbody>
</table>

The Internet Today

127

The backbone has been likened to a giant pipeline that transports data around the world in milliseconds. In the United States, the backbone is composed entirely of fiber-optic cable (described more fully below), with bandwidths ranging from 155 Mbps to 2.5 Gbps. Bandwidth measures how much data can be transferred over a communications medium within a fixed period of time, and is usually expressed in bits per second (bps), kilobits (thousands of bits) per second (Kbps), megabits (millions of bits) per second (Mbps), or gigabits (billions of bits) per second (Gbps).

Connections to other continents are made via a combination of undersea fiber optic cable and satellite links. The backbones in foreign countries typically are operated by a mixture of private and public owners. The U.S. backbone is one of the most developed because the Internet's infrastructure was developed here. The backbone has built-in redundancy so that if one part breaks down, data can be rerouted to another part of the backbone. Redundancy refers to multiple duplicate devices and paths in a network.

Network Access Points and Metropolitan Area Exchanges

In the United States there are a number of hubs where the backbone intersects with regional and local networks, and where the backbone owners connect with one another (see Figure 3.13). These hubs are called Network Access Points (NAPs) or Metropolitan Area Exchanges (MAEs), and use high-speed switching computers to connect the backbone to regional and local networks, and exchange messages with one another. The regional and local networks are owned by local Bell operating companies (RBOCs — pronounced “ree-bocks”), and private telecommunications firms such as MFS Corporation; they generally are fiber optic networks operating at over 100 Mbps. The regional networks lease access to Internet Service Providers, private companies, and government institutions.

Bandwidth measures how much data can be transferred over a communications medium within a fixed period of time; is usually expressed in bits per second (bps), kilobits per second (Kbps), or megabits (or millions of bits) per second (Mbps).

Redundancy multiple duplicate devices and paths in a network.

Network Access Point (NAP) one of the hubs where the backbone intersects with regional and local networks, and where the backbone owners connect with one another.

Metropolitan Area Exchanges (MAEs) another name for one of the hubs where the backbone intersects with regional and local networks, and where the backbone owners connect with one another.
### FIGURE 3.13  INTERNET NAPS AND MAES

**MAJOR U.S. INTERCONNECT POINTS**

<table>
<thead>
<tr>
<th>Location</th>
<th>Owner/Operator</th>
</tr>
</thead>
<tbody>
<tr>
<td>Chicago NAP</td>
<td>Ameritech Advanced Data Services and Bellcorp</td>
</tr>
<tr>
<td>Santa Clara, CA</td>
<td>CIX Commercial Internet Exchange</td>
</tr>
<tr>
<td>Palo Alto, CA</td>
<td>Digital IX/PAIX</td>
</tr>
<tr>
<td>Mountain View, CA (FIX-West)</td>
<td>Federal Internet Exchange (FIX)</td>
</tr>
<tr>
<td>College Park, MD (FIX-East)</td>
<td></td>
</tr>
<tr>
<td>San Jose (MAE-West)</td>
<td>MCI WorldCom</td>
</tr>
<tr>
<td>San Francisco</td>
<td></td>
</tr>
<tr>
<td>Los Angeles</td>
<td></td>
</tr>
<tr>
<td>Chicago</td>
<td></td>
</tr>
<tr>
<td>Dallas</td>
<td></td>
</tr>
<tr>
<td>Houston</td>
<td></td>
</tr>
<tr>
<td>Washington D.C. (MAE-East)</td>
<td></td>
</tr>
<tr>
<td>New York NAP (Pennsauken, NJ)</td>
<td>SprintLink</td>
</tr>
<tr>
<td>San Francisco NAP</td>
<td>Pacific Bell</td>
</tr>
</tbody>
</table>

![Map of Internet NAPS and MAES](image-url)
The Internet backbone connects regional networks, which in turn provide access to the Internet to Internet Service Providers, large firms, and government agencies.

CAMPUS NETWORKS
There are an estimated one million campus networks attached to the Internet worldwide (Computer Industry Almanac Inc., 2001). **Campus networks** are generally local area networks operating with a single organization — such as New York University or Microsoft Corporation. In fact, most large organizations have hundreds of such local area networks. These organizations (representing about 60 million workers) are sufficiently large that they lease access to the Web directly from regional and national carriers. These local area networks generally are running Ethernet (a local area network protocol) and have operating systems such as Windows 2000 (NT), Novell, or others that permit desktop clients to connect to the Internet through a local Internet server attached to their campus networks. Connection speeds in campus networks are in the range of 10–100 Mbps to the desktop.

INTERNET SERVICE PROVIDERS
The firms that provide the lowest level of service in the multi-tiered Internet architecture by leasing Internet access to home owners, small businesses, and some large institutions are called **Internet Service Providers (ISPs)**. ISPs are retail providers — they deal with “the last mile of service” to the curb, the home, the business office. About 45 million American households connect to the Internet through either national or local ISPs. ISPs typically connect to the Internet and MAEs or NAPs with high-speed telephone or cable lines (up to 45 Mbps).

There are major ISPs such as America Online, MSN Network, and AT&T WorldNet and about 5,000 local ISPs in the United States, ranging from local telephone companies offering dial-up and DSL telephone access, to cable companies offering cable modem service, to small “mom and pop” Internet shops that service a small town, city, or even county with mostly dial-up phone access (Boardwatch, 2001). If you have home or small business Internet access, an ISP will be providing you the service.

Table 3.3 summarizes the variety of services, speeds, and costs of ISP Internet connections. There are two types of ISP service: narrowband and broadband. **Narrowband** service is the traditional telephone modem connection now operating at 56.6 Kbps (although the actual throughput hovers around 30 Kbps due to line noise that causes extensive resending of packets). This is the most common form of connection worldwide. **Broadband** service is based on DSL, cable modem, telephone (T1 and T3 lines), and satellite technologies. Broadband — in the context of Internet service — refers to any communication technology that permits clients to play streaming audio and video files at acceptable speeds — generally anything above 100 Kbps.

**campus networks**
generally local area networks operating with a single organization that leases access to the Web directly from regional and national carriers

**Internet Service Provider (ISP)**
firn that provides the lowest level of service in the multi-tiered Internet architecture by leasing Internet access to home owners, small businesses, and some large institutions

**narrowband**
the traditional telephone modem connection, now operating at 56.6 Kbps

**broadband**
refers to any communication technology that permits clients to play streaming audio and video files at acceptable speeds — generally anything above 100 Kbps
The term **DSL** refers to digital subscriber line service, which is a telephone technology for delivering high-speed access through ordinary telephone lines found in homes or businesses. Service levels range from about 150 Kbps all the way up to 1 Mbps. DSL service requires that customers live within two miles (about 4,000 meters) of a neighborhood telephone switching center.

**Cable modem** refers to a cable television technology that piggybacks digital access to the Internet on top of the analog video cable providing television signals to a home. Cable modem services ranges from 350 Kbps up to 1 Mbps. Cable service may degrade if many people in a neighborhood log on and demand high-speed service all at once.

**T1** and **T3** are international telephone standards for digital communication. T1 lines offer guaranteed delivery at 1.54 Mbps, while T3 lines offer delivery at 43 Mbps. T1 lines cost about $1,000–$2,000 per month, and T3 lines between $10,000 and $30,000 per month. These are leased, dedicated, guaranteed lines suitable for corporations, government agencies, and businesses such as ISPs requiring high-speed guaranteed service levels.

Some satellite companies are offering broadband high-speed digital downloading of Internet content to homes and offices that deploy 18" satellite antennas. Service is available beginning at 256 Kbps up to 1 Mbps. In general, satellite connections are not viable for homes and small businesses because they are only one-way — you can download from the Internet at high speed, but cannot upload to the Internet at all. Instead, users require a phone or cable connection for their uploading.

**Broadband service** — DSL and cable modem — will be available to approximately 8–10 million homes and small businesses in 2001. Most professional organizations and

---

### TABLE 3.3 ISP SERVICE LEVELS CHOICES

<table>
<thead>
<tr>
<th>Service</th>
<th>Cost/Month</th>
<th>Speed to Desktop (Kbps)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Telephone Modem</td>
<td>$21–25</td>
<td>30–56 Kbps</td>
</tr>
<tr>
<td>DSL Lite</td>
<td>$50–75</td>
<td>150–384 Kbps</td>
</tr>
<tr>
<td>DSL Regular</td>
<td>$100–150</td>
<td>385 Kbps–1 Mbps</td>
</tr>
<tr>
<td>Cable Modem</td>
<td>$50–75</td>
<td>350 Kbps–1 Mbps</td>
</tr>
<tr>
<td>Satellite Dish</td>
<td>$35–50</td>
<td>250 Kbps–1 Mbps</td>
</tr>
<tr>
<td>T1</td>
<td>$1000–2000</td>
<td>1.554 Mbps</td>
</tr>
</tbody>
</table>

The actual throughput of data will depend on a variety of factors including noise in the line and the number of subscribers requesting service.
nearly all large business firms and government agencies have broadband connections to the Internet. About 60 million other homes — the vast majority of Internet users — still use the much slower 56.6 Kbps modem and ordinary telephone connections. Demand for broadband service is growing because customers are frustrated by the lengthy delays experienced using telephone modems when downloading large files (see Table 3.4). As the quality of Internet service offerings expands to include Hollywood movies, music, games, and other rich media streaming content, the demand for broadband access will swell rapidly. Currently, Internet service cannot deliver these types of services to millions of users simultaneously.

**INTRANETS AND EXTRANETS**

The very same Internet technologies that make it possible to operate a worldwide public network can also be used by private and government organizations as internal networks. An **intranet** is a TCP/IP network located within a single organization for purposes of communications and information processing. Many corporations are moving away from proprietary local area networks such as Windows 2000 and Novell, and toward a single internal intranet to handle the firm’s information processing and communication needs. Internet technologies are generally far less expensive than proprietary networks, and there is a global source of new applications that can run on intranets. In fact, all the applications available on the public Internet can be used in private intranets.

<table>
<thead>
<tr>
<th>TABLE 3.4</th>
<th>TIME TO DOWNLOAD A 10 MEGABYTE FILE BY TYPE OF INTERNET SERVICE</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>TYPE OF INTERNET SERVICE</strong></td>
<td><strong>TIME TO DOWNLOAD</strong></td>
</tr>
<tr>
<td>Narrowband Services</td>
<td></td>
</tr>
<tr>
<td>Telephone modem</td>
<td>25 minutes</td>
</tr>
<tr>
<td>Broadband Services</td>
<td></td>
</tr>
<tr>
<td>DSL lite</td>
<td>9 minutes</td>
</tr>
<tr>
<td>DSL regular</td>
<td>3.5 minutes</td>
</tr>
<tr>
<td>Cable modem</td>
<td>3.5 minutes</td>
</tr>
<tr>
<td>T-1</td>
<td>51 seconds</td>
</tr>
<tr>
<td>T-3</td>
<td>2 seconds</td>
</tr>
</tbody>
</table>

**intranet**
a TCP/IP network located within a single organization for purposes of communications and information processing
Extranets are formed when firms permit outsiders to access their internal TCP/IP networks. For instance, General Motors permits parts suppliers to gain access to GM’s intranet that contains GM’s production schedules. In this way, parts suppliers know exactly when GM needs parts, and where and when to deliver the parts.

Intranets and extranets generally do not involve commercial transactions in a marketplace, and they are mostly beyond the scope of this text. Extranets will receive some attention as a type of B2B exchange.

WHO GOVERNS THE INTERNET?

Aficionados and promoters of the Internet often claim that the Internet is governed by no one, and indeed cannot be governed, and that it is inherently above and beyond the law. In fact, the Internet is tied into a complex web of governing bodies, national legislatures, and international professional societies. There is no one governing body that controls activity on the Internet. Instead, there are several organizations that influence the system and monitor its operations. Among the governing bodies of the Internet are:

- The Internet Architecture Board (IAB), which helps define the overall structure of the Internet.
- The Internet Corporation for Assigned Names and Numbers (ICANN), which assigns IP addresses, and the Internet Network Information Center (InterNIC), which assigns domain names.
- The Internet Engineering Steering Group (IESG), which oversees standard setting with respect to the Internet.
- The Internet Engineering Task Force (IETF), which forecasts the next step in the growth of the Internet, keeping watch over its evolution and operation.
- The Internet Society (ISOC), which is a consortium of corporations, government agencies, and nonprofit organizations that monitors Internet policies and practices.
- The World Wide Web Consortium (W3C), which sets HTML and other programming standards for the Web.

While none of these organizations has actual control over the Internet and how it functions, they can and do influence government agencies, major network owners, ISPs, corporations, and software developers with the goal of keeping the Internet operating as efficiently as possible.

In addition to these professional bodies, the Internet must also conform to the laws of the sovereign nation-states in which it operates, as well as the technical infrastructures that exist within the nation-state. Although in the early years of the Internet and the Web there was very little legislative or executive interference, this situation will change in the near future as the Internet plays a growing role in the distribution of information and knowledge, including content that some find objectionable. Read
3.3 INTERNET II: THE FUTURE INFRASTRUCTURE

To appreciate the benefits of Internet II, you must first understand the limitations of the Internet's current infrastructure.

LIMITATIONS OF INTERNET I

Much of the Internet's current infrastructure is several decades old (equivalent to a century in Internet time). It suffers from a number of limitations, including:

• **Bandwidth limitations.** There is insufficient capacity throughout the backbone, the metropolitan switching centers, and most importantly, to the “last mile” to the house and small business. The result is slow service (congestion) and a very limited ability to handle video and voice traffic.

• **Quality of service limitations.** Today’s information packets take a circuitous route to get to their final destinations. This creates the phenomenon of **latency** — delays in messages caused by the uneven flow of information packets through the network. In the case of e-mail, latency is not noticeable. However, with streaming video and synchronous communication, such as a telephone call, latency is noticeable to the user and perceived as “jerkiness” in movies or delays in voice communication. Today’s Internet uses “best efforts” quality of service, (QOS), which makes no guarantees about when or whether data will be delivered, and provides each packet with the same level of service, no matter who the user is or what type of data is contained in the packet. A higher level of service quality is required if the Internet is to keep expanding into new services (such as video on demand or telephony). (CSTB, 2000).

• **Network architecture limitations.** Today, a thousand requests for a single music track from a central server will result in a thousand efforts by the server to download the music to each requesting client. This slows down network performance as the same music track is sent out a thousand times to clients that might be located in the same metropolitan area. This is very different from television, where the program is broadcast once to millions of homes.

• **Language development limitations.** HTML, the language of Web pages, is fine for text and simple graphics, but poor at defining and communicating “rich documents” such as databases, business documents, or graphics. The tags used to define an HTML page are fixed and generic.

Now imagine an Internet at least 100 times as powerful as today’s Internet, an Internet not subjected to the limitations of bandwidth, protocols, architecture, and...
CHAPTER 3 The Internet and World Wide Web

Who controls the Internet? It seems France wants some control; at least over what its citizens can access on the World Wide Web. In November 2000, French judge Jean-Jacques Gomez ruled that U.S.-based Yahoo! must block French users from access to Nazi-related memorabilia available on the site. In France, Nazi paraphernalia is illegal. But should France have the authority to determine what all other Internet users can and can't see and buy? Yahoo! thinks not and, although it has contested the ruling both on the grounds that it's impossible to block access and that the French court does not have jurisdiction, the company did remove all Nazi items in January, 2001. Web portal sites often claim they are "common carriers" and cannot technically control the content their users post, and in any event, are not responsible for what their users say or post to the site.

Such growing restrictions on the Internet are making many people nervous. Just the fact that Yahoo! took action to appease the two groups that sued the company — the League Against Racism and Anti-Semitism (LICRA) and the Union of French Jewish Students — has raised some eyebrows. Yahoo! denies that it acted because of the lawsuit, stating that it decided on its own that the Nazi items were unacceptable.

However, if other countries gain authority to police Web sites according to the laws of their own countries, we're going to see some major inequities with respect to who sees what. South Korea, for example, has outlawed access to gambling Web sites, some Muslim countries forbid religious discussions, and China holds Web sites responsible for any illegal content found on the site. But illegal according to whose laws? That's the question. And can and should companies be forced to police content on their Web sites at all?

Attempting to enforce the various and often contradictory laws of every country is what some are calling "legal harmonization." However, instead of creating harmony, such efforts are likely to do anything but. In the end, we may end up with a "lowest common denominator standard for protected speech on the Net," cautions New York Times writer Carl Kaplan, where what is acceptable is what is legal absolutely everywhere. This means that there won't be much information available.

The irony here is that the Internet was developed as a means of fostering global communication. Yet it is now very clear that many countries will put stricter limits on freedom of expression than the United States. The practicalities of a global perspective are proving more difficult socially and politically than the Internet's founders had hoped.


INSIGHT ON SOCIETY

YAHOO! FRANCE — GOVERNMENT REGULATION OF THE INTERNET

Who controls the Internet? It seems France wants some control; at least over what its citizens can access on the World Wide Web. In November 2000, French judge Jean-Jacques Gomez ruled that U.S.-based Yahoo! must block French users from access to Nazi-related memorabilia available on the site. In France, Nazi paraphernalia is illegal. But should France have the authority to determine what all other Internet users can and can’t see and buy? Yahoo! thinks not and, although it has contested the ruling both on the grounds that it’s impossible to block access and that the French court does not have jurisdiction, the company did remove all Nazi items in January, 2001. Web portal sites often claim they are "common carriers" and cannot technically control the content their users post, and in any event, are not responsible for what their users say or post to the site.

Such growing restrictions on the Internet are making many people nervous. Just the fact that Yahoo! took action to appease the two groups that sued the company — the League Against Racism and Anti-Semitism (LICRA) and the Union of French Jewish Students — has raised some eyebrows. Yahoo! denies that it acted because of the lawsuit, stating that it decided on its own that the Nazi items were unacceptable.

However, if other countries gain authority to police Web sites according to the laws of their own countries, we’re going to see some major inequities with respect to who sees what. South Korea, for example, has outlawed access to gambling Web sites, some Muslim countries forbid religious discussions, and China holds Web sites responsible for any illegal content found on the site. But illegal according to whose laws? That’s the question. And can and should companies be forced to police content on their Web sites at all?

Attempting to enforce the various and often contradictory laws of every country is what some are calling “legal harmonization.” However, instead of creating harmony, such efforts are likely to do anything but. In the end, we may end up with a “lowest common denominator standard for protected speech on the Net,” cautions New York Times writer Carl Kaplan, where what is acceptable is what is legal absolutely everywhere. This means that there won’t be much information available.

The irony here is that the Internet was developed as a means of fostering global communication. Yet it is now very clear that many countries will put stricter limits on freedom of expression than the United States. The practicalities of a global perspective are proving more difficult socially and politically than the Internet’s founders had hoped.

language detailed above. Welcome to the world of Internet II, and the next generation of e-commerce services and products.

**THE INTERNET2® PROJECT**

Internet2® is a consortium of more than 180 universities, government agencies, and private businesses that are collaborating to find ways to make the Internet more efficient. Their work together is a continuation of the kind of cooperation among government, private, and educational organizations that created the original Internet.

The idea behind Internet2 is to create a “giant test bed” where new technologies can be tested without impacting the existing Internet.

The three primary goals of Internet2 are to:

- Create a leading edge network capability for the national research community;
- Enable revolutionary Internet applications; and
- Ensure the rapid transfer of new network services and applications to the broader Internet community.

Some of the areas Internet2 participants are focusing on in this pursuit are advanced network infrastructure, new networking capabilities, middleware, and advanced applications. We discuss each of these in the following sections.

**Advanced Network Infrastructure.** The advanced networks created and in use by Internet2 members provide the environment in which new technologies can be tested and enhanced. Several new networks have been established, including Abilene and vBNS (a Worldcom/NSF partnership). Abilene and vBNS (short for very high performance Backbone Network Service) are high performance backbone networks with bandwidths ranging from 2.5 Gbps to 9.6 Gbps that interconnect the gigaPoPs used by Internet2 members to access the network. A gigaPoP is a regional Gigabit Point of Presence, or point of access to the Internet2 network that supports data transfers at the rate of 1 Gbps or higher (see Figure 3.14).

**New Networking Capabilities.** Internet2 is identifying, developing, and testing new networking services and technologies to provide the reliable performance advanced applications require. Internet2 networking projects include:

- deploying the IPV6 addressing protocol;
- developing and implementing new quality of service technologies that will enable the Internet to provide differing levels of service depending on the type and importance of the data being transmitted;
- developing more effective routing practices;

The Internet2® project is just one aspect of the larger second generation Internet we call Internet II.
coordinating the interconnection of the different components of the Internet2 infrastructure — backbones, GigaPoPs, campus LANs, and exchange points; and

creating an infrastructure to efficiently handle one-to-many communications over the Internet (multicasting, described further in the next section).

**Middleware.** Internet2 is developing new middleware capabilities. Researchers are developing standardized middleware that incorporates identification, authentication, authorization, directory, and security services that today are often handled as a part of applications running on the Internet. Internet2 researchers believe advanced middleware will aid application development, increase robustness, assist data management, and provide overall operating efficiencies.

**Advanced Applications.** Internet2 work teams are collaborating on a number of advanced applications, including distributed computation, virtual laboratories, digital libraries, distributed learning, tele-immersion, and a synthesis of all of these working in combination. We will discuss these applications in greater depth in Section 3.5.

In the end, the basic goal of Internet2 is to radically enhance the transmission of video and audio and rich documents to enable wider and more extensive use of the Internet for communications and knowledge sharing.