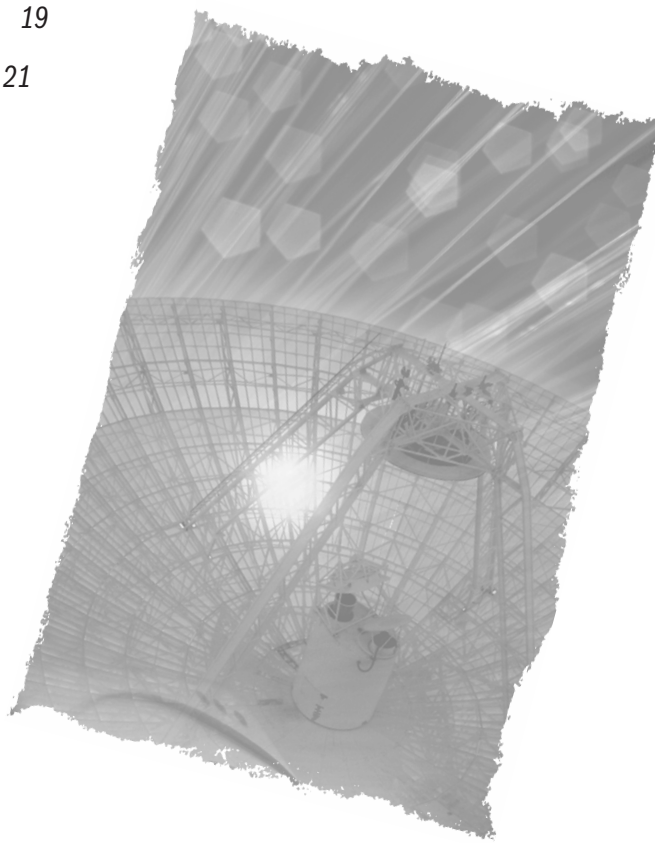
1 Basic Concepts

In this chapter:



Basics matter; new products and services are often developed using technologies that have been available for many years. Continual improvements in these basic tools have led to important innovations. For example, advances in compression spurred developments in downloading music and digital entertainment.

Apple Computer's iTunes service is made possible because the music is compressed, made smaller. Compression squeezes large amounts of data into smaller "pipes," something like putting data into a trash compactor. In addition, compression makes it possible for video to use less of a network's capacity when it is transmitted. Cable and satellite TV operators compress and digitize television signals to expand the number of channels for premium movies and video-on-demand that can be carried over existing network facilities.

Multiplexing is an enabling technology for innovative services in broadband wireless and landline networks. Multiplexing is a way to carry information more efficiently on networks. However, unlike compression, it does not shrink data. Rather, it enables multiple devices and sources of traffic to share telecommunications paths. It uses existing fiber-optic, wireless media and copper cabling to carry an ever-increasing amount of entertainment, voice traffic, and information from multiple sources. With multiplexing, a small number of fiber-optic cables can support entire office parks. Telephone companies no longer bear the expense of laying many strands of copper cabling to support each building in an office park.

Multiplexing and compression could not have made such dramatic breakthroughs without the transition from analog to digital services. Digital signals are clearer, have fewer errors, take up less space, and can be transmitted at higher speeds than analog signals. Digital cable television can carry ten times the number of channels as analog cable television. Moreover, digital TV is spurring the sale of new home entertainment centers to take advantage of surround-sound audio and movie-theater-quality video on some types of digital television sets.

Standardized protocols enabled many changes in how corporations conduct business and consumers communicate. Protocols define how devices and networks communicate with each other. For example, a suite of protocols, transmission control protocol/Internet protocol (TCP/IP), spells out rules for sending voice, images, and data across the Internet and in corporate networks. Corporations and small businesses that initially used the Internet for casual e-mail are now putting important business processes on internal networks and on the Internet. "Open," widely understood Internet protocols like TCP/IP leave networks vulnerable to hackers when they are poorly implemented. Specific protocols such secure socket layer (SSL) have been developed to protect public and private networks from external threats.

Computers are no longer the standalone entities they were initially. Nor are local area networks like the early local area networks that were isolated within departments to share expensive printers or to meet specialized needs such as finance departments'

requirements for accounting packages. Technology that was first developed to connect diverse internal networks to exchange information and e-mail messages within a building and then on campuses now is used to link corporate main offices and remote sales and manufacturing sites. Wide area networks (WANs) link sites *between* metropolitan areas; metropolitan area networks (MANs) link locations *within* metropolitan areas.

Government regulations have added to the amount of traffic and the security requirements on networks. For example, the Sarbanes-Oxley Act of 2002 not only requires that public firms retain more financial documents for longer periods; in addition, internal processes and controls are liable to be audited by the government. Moreover, healthcare institutions need to comply with Health Insurance Portability and Accountability Act of 1996 (HIPPA) rules. HIPPA mandates that healthcare providers protect patient records from snoopers. The bottom line is that LAN networks and devices need to securely handle, store, and back up larger amounts of traffic.

THE TRANSITION TO DIGITAL

The transition from analog to digital networks is a major factor in the economic and technical forces that changed telecommunications dramatically in the twentieth and twenty-first centuries. The analog format, which was designed for lower volumes of voice traffic, is inadequate for the large amounts of voice, data, music, and video images carried on our cellular, public telephone, Internet, and cable TV networks.

Analog Signals—Slower, More Prone to Errors

Analog services are slower and more prone to errors than digital service. Analog signals take the form of waves that are more complex to re-create than digital off and on bits. This is one reason speeds on analog lines are slower than those on digital links. Analog signals also lose strength over shorter distances than digital signals and therefore require more equipment to boost their strength. However, boosting the strength of analog signals introduces impairments such as static in voice calls and blurry images in television signals as they travel further from transmitters.

Impairments on Analog Services—Electrical Interference

Analog telephone signals are analogous to water flowing through a pipe. Rushing water loses force as it travels through a pipe. The further it travels in the pipe, the more force it loses and the weaker it becomes. Similarly, an analog signal weakens as

it travels over distances, whether it is sent over copper, coaxial cable, or through the air as a radio or microwave signal. The signal meets resistance in the media (copper, coaxial cable, air) over which it is sent, causing the signal to fade. In voice conversation, the voice will sound softer. This is referred to as *attenuation*.

In addition to becoming weaker, analog signals react to electrical interference, or "noise," on the line. Power lines, lights, and electric machinery all inject noise in the form of electrical energy into the analog signal. In voice conversations, noise on analog lines is heard as static.

To overcome resistance and boost the signal, an analog wave is periodically strengthened with a device called an *amplifier*. In analog services, the amplifier that strengthens the signal cannot tell the difference between the electrical energy present in the form of noise and the actual voice, video, or data signals. Thus, the noise as well as the signal is amplified. The last mile of cable TV systems in neighborhoods where the cable connects to homes is usually made up of coaxial cabling. In this analog portion, signals are amplified every half a mile. In these systems, amplifying the signal also amplifies the noise. Thus, the television signals are amplified more often as they travel further from the cable providers' equipment, more noise is introduced, and TV reception becomes blurrier. In analog systems, people who live further from their providers have poorer quality TV reception, but they can generally still see the images.

Frequency on Analog Services—Wavelengths

Analog signals move down telephone lines as electromagnetic waves, wavelengths. A *wavelength* is a complete cycle, as illustrated in Figure 1.1. It starts at a zero point of voltage, goes to the highest positive part of the wave, down to the negative voltage portion, and then back to zero. Frequency is expressed in cycles per second, the number of times per second that a wave oscillates, or swings back and forth, in a complete cycle from its starting point to its endpoint.

The higher the frequency, the more cycles of a wave are transmitted in a period of time. This is because the higher the number of waveforms sent, the more data the line can carry. Thus, higher frequencies have more capacity because each wavelength carries voice or data information. *Modulation*, the process of varying characteristics such as amplitude (height), frequency, and phase (shape) of wavelengths, also impacts carrying capacity. Advanced modulation schemes enable wavelengths to carry, for example, 8 bits per wavelength. New wireless services that use advanced modulation are being developed for broadband wireless Internet access.

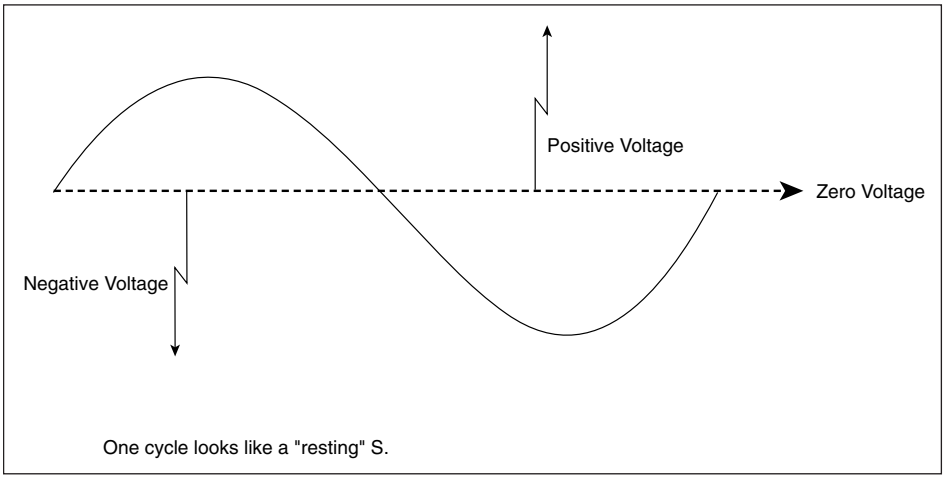


Figure 1.1
One cycle of an analog wave, 1 hertz (Hz).

This speed or frequency is stated in hertz (Hz). For example, a wavelength that oscillates, or swings back and forth, 10 times per second has a speed of 10 hertz (Hz) or cycles per second.

Analog frequencies are expressed in the following abbreviated forms:

- kilohertz or kHz = thousands of cycles per second

  Voice is carried in the frequency range of .3kHz to 3.3kHz, or 3000Hz.

- megahertz or MHz = millions of cycles per second

  Analog cable TV signals are carried in the frequency range of 54MHz to 750MHz.

- gigahertz or GHz = billions of cycles per second

  Most analog microwave towers operate at between 2GHz and 12GHz.

Digital Signals

It wasn't until the 1960s that carriers started taking advantage of the superiority of digital service when they used T-1 links between telephone company central offices. T-1 enabled telephone companies to save on the cost of outside cabling by packing

24 voice channels on two pairs of copper cabling. Digital signals have the following advantages over analog signals:

- Higher speeds
- Clearer video and audio quality
- Greater capacity
- Fewer errors
- More reliability

Binary Bits—On and Off Signals

Instead of waves, digital signals are transmitted in the form of binary bits. The term *binary* means that there are two values for transmitted bits: on and off. On bits are depicted as ones and off bits as zeroes in programming and binary notations. For data transmitted on copper cabling, on bits are represented by positive voltage and off bits by the absence of voltage. In fiber-optic cabling, on bits are represented by light pulses and off bits by the absence of light pulses.

Fewer Errors, Higher Speeds, Additional Reliability

It is faster to re-create binary digital ones and zeros than more complex analog wavelengths. Whereas the highest speed projected for analog dial-up modems is 33,600 bits per second when sending data, digital routers operate at terabit-per-second speeds. A *terabit* is equal to a thousand gigabits; 2,000,000,000,000 bits per second equals two terabits per second.

Digital signals can be re-created more reliably than analog waves. Both analog and digital signals are subject to impairments: They lose strength, fade over distance, and are susceptible to interference such as noise. However, digital signals travel further before fading. Thus, less equipment is needed to boost the signals.

Fewer pieces of equipment translate to lower maintenance and installation costs. At every point that a signal fades, amplifiers or regenerators are required. Each amplifier is a place for a possible failure. For example, water can leak into a telephone company's manhole, or the amplifier itself might fail. Organizations that use digital lines such as T-1 often experience only one or two brief failures in an entire year. High reliability results in lower maintenance costs for telephone companies.

Moreover, digital signals can be "repaired" more cleanly than analog signals. Figure 1.2 illustrates that when a digital signal loses strength and fades over distance, equipment regenerates the signal and discards the noise and static. The noise is not, as in an analog signal in Figure 1.2, regenerated. In digital transmissions, where

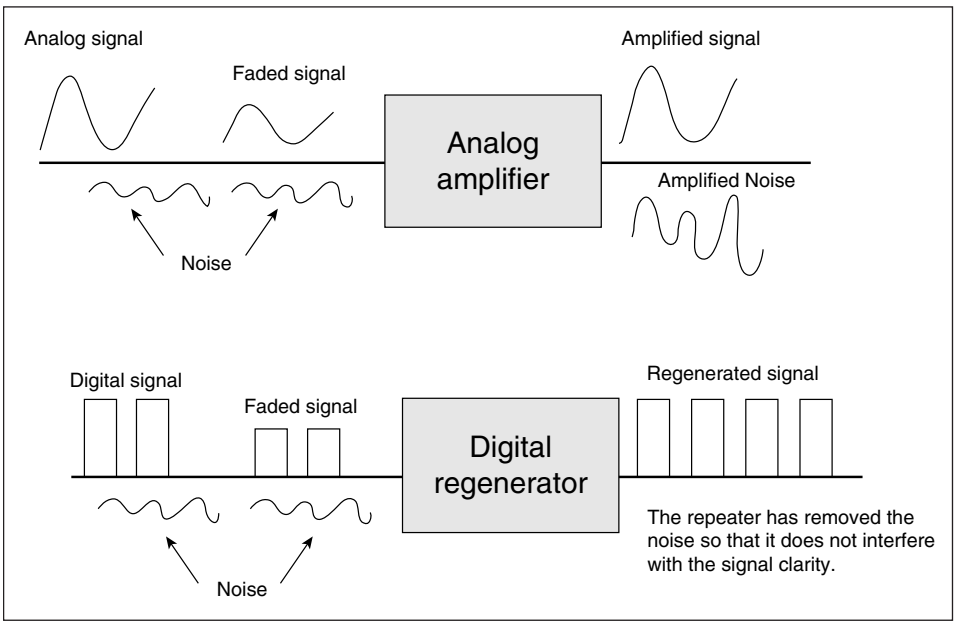


Figure 1.2
Noise amplified on the analog line, eliminated on digital service.

noise is discarded, garbling occurs less frequently; thus, there are fewer errors in the communication.

ADDING MEANING TO SIGNALS—CODES AND BITS

Computers communicate with each other using specialized codes made up of bits. Without these standardized codes, computers would not be able to interpret bits into consistent words in, for example, e-mail messages. Computers can "read" each other's on and off binary bits when these bits are arranged in a standard, predefined series of on and off bits.

People use the terms "bits," "baud rate," and "bytes" interchangeably. Their meanings, however, differ significantly. The signaling speed on analog lines is the *baud rate*, the number of times per second a cycle is completed. The baud rate is measured differently than bits per second. *Bits per second* are the actual number of bits sent in a given time from point A to point B.

A Byte = A Character

Bits organized into groups of 7 or 8 bits are bytes. Each byte is a character, piece of punctuation, or space. Computer hard drive capacity tends to be measured in bytes, but speeds on digital lines are measured in the number of bits transmitted per second. Bytes stored on computer drives are stored in digital form. To summarize, a byte is a character made up of 7 or 8 bits. A bit is an on or off electrical pulse or light pulse.

Baud Rate vs. Bits per Second—Electrical Signal Rates vs. Amount of Information Sent

A *baud* is one analog electrical signal or wavelength. One cycle of an analog wave equals one baud. A complete cycle starts at zero voltage, goes to the highest voltage, down to the lowest negative voltage, and back to zero voltage, the resting S in Figure 1.1. A 1,200-baud line means that the analog wave completes 1,200 cycles in one second. A 2,400-baud line carries 2,400 complete cycles in one second. The term *baud rate* does not indicate the amount of information sent on these waves. It refers only to the number of analog electrical signals—wavelengths or cycles per second.

The public switched telephone network (PSTN) runs at only 2,400 bauds per second. To achieve greater capacity, modem manufacturers design modems capable of carrying more than one bit on each analog wave. Thus, a 9,600-bit-per-second (bps) modem sends 4 bits of data on each analog wave (9600 ÷ 2400 = 4). It is correct to state that the 9,600bps modem runs at 2,400 baud but carries 9,600 bits per second. It still uses a 2,400-baud line.

Baud rate refers to analog, not digital, transmission services. Digital services transmit information as on or off electrical signals in the case of copper wires, and on or off light pulses on fiber-optic lines. On digital services, 56,000-bit-per-second lines can carry 56,000 bits in one second. The speed is 56 Kbps, or 56 kilobits per second.

Codes—Adding Meaning to Bits

All computers use codes so that they can translate bits into meaningful language. The main code American Standard Code for Information Interchange (ASCII), is used in English-language personal computers. The international version of ASCII is known as the International Reference Alphabet (IRA). IBM minis and mainframes use a different code, the Extended Binary Coded Decimal Interexchange Code (EBCDIC).

Distant computers can read simple e-mail messages because they are both in ASCII. American Standard Code for Information Interchange is a 7-bit code. Each character is made up of 7 bits. ASCII is limited to 128 characters. Most PCs now use extended ASCII, which supports 8-bit codes. These characters include all of the

upper- and lowercase letters of the alphabet, numbers, and punctuation such as !, ", and : (see Table 1.1).

Table 1.1 Examples of ASCII Code

Character	ASCII Representation
!	0100001
A	1000001
m	1101101

The limited number of ASCII characters, 128 or 256, results in ASCII not including formatting characters such as underlining, tabs, and columns. Specialized word processing and spreadsheet programs supplement ASCII with formatting and proprietary features such as columns. This is why Microsoft Word documents, for example, need to be "translated" when they are opened in a WordPerfect program. The translation converts Microsoft Word code to WordPerfect code.

In addition, specialized, non-ASCII formatting for tabs, tables, and columns in e-mail messages requires specialized formatting. For example, the Hypertext Markup Language (HTML) and Rich Text Format (RTF) in Microsoft Outlook's e-mail program support this formatting. HTML is the *markup language* used on the World Wide Web. Markup languages specify how characters should be formatted. In Hypertext Markup Language, brackets <> precede text with formatting commands. For example, <bold> tells the e-mail program to bold characters. Other commands in HTML are for linking Web addresses included in e-mail messages to particular Web sites or for adding italics, graphics such as smiley faces, or bulleted text.

MEASURING SPEED AND CAPACITY

In telecommunications, bandwidth refers to capacity. Bandwidth is expressed differently in analog and digital transmissions. The capacity of analog media, such as coaxial cable, is referred to as *frequency.* The bandwidth of an analog service is the difference between the highest and lowest frequency within which the medium carries traffic. For example, in the early 1980s when the government gave spectrum (a range of frequencies) rights to local telephone companies for analog cellular service, it gave it to them in the range of 894MHz to 869MHz. It gave them 25MHz ($894 \times 869 = 25$)

of spectrum. Analog cable TV in the United States uses 6MHz for each channel carried. The greater the difference between the highest and lowest frequency, the higher the capacity or bandwidth supported.

For digital services such as ISDN, T-1, and ATM, speed is stated in bits per second. Simply put, it is the number of bits that can be transmitted in one second. T-1 has a bandwidth of 1.54 million bits per second. Bandwidth or hertz can be expressed in many ways. Some of these include:

- T-1 North American and Japanese circuits have a bandwidth of 1.54 million bits per second, or 1.54 megabits per second (Mbps).
- E-1 European standard circuits have a bandwidth of 2.048 million bits per second, 2.048 megabits per second or 2.048 Mbps.
- Some ATM systems have the capacity for 13.22 billion bits per second, or 13.22 gigabits per second (Gbps).
- One thousand gigabits is called 1 terabit; 10 terabits per second = 10,000,000,000,000 bits per second.

The letter C for *concatenated* is sometimes added to high-speed designations used on optical networks. Concatenated means multiple streams from the same source—such as video—travel together so there are no interruptions in video transmissions that share a multiplexed fiber path with traffic from other sources. To the people watching the video, the images appear as a single stream of video.

Broadband Service—Multiple Data Streams

The International Telecommunication Union (ITU), a standards organization based in Geneva, Switzerland, refers to broadband services as those that generally have the following functionality:

- Operate at higher than 1.54 or 2 megabits per second
- Carry full-motion video, such as that in corporate video conference systems but not as high a quality as broadcast television
- Support multiple streams of traffic simultaneously

The definition of broadband has evolved over time. Broadband originally referred to internal, high-speed, local area networks such Wang Laboratories' WangNet™. This coaxial-cabling-based network transported signals concurrently from multiple personal computers within facilities. One early definition of broadband referred to networks such as cable TV networks in which multiple streams of television channels are transmitted simultaneously. The definition of broadband differs within the industry. An example of this evolution is shown in Table 1.2.

For example, DSL carries data over the same lines used for voice. Cable TV neighborhood networks transport Internet access along with television and voice traffic. The ITU points out that because compression enables slower-speed networks to transmit images, music, and video at higher quality than previously, speed is not always indicative of broadband capabilities. (See the following section for information on compression.) The ITU notes that countries with more wireless than wired telephones concentrate their focus on wireless services to provide widespread broadband Internet access.

Broadband services are characterized as being transported on larger pipes. Just as more water fits into a wider pipe, broadband services carry more information than narrowband lines such as those for analog voice. Some experts define broadband services as those at T-3 and higher speeds. Table 1.2 offers a comparison of broadband and narrowband services.

Table 1.2 Broadband and Narrowband Services

Narrowband	Broadband
T-1 at 1.54Mbps Twenty-four voice or data conversations on fiber optics, infrared, microwave, or two pairs of wire.	***Analog broadcast and cable TV services—use 6MHz per channel*** Multiple television channels broadcast, each using 6MHz of capacity
Analog telephone lines at 3,000Hz Plain old telephone service (POTS) modems used for Internet access.	***Digital broadcast, satellite, and cable TV*** Four to ten channels of programming carried on 6MHz of bandwidth. Newer, digital high definition TV (HDTV) offers enhanced clarity over analog TV.
BRI ISDN at 144Kbps Two paths for voice or data, each at 64Kbps. One path for signals at 16Kbps.	***Mobile data networks*** Advanced wireless networks that enable users to access data at 144 kilobits per second and above speeds.
	T-3 at 44.7megabits per second (equivalent to 28 T-1 circuits) A way of transmitting 672 conversations over fiber optics or digital microwave.

IMPROVING UTILIZATION—COMPRESSION AND MULTIPLEXING

Compression and multiplexing improve efficiency on wireless and wireline networks. Compression shrinks the data, and multiplexing combines data from multiple sources onto a single path.

Compression—Shrinking Data to Send More Information

Just as a trash compactor makes trash smaller so that more refuse can be packed into a garbage barrel, compression makes data smaller so that more information can be packed into networks. It is a technique to add more capacity on telephone lines, cable TV networks, the Internet, advanced cellular networks, and airwaves used for broadcasts. Advances in compression have enormous potential to make cable modems, DSL services, and cellular networks adequate for movies, games, music, and downloading graphics such as JPEG and PowerPoint images.

In addition, enterprise customers use compression as one way to add capacity to their internal networks and to the links between their sites. For example, instead of upgrading to higher-speed lines to other branch offices, they may add hardware with software that compresses traffic before it is transmitted to the branch office. At the remote site, a device decompresses the voice and data back to its original format.

In video, compression works by transmitting only the changed image, not the same image over and over. For example, in a videoconference, nothing is transmitted after the initial image of a person until that person moves or speaks. Fixed objects such as walls, desks and background are not repeatedly transmitted. The device performing the compression, the *codec*, knows that discarding minor changes in the image won't noticeably distort the viewed image.

Throughput—User Information Transmitted

Throughput is the actual amount of useful data sent on a transmission. Improvements in throughput increase the amount of data transmitted in a given amount of time over, for example, DSL or cable modems. Compression increases throughput without changing the actual speed of the line. For instance, a song that is compressed may be downloaded in just a few seconds rather than a minute or two. Users often send large graphics attachments in compressed formats; this makes the files smaller and quicker to send. They use compression software such as Stuffit®. However, the network's speed has not changed. The file has been squeezed into a smaller format at the sending end and put back into a larger format by the receiver's compatible software.

When compression is used with text and facsimile, data to be transmitted is reduced by removing white spaces and redundant images and by abbreviating the most frequently appearing letters. When modems equipped with compression transmit text, repeated letters are abbreviated into smaller codes. For example, the letters E, T, O, and I appear frequently in text. Compression sends shortened versions of these letters with 3 bits rather than the entire 8 bits for each letter. Thus, a page of text might be sent using 1,600 bits rather than 2,200 bits. With facsimile, compression removes white spaces from pictures and only transmits the images.

Compression Standards = Interoperability

There are many types of compression methods. A device called a codec (short for coder-decoder) encodes text, audio, video, or images using a mathematical algorithm. For compression to work, both the sending and receiving ends must use the same compression method. The sending end looks at the data, voice, or image. It then compresses it using a mathematical algorithm. The receiver decodes the transmission. Compression on devices such as modems and video teleconferencing from various manufacturers can interoperate when both devices use agreed-upon compression standards.

More powerful personal computers as well as improvements in compression have increased the use of streaming audio and video over the Internet. Further improvements in compression make streaming audio and graphics viable for slower-speed cellular devices. RealNetworks®, Inc. makes its decoding compression and player software available free or at minimal costs to consumers. The strategy is to make its software so prevalent among consumers that software developers will purchase RealNetworks' server products to create content such as Web ads and other graphics in Web pages. See the Table 1.3 at the end of this chapter for compression standards.

MPEG Standards—Compressing Audio and Video

The International Telecommunications Union (ITU) formed the Moving Picture Experts Group (MPEG) in 1991 to develop compression standards for playback of video clips and digital TV. MPEG-3 also came to be used for streaming audio. MPEG and proprietary streaming media compression schemes are asymmetrical. It takes more processing power to encode at the Internet, satellite TV, broadcaster, or cable TV provider than to decode an image at the customer. Streaming compression algorithms assume that the end user will have less processing power to decode transmissions than the developers and broadcasters that encode the video and audio. A newer

standard, MPEG-4, is designed for multimedia files and television and is able to compress files to use four times less capacity than MPEG-2.

Some applications require better resolution than supplied by asymmetric compression software. Radiology departments for viewing images, firefighters for viewing forest fires images beamed from airplanes, and the FBI for fingerprint viewing are examples that might use symmetric compression software.

Streaming—Listening and Viewing Without Downloading

Streaming, an important feature of browsers, is different than downloading. When text, music, or graphics are downloaded, the entire file must be downloaded before it can be viewed or played. When music is streamed, callers listen to the music but cannot store it to listen to it later. Downloading actually stores the music files on a listener's computer hard drive.

Streaming speeds up transmission of video, images, and audio over the Internet. When graphics and text are sent to an Internet user's browser, the text can be viewed as soon as it reaches the PC. The graphics, which take longer to be viewed, are filled in as they are received.

Compressing and Digitizing Speech

Speech, audio, and television are analog in their original form. Before they are transmitted over digital landline or wireless networks, codecs compress (encode) them and convert them to digital. Codecs sample speech at different heights (amplitude) along the sound wave and convert it to a one or a zero. At the receiving end, decoders convert the ones and zeros back to sound or video waves. With compression, codecs do not have to sample every height on the sound wave to achieve high-quality sound. For example, they skip silence or predict the next sound based on the previous sound. Thus, fewer bits per second are transmitted to represent the speech. Codecs are located in cellular handsets, telephones, high definition TV transmitters, set-top boxes, televisions, IP telephones, and radios. Codecs also compress voice in speech recognition systems.

Multiplexing—Let's Share

Multiplexing combines traffic from multiple voice or data devices into one stream so that it can share a telecommunications path. Like compression, multiplexing enables companies and carriers to send more information on cellular airwaves and telephone

networks. However, unlike compression, multiplexing does not alter the actual data sent. Multiplexing equipment is located in long distance companies, in local telephone companies, and at end user premises. It is used with both analog and digital services. Examples of multiplexing over digital facilities include T-1, fractional T-1, E-1, E-3, T-3, ISDN, and ATM. See Figure 1.3.

The oldest multiplexing techniques were devised by AT&T for use with analog voice services. The goal was to make more efficient use of the most expensive portion of the public telephone network, the outside wires used to connect homes and telephone offices to each other. This analog technique was referred to as *frequency division multiplexing*. Frequency division multiplexing divides the available range of frequencies among multiple users. It enabled multiple voice and later data calls to

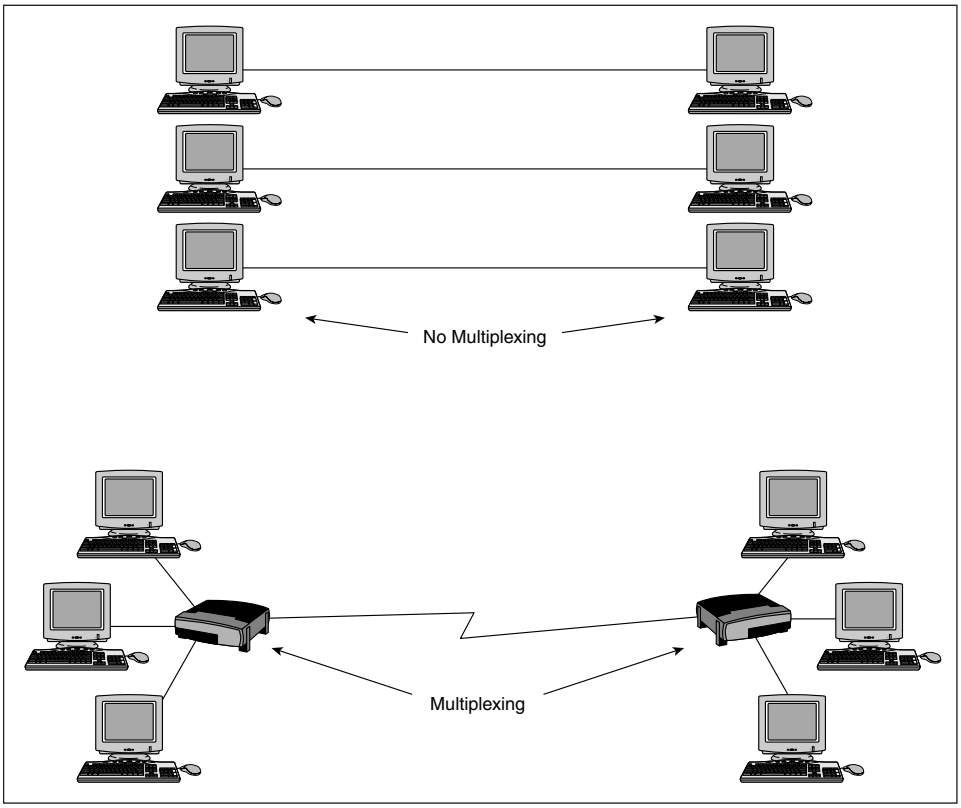


Figure 1.3
Multiplexing.

share paths between central offices. Thus, AT&T did not need to provide a cable connection for each conversation. Rather, multiple conversations could share the same wire between telephone company central offices.

Time Division Multiplexing—Higher Capacity with Digital Multiplexing

Time division multiplexing is a digital multiplexing scheme that saves capacity for each device or voice on a telephone call. Once a connection is established, capacity is saved even when the device is not sending information. For example, if a call is put on hold, no other device can use this spare capacity. Small slices of silence with thousands of calls in progress in carriers' networks result in high amounts of unused capacity. This is the reason time division multiplexing is not as efficient as newer technologies such as Voice over IP, in which voice and data are interspersed whenever possible.

Both T-1 and T-3 use time division multiplexing. T-3 carries 672 conversations over one line at a speed of 45 megabits per second. A matching multiplexer is required at both the sending and receiving end of the channel. T-3 is used for very large customers and Internet service provider networks. At telephone companies, higher speeds are replacing T-3 lines.

T-1 is lower in cost and capacity than T-3. T-1 allows 24 voice, video, and/or data conversations to share one path. It is the most common form of multiplexing at end user organizations. T-1 applications include linking organization sites together for voice calls, Internet access, and links between business customers and telephone companies. Price competition among carriers and manufacturing efficiencies have driven down T-1 costs to make it affordable for small organizations that frequently use one T-1 circuit for both Internet access and voice calling.

Statistical Multiplexing—First Come, First Served Prioritization

Statistical multiplexers do not guarantee capacity for each device connected to it. Rather, they transmit voice, data, and images on a first come, first serve basis as long as there is capacity. Asynchronous transfer mode (ATM) and Ethernet are examples of statistical multiplexing techniques. ATM supports a variety of classes of services. One of these is variable bit rate (VBR). VBR traffic is sent over available capacity not used for traffic with a higher priority.

Statistical multiplexers support more devices than time division multiplexers because they don't need to save capacity when a device is not active. Carriers can sell

aggregated Internet access equal to higher speeds than the ports on their network. For example, Internet service providers may sell 250 megabits of Internet access supported by a 155-MBps ATM multiplexer.

INTEROPERABILITY—PROTOCOLS AND ARCHITECTURES

Protocols enable like devices to communicate with each other by providing a common set of rules. Standardized protocols for wireless local area networks (LANs) have made the convenience of affordable wireless services available to more homes and smaller businesses than ever before. (See Chapter 9 for wireless LANs.)

Protocols—A Common Set of Rules

Protocols are key enablers for all types of communications, including the proliferation of affordable Internet access. Devices communicate over the Internet using a suite of protocols called TCP/IP. For example, the IP, or Internet protocol, portion of TCP/IP allows portions of messages called datagrams to take different routes through the Internet. The datagrams are assembled into one message at the receiving end of the route. Other protocols, such as Bluetooth, make possible wireless communications among devices located within 33 feet of each other.

The following are examples of protocol functions:

- Who transmits first?
- Which network sent this packet?
- In a network with many devices, how is it decided whose turn it is to transmit?
- How is it determined if an error has occurred?
- Which applications is this message allowed to access?
- What is this packet's priority?
- If there is an error, does the entire transmission have to be re-sent or just the portion with the error?
- How is data packaged to be sent, one bit at a time or one block of bits at a time? How many bits are in each block? Should data be put into envelopes called packets?

Protocol structures impact speed, cost, and efficiency. The following protocols illustrate this point:

- *Secure sockets layer (SSL)*—Encrypts (scrambles) communications between a user's browser and Web pages so that only the authorized server (computer containing the electronic commerce application) can read credit card information. It also provides authentication—are you who you say you are? Users know if a site uses SLL by the locked padlock displayed on their screens during transactions.
- *Session initiation protocol (SIP)*—SIP is a signaling protocol used to set up phone calls in some Voice over IP telephone systems that convert voice into packets in data networks. As the session initiation protocol is adopted uniformly, it is hoped that feature-rich telephones and applications from many manufacturers can be intermixed in telephone systems. The expectation is that this will drive down the cost of multibutton telephones for Voice over IP systems. SIP is also used to set up real time audio conferences, videoconferences and instant-messaging sessions.

Architectures—How Devices Fit Together in a Network

Architectures define how computers are tied together. The main goal of architectures is to enable dissimilar protocols and computer networks to communicate. During the 1970s, the International Organization for Standardization developed an architecture, Open System Interconnection (OSI), to provide the means for devices from multiple vendors to interoperate. OSI is based on the earlier four-layer suite of protocols, TCP/IP. The short form of the name for the International Organization for Standardization is ISO, which is Greek for "same or equal."

Although OSI was not widely implemented because of its complexity, it has had a profound influence on telecommunications. It laid the foundation for the concept of open communications among multiple manufacturers' devices. The basic concept of OSI is that of layering. (See Table 1.4 at the conclusion of this chapter.) Groups of functions are broken up into seven layers, which can be changed and developed without having to change any other layer. LANs, public networks, and the Internet's TCP/IP suite of protocols are based a layered architecture.

The Internet suite of protocols, TCP/IP, corresponds to the functions in Layers 3 and 4 of the OSI model. These functions are addressing, error control, and access to the network. The TCP/IP suite of protocols provides a uniform way for diverse devices to communicate with each other from all over the world. It was developed in the 1970s by the U.S. Department of Defense and was provided at no charge to end

users in its basic format. Having a readily available, standard protocol is a key ingredient in the spread of the Internet.

In layered architectures or protocol suites, when transmitting, layers communicate with the layer immediately below them. Only Layer 1 actually transmits to the network. On the receiving end, Layer 1 receives the data and sends it to Layer 2, which then reads the Layer 2 protocol before sending the message to the next higher layer, and so on to the application layer.

TYPES OF NETWORKS—LANS, MANS, AND WANS...

The difference between LANs, MANs, and WANs is the distance over which devices can communicate with others. (See Table 1.5 at the end of this chapter.) As the name implies, a local area network is local in nature. It is owned by one organization and is located in a limited geographic area, most commonly a single building. In large organizations, LANs can be linked together within a complex of buildings on a campus. These organizations often refer to their linked LANs as their network (see Figure 1.4). Devices such as computers linked together within a city or metropolitan area are part of a metropolitan area network (MAN). Similarly, devices that are linked together between cities are part of a wide area network (WAN).

LANs—Local Area Networks

A discrete LAN is typically located on the same floor or within the same department of an organization. LANs first appeared in 1980. The initial impetus for tying PCs together was to share costly peripherals such as high-speed printers. Users exchange files and e-mail, access the Internet, and share resources over local area networks (LANs). Examples of devices within LANs are shared printers, PCs, alarm devices, factory automation gear, quality-control systems, shared databases, voice mail, telephone systems, factory and retail scanners, and security monitors.

Network operating systems control access to the LAN where resources such as files, printers, and security applications are located. Microsoft Windows 2000 and Advanced Server, and Novell NetWare are client-server-based LAN network operating systems.

LAN network operating systems (NOS) software is located on specialized computers called file servers connected to the LAN. In addition, LAN operating system client software is located on each device, such as PCs and printers connected to the LAN. Access to file servers can be limited by password to only approved users (clients). Most operating systems in use today are built on the client-server model. Clients (PCs) request services such as printing and access to databases. Applications such as print and e-mail servers run access to services (such as printers and databases).

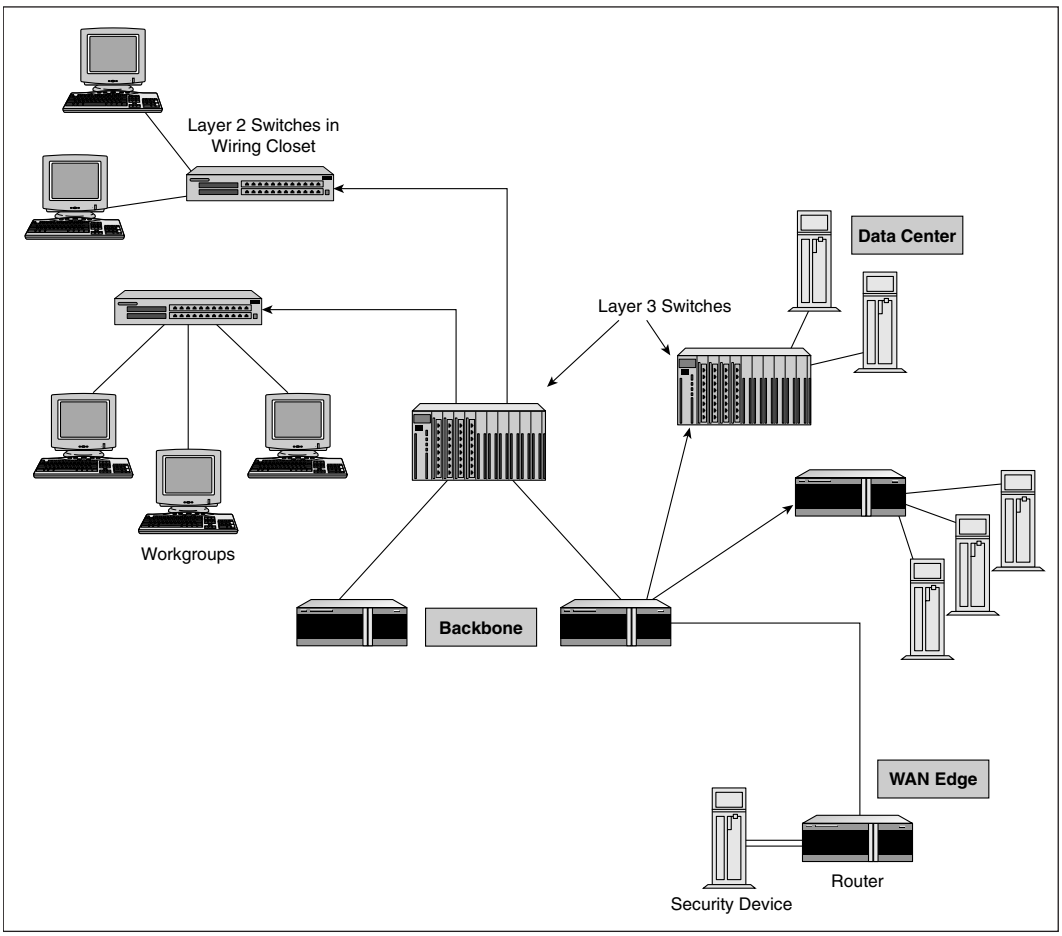


Figure 1.4
LAN architecture.

The Ethernet Protocol—Within LANs

Ethernet, which is based on the 802.3 standard approved by the Institute of Electrical and Electronics Engineers (IEEE), is used by devices such as personal computers to access the LAN and to retrieve packets carried on the LAN. Each device on an Ethernet local area network has a medium access control (MAC) address. Wi-Fi and other 802.11-type wireless LANs also use Ethernet to access the LAN. But the version used on wireless networks operates a little differently. (See Chapter 9 for Wireless LAN networks.) For the most part, devices are connected to a LAN by twisted pair cabling

that is similar to but sometimes of a higher quality than cabling used for business telephones. (Media options are covered in Chapter 2, "VoIP Systems, Circuit Switched PBXs, and Cabling.")

TCP/IP Protocols—Communications Between Networks

Whereas Ethernet is a way for individual packets to access LANs and retrieve packets from local networks, TCP/IP is used to tie LANs together and to route packets between networks. As the need arose to tie LANs together for e-mail and file sharing, compatibility between LANs from different manufacturers became a problem. The TCP/IP suite of protocols became a popular choice for overcoming these incompatibilities and for managing the flow of information on LANs. NetBEUI is another high-level protocol that manages communications between devices on a LAN. It is an early protocol based on an IBM's NetBIOS protocol. It is used primarily for devices in smaller, departmental LANS.

Bridges and routers were developed to send data between LANs. Routers send packets to individual networks based on their Internet protocol (IP) address. IP addresses are assigned to individual networks.

LAN and WAN Devices—Higher Speeds, Lower Prices

LAN and WAN gear handle more traffic in carrier and enterprise networks than ever before. Early LANs operated at 10 megabits per second. New backbone LAN switches typically operate at gigabit (billion bit per second) speeds and are connected to each other with fiber-optic rather than unshielded twisted pair (copper) cabling. In addition, connections on Layer 2 and Layer 3 switches run at *wire speed.* Wire speed refers to switches able to forward packets equal to the full speed of their ports. Ports are the interfaces to which cabling is connected. Wire speed is achieved with powerful switch processors, the computers that look up addresses and forward packets.

Lower equipment prices are making LANs feasible for small businesses and residences. One factor in lower prices is the fact that many devices are based on standards so that manufacturing costs have been driven lower.

The major challenges in managing local area networks are keeping networks secure from hackers and virus free. The fact that networks operate on common protocols that hackers understand makes it easier for these hackers to create malicious software with embedded code capable of corrupting and destroying files. The embedded

code often takes over computers and uses them to send malicious code to hundreds of other computers, thus wrecking havoc on networks.

The Impact of High-Bandwidth Applications

LANs no longer carry mostly "bursty" traffic such as brief e-mail messages for which early LANs were designed. New applications consist of traffic with a longer duration and shorter pauses between packets for other devices to transmit. The following are some examples:

- Large graphical attachments such as PowerPoint® files.
- Server farms, centralized locations in corporations' or carriers' networks with groups of servers containing large databases and backup copies of databases.
- Daily backups to databases of entire corporate electronic files.
- Web downloads of long, continuous streams of images, audio, and video files.
- Voice mail, call center, and voice traffic.
- Web access typified by users with four or more pages open concurrently. Each open Web page is a session, an open communication with packets traveling between the user and the Internet.

MANAGING WEB PAGES—LAYER 4 SWITCHES, ACCELERATORS, AND DEEP PACKET INSPECTION

The images people click on and the Web addresses they type in when they browse the Internet send them to specific Web pages. The Web pages are at sites owned by medium and large businesses, government offices, and educational and healthcare institutions. They are also located at sites that host Web pages for small and medium-sized businesses and large enterprises that don't want to dedicate resources to managing their own Web pages. Hosting companies include carriers such as AT&T, MCI, Sprint, and SAVVIS Communications Corporation, which purchased Cable & Wireless USA, Inc., including their hosting service (Exodus). (Purchases of AT&T by SBC Communications and MCI by either Verizon Communications or Qwest Communications International have been announced.)

MANAGING WEB PAGES—LAYER 4 SWITCHES, ACCELERATORS, AND DEEP PACKET INSPECTION (CONTINUED)

The actual Web pages that people view when they browse the Internet are located on clusters of computers called Web server farms. The Web servers communicate with application servers that store applications for business processes such as purchases and surveys conducted online. When someone is making a purchase online, he or she is using software on these application servers. The application server, in turn, may be pulling information about the product or user from large enterprise applications such as those offered by Oracle or PeopleSoft. Databases used by these applications are located in storage networks.

Hosting sites use Layer 4 switches, also known as content switches, to improve the up time (availability) of Web server farms. They also make these sites more efficient by balancing traffic among the servers in which Web pages are located. For example, they send traffic either in a round robin, predetermined fashion or to the server or port that has been idle the longest.

Layer 4 switches look deeper into packets so that they can send them to particular ports on servers. Layer 3 switches only look at the packet's IP address, which identifies the network. They keep track of which Web servers are up and which are out of service. They monitor each session for the duration of the connection. They can take servers out of service without disrupting transactions or Web surfing. For example, if someone is in the middle of making a purchase when the server he or she is connected to goes down, he or she is transferred to a different server seamlessly without losing data already entered for the transaction. This is because the Layer 4 switch has stayed on the "call" to manage it.

Next-generation Layer 7 switches provide deep packet inspection to improve security on Web traffic. Deep packet inspection looks deeper into the packet than Layer 4 switches to learn which application is being used. They look at bits in the packet, the "signature," that indicate which application is associated with the packet. It can determine, for example, if the packet is used for an Oracle, PeopleSoft, or Microsoft application. Specialized cards in the switch decrypt, or unscramble, data as it enters the Web site and re-encrypt data sent to the user. Software companies that develop these applications need to share information with vendors that produce Layer 7 switches so that they can recognize "signature" arrangements of bits for particular applications.

MANAGING WEB PAGES—LAYER 4 SWITCHES, ACCELERATORS, AND DEEP PACKET INSPECTION (CONTINUED)

Another new development is accelerators that are installed on separate computers called appliances and that use compression to make files smaller so that they take less time to be transmitted to end users. This enables sites to handle more traffic without adding capacity because browsing and viewing graphics and video tie up Web sites for shorter amounts of time when they are accelerated (compressed).

In addition to the preceding equipment that increases Web sites' robustness and efficiency, large organizations often have backups offsite or locally of their entire Web server farm, Web application server, and databases.

Hubs and Bridges

Hubs and bridges were deployed in the 1980s and the 1990s. Using hubs reduced the cost of cabling in LANs. Bridges were used to link local area networks that used the same protocols or a limited number of different protocols together.

Hubs—Largely Replaced by Switches

Hubs were developed to enable devices on LANs to be linked together by twisted pair copper wire instead of the heavier, thicker coaxial cable that was used in early LANs. Coaxial cable is expensive to install and move and requires more space in dropped ceilings and conduit. Hubs operate as "repeaters." Each device repeats each message to the next device on the network, and the device to which the message is addressed takes it off the network.

With a hub, each node or device is wired back to the hub in a star pattern. The hub creates a star design, or topology. (Topology is "the view from above"—in the case of hubs, each device is connected to a central device, the hub.) Prior to hubs, each device in a LAN was wired to another device in a "bus" arrangement. In the bus topology, if one PC is out of service or if there is a break in the cable, other nodes (devices attached to the LAN) are affected. By employing a hub, a device can be moved or taken out of service if it is defective without affecting other devices on the LAN. A hub is located in the wiring closet of each floor within a building.

Layer 2 switches have generally replaced hubs because of hubs' limitations:

- Only one device at a time can communicate on each LAN.

- Each message is sent to every node (device attached to the LAN).
- Hubs can't accommodate the multimedia services on today's networks. Although speeds are 10 megabits, actual throughput, user information transmitted, is much less because of retransmissions and collisions that occur when multiple nodes attempt to transmit simultaneously.

Bridges—Less Flexible Than Routers and Switches

Bridges became available in the 1980s as a way to connect a small number of LANs together. Bridges provide one common path over which multiple LANs can be connected together. For example, if an organization has two locations in different cities that need to exchange data, a bridge can be used. Bridges also are used as a way to reduce LAN congestion. The bridge can connect two different departments so that each departmental LAN is not congested with interdepartmental traffic. Bridges most often connect two LANs with like protocols such as an Ethernet LAN to an Ethernet LAN. There are more sophisticated bridges that connect an IBM token ring network to an Ethernet LAN.

As LANs proliferated and router prices dropped, people turned to more powerful and feature-rich routers and switches rather than bridges.

Layer 2 Switches—Connections to the Desktop

Layer 2 devices store and forward packets and filter packets so that they need not be broadcast to all users. Devices on LANs such as PCs, workstations, and printers are connected to Layer 2 switches located in each floors' wiring closet.

Networks that use switches

- Are faster than hubs
- Don't broadcast every message to each user
- Are simpler to manage than routers because each device's address does not need to be maintained in the switch memory (see the section on routers below)
- Provide more bandwidth per device than hubs

Some Layer 2 switches are *non-blocking*. They have enough capability so that each device can communicate at the same time up to the full speed of the port to which they are connected. For example, a switch capable of forwarding packets at 100 million bits per second would be non-blocking if 10 users were connected to the switch and each could concurrently forward 10 million packets per second ($10 \times 10{,}000{,}000 = 100{,}000{,}000$).

Layer 2 switches are located either in work groups where they are connected to a group of 24 or 48 or so users or in wiring closets serving a few hundred users. The

number of nodes (devices) connected to a switch depends on the switch's speed and the users' requirements.

Virtual LANs—A Way to Segregate Devices

A virtual local area network is made up of devices, such as personal computers and wireless telephones, whose addresses are programmed as a group in Layer 2 switches to give them higher capacity or special privileges or to segregate them from the rest of the corporate network for higher security. They are programmed as a separate LAN but are sometimes connected to the same switch as other devices. Voice over Internet protocol telephones that send voice as packets over networks and wireless LAN devices are often programmed into their own virtual LANs. These devices allow only certain types of equipment, such as other telephones, to communicate with them. Some computers are put into virtual LANs so that they can access secure files such as healthcare records.

Layer 3 Switches—Also Known as Switching Routers

Layer 3 switches are faster and more complex to install and maintain than Layer 2 switches. A Layer 3 switch has connections to multiple Layer 2 switches, and each port has routing capability. If a link to one switch is down, the Layer 3 switch can send traffic via another link. Layer 3 switches generally are located in wiring closets (connecting hundreds of users) or LAN data centers (connecting many wiring closets or buildings together). Most enterprises use Layer 3 switches to connect traffic on the LAN or campus backbone.

Because of increased traffic on corporate local area networks, most new Layer 3 switches support 1 gigabit and 10 gigabit speeds. In addition, they tend to be larger than Layer 2 switches. They are housed in chassis (cabinets). Chassis look like refrigerators. They have multiple or single carriers (shelves) with blades (circuit packs) positioned vertically in slots (see Figure 1.5). Many Layer 2 switches are rack mounted with horizontally positioned blades. Rack-mounted equipment is 19 inches wide and is housed in equipment racks with other LAN devices.

Routers—To Access the Internet and Carry Internet Traffic

In enterprise and home networks, routers connect LANs to the Internet, to carriers' networks, and to other corporate sites. Internet-based routers in carriers' networks forward packets over the least congested paths, also called *hops* because packets "hop" from router to router to reach their destination. To illustrate, a user may send two mes-

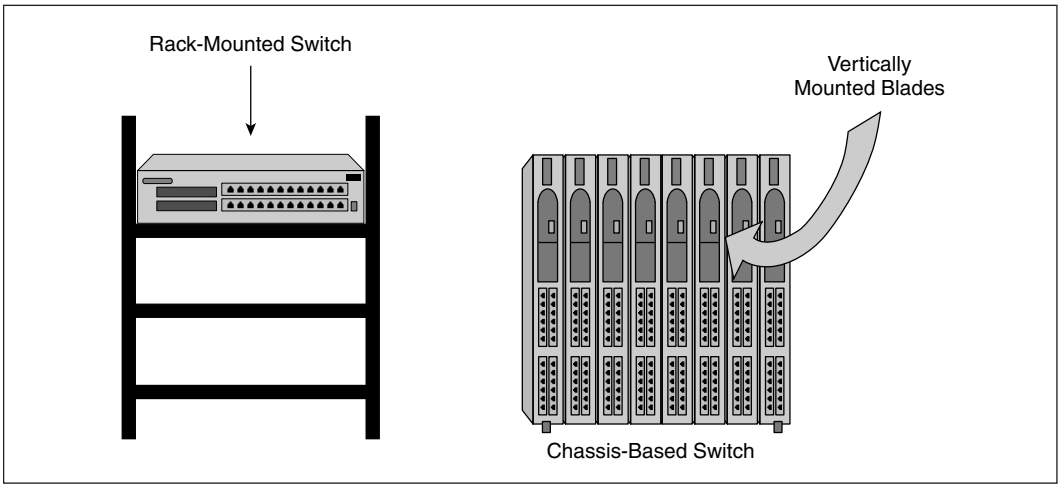


Figure 1.5
Rack-mounted and chassis-based switches.

sages from Chicago to Los Angeles. The first message might travel via Alaska and the second via Texas. Because of congestion and the route taken, the second message might arrive before the first one. A major advantage of routers is their capability to forward differing protocols from varied departmental local area networks. It is important to note that routers do not translate application protocols. A UNIX computer cannot read a Microsoft Windows word processing document. The router merely transports differing LAN protocols in corporate and carrier networks.

Router capabilities include:

- *Queuing*—If the path the data takes is congested, the router can hold the data in a queue until capacity is available.
- *Path optimization*—The sending router selects the best available path by checking routing tables contained within the router.
- *Priority routing*—Some routers contain protocols that let them assign priority to packets with particular types of headers.

Intelligence inherent in routers leads to a major disadvantage: Routers are complex to install and maintain. Every router in an organization's network must have up-to-date address tables. Each device on a LAN is called a node and has an address. For example, if a printer or PC is moved from one LAN to another, the router table must be updated or messages will not reach that device. New routers are faster because they do not look up each packet's address in the CPU's memory. Routers check the routing table for the first packet's address and then store the address in chips on a card or a module.

Blades

Routers contain circuit boards located in slots within the router. Circuit boards are often referred to as *blades* when they are dense—for example, when they have many ports (connections). Specialized blades are available for wide area network T-1 and T-3 connections. (See Chapter 5, "VPNs and Specialized Network Services," for T-1 and T-3.) Blades may also be firewalls, hardware and software used to block hacker access to internal networks. Blades are also used in switches.

The functions of congestion control, routing, sequencing, and receipt acknowledgment make routers network Layer 3 devices.

Home LANs—Sharing High-Speed Internet Access

According to statistics released in April 2004 by the Pew Internet & American Life Project, 34% of U.S. residential broadband users have home networks, 21% use wired home networks, and 13% use wireless products such as Wi-Fi. (See Chapter 9 for wireless home networks.) In addition, Pew found that 6% of dial-up users have home networks. Home networks enable residents to share DSL and cable modem Internet access, printers, and multimedia files such as television and movies among multiple computers. The following factors have led to a growth of home networks:

- Lower broadband Internet access prices are spurring purchase of DSL and cable modem connections.
- The availability of less-complex setup procedures for home networks.
- Decreases in router costs.
- More powerful PCs with larger memories to handle Web and music files downloaded from the Internet.
- The desire by users for e-mail and Internet access at home.
- Lower-cost PCs so that families can purchase separate computers for parents and children.
- The requirement for people who work from home full time or part time to access files remotely using high-speed Internet access.

Although often slower and less complex, home networks are created along the same line as corporate networks. Hubs and switches (built into home routers) connect devices together via cabling or wireless media. Routers provide shared access for all PCs to high-speed Internet connections. Equipment on home LANs includes PCs, switch/routers, media centers with movies and television shows, printers, and scanners. Each computer and printer connected to the LAN needs an Ethernet card for connection to a cable that is plugged into the switch/router. If the computer is in

another room, the PC is plugged into an RJ-45 data jack from which unshielded twisted pair cabling is run to the switch/router. RJ-45 jacks are similar to jacks that analog phones plug into except that they have four wires (two pair) instead of the one pair used for analog phone service.

To share high-speed DSL or cable modem service, users purchase switch and router functions in one "box" from vendors such as LinkSys, 3Com, and NETGEAR for Windows and Xsense for Macintosh computers (see Figure 1.6). In addition to cabling, computer software needs to be installed on personal computers. In addition to wireless and coaxial-cabling-based networks, running data and multimedia is possible through a home's electrical wiring using a standard called HomePlug. HomePlug service for the most part augments wireless home networks in instances in which the wireless network coverage does not extend to another floor or porch. With HomePlug hardware, users plug their router into a 4-inch by 2-inch device that is plugged into a wall outlet. In the distant room, a computer is plugged into another 4-inch by 2-inch device that is also plugged into an electrical outlet. The top speed on HomePlug is 14 megabits per second.

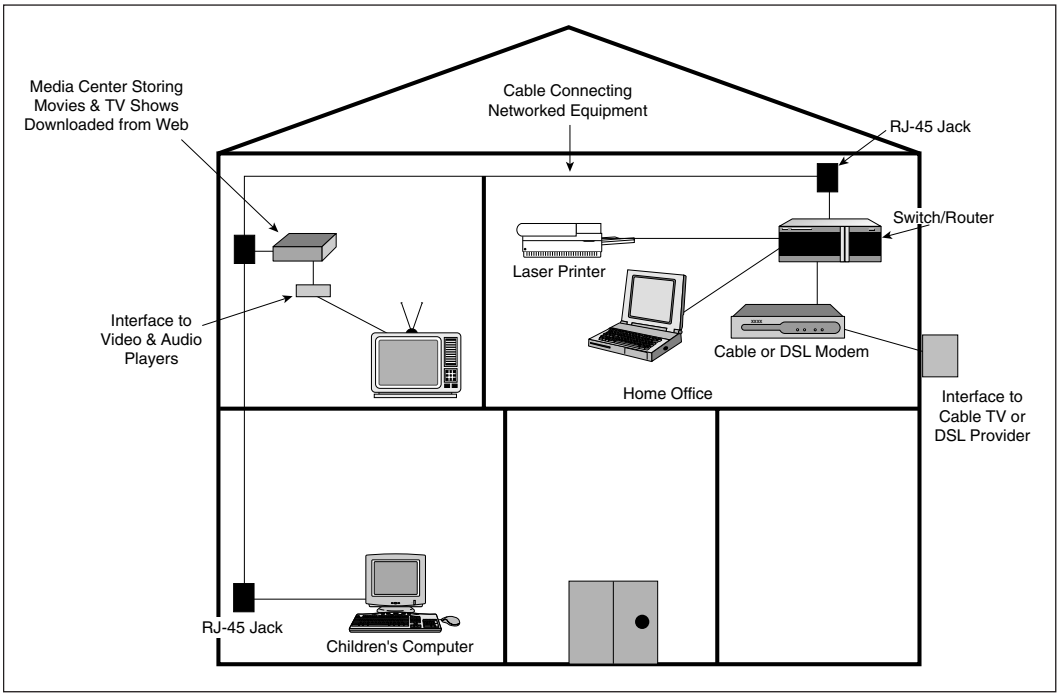


Figure 1.6
Home LAN.

The biggest challenge to implementing home networks is making them secure against viruses that are inadvertently downloaded when people open e-mail attachments and from hackers that access files on peoples' computers that are on and connected to broadband networks. Homes users often purchase routers equipped with firewall software to keep out hackers and anti virus software that they install on their computers and keep updated with the latest anti virus updates.

Poor customer support is a major impediment to the implementation of home networks. Customers often require help from router companies, friends, and the MIS staff where they work to set up their networks.

Most carriers that sell high-speed Internet access to consumers are concerned about home LANs that generate large amounts of traffic with applications such as online games and song sharing, also referred to as peering. Some cable companies and DSL providers charge higher fees to customers who generate large amounts of traffic. The growing residential adoption of broadband is adding traffic to Internet backbones and edge networks operated by carriers such as Level 3, AT&T, Sprint, and MCI.

MANs—Metropolitan Area Networks . . . Links Within Cities

Metropolitan area networks, or MANs, are connections between local area networks within a city or within a large campus. Campus MANs are spread out over many blocks of a city. Examples of MANs are those at large hospitals and university complexes. For example, a hospital in downtown Boston keeps its x-rays and medical records in a nearby section of the city. Instead of trucking records and x-rays between the two sites, the hospital leases high-capacity telephone lines to transmit records and images. The connections between these two sites are metropolitan area networks. These links can be leased from a telephone company or constructed by the organization. They operate over fiber-optic, copper, or microwave-based media. They also include the same services mentioned for WANs, such as Gigabit Ethernet, T-3, and T-1.

WANs—Wide Area Networks . . . Links Between Cities

The term "WAN" refers to connections between locations over long distances via telecommunications links. For example, a warehouse in Alabama connected to a sales office in Massachusetts by a T-1 line is a wide area network (WAN) connection. In contrast to a local area network, a WAN is not contained within a limited geographical location. The variety of WAN connections available is complex. Selection of an appropriate WAN service depends on the amount of traffic between locations, the

quality of service needed, the price, and the compatibility with the organization's computer systems. WAN technologies and WAN vendors are reviewed in Chapter 6. These include ISDN, T-1, T-3, ATM, and frame relay.

Instead of complex WANs, many organizations now have high-speed connections either to the Internet or to carriers instead of directly to other corporate locations. Carriers manage the security and transmission of their customers' telecommunications in virtual private network (VPN) arrangements. (See Chapter 5, "VPNs and Specialized Network Services," for VPNs.)

Higher Speed Services for LAN Traffic

Not only is the nature of LAN traffic changing but the number of applications is growing.

- Gigabit Ethernet is a high-speed Ethernet protocol. It requires fiber-optic cabling or Level 6 unshielded twisted pair because of its high speeds. Level 6 cabling is built to higher standards of performance than Level 3 and Level 5 cabling. (See Chapter 2 for media.) Gigabit Ethernet is used for connections on backbone enterprise networks and servers in data centers. New Layer 3 switches operate at gigabit speeds.
- Fibre channel protocols are used for gigabit speed, highly reliable short-distance access to devices such as disks, graphics equipment, video input/output devices, and storage devices that hold massive amounts of data. Backing up corporate files is an important fibre channel application. Fewer overhead bits for tasks such as error control and addressing are included in the fibre channel protocol, which uses a device's input/output interface to communicate directly with switches. Enterprise system connection (ESCON) is another storage-oriented protocol.
- *MPLS (multiprotocol label switching)* is used in switches and routers to speed up networks and provide type-of-service instructions. Bits representing the address are placed in the router's short-term cache memory. In MPLS, short, fixed-length "labels" tell the router how to route each packet so that the router does not have to examine the entire header of each packet after the first point in the carrier's network. The router merely looks at the label in its short-term memory for routing instructions. Multiprotocol label switching also provides networks with the capability to treat packets differently if they are voice or video packets. For example, voice and video can have tags that classify them with higher a priority than data bits.

Carrier and Internet Service Provider Networks

Customers access the network edge via cellular devices, cable modems, DSL, or plain old telephones. The network edge, the point where customer lines are connected to carriers' networks, sends traffic to the network core. Major carriers have backbone networks over which their greatest concentration of voice, data, and video traffic travels. Backbone networks consist of fiber-optic cabling connected by high-speed routers and switches. Carriers' backbone networks span multiple states. Incumbent telephone companies such as SBC carry high concentrations of traffic in metropolitan area backbones, within large cities, and between suburban and rural locales.

Carrier backbone networks are starting to look more alike. Carriers such as cellular providers and former Bell telephone companies that in earlier decades supported a higher percentage of voice services relied on voice switches and T-1 and T-3 lines. They had separate networks for data services. Much of the equipment suited mostly for voice is still in place, but carriers are planning and starting to implement converged, unified networks appropriate for data as well as voice.

Convergence is occurring at a faster pace in the core rather than at the edge. This is because more services are needed at the edge such as billing and prioritizing traffic, which tend to make edge devices more complex, requiring more features. In core or backbone devices, speed, reliability, and brute strength are needed. In addition, there are more edge devices, so the cost to upgrade the edge is higher. There is more equipment to upgrade and more features to program at the edge.

Reliability, quality of service, and security in public networks have always been important for public safety and emergency communications. However, terrorist threats, added vulnerability to hackers and worms, and more critical applications from enterprise, government, and healthcare institutions have heightened these concerns and raised the bar on performance. Carriers need to carry more types of traffic faster.

Enterprise and residential customers have used the Internet and various data networks for years. However, customers are adding more critical applications to networks, and additional residential customers are using broadband access. Networks need to scale, grow larger to accommodate this growth.

An added pressure carriers are facing is price competition. To keep their own costs low and stay price competitive, they are looking at operating one network for voice, frame relay, and data instead of multiple networks. The thought is that one network costs less to build and support than two or three networks. For carriers, keeping costs low and reliability high is a vital challenge. In particular, if the one network crashes, all customers lose all services on the carrier's network.

Vendors that sell edge and core routers include Juniper Networks, Cisco Systems, and Avici Systems.

MINIMIZING RISKS WHEN ADOPTING NEW TECHNOLOGY

Availability and reliability are key selection criteria for carriers when they purchase equipment. Carriers that upgrade networks to take advantage of new technology need to determine how these systems will perform and the viability of manufacturers that supply them.

Reliability refers to how often a device operates without failing. Carriers typically require NEBS Level 3 compliance on equipment they purchase. NEBS stands for Network Equipment Building System. Bellcore, (now Telcordia) the former R&D arm of the Regional Bell Operating Companies, developed NEBS standards. The standards include compliance with thermal, electrical, redundancy, and earthquake-resistance tests. Carriers often test reliability in their own labs by subjecting vendor equipment to fire, water, and other conditions to see how the equipment stands up.

In evaluating vendor performance, some carriers check whether vendors are TL9000 certified. TL9000 is a way to audit vendor processes. It includes ISO 9001, an international standard for internal quality management, plus other measurements specifically for telecommunications suppliers. For example, TL9000 looks at the formal process a vendor has in place for corrective action if equipment it manufactures fails. TL9000 metrics apply to hardware, software, and service providers.

Availability refers to how long it takes to repair equipment, or having the equipment in service even though part of it is not working. For example, if ports are inoperable, the other ports should be available to route calls normally handled by the inoperable ports. In the same vein, backup central processing units (CPUs) should be able to automatically take over if the main CPU goes down.

Core Routing— In Carrier Networks . . . Speed, Reliability, and Capacity

Requirements for routers built for carriers are more complex than for routers built for enterprise customers. Routers made primarily for carriers need higher reliability, scal-

ability, and security than those built primarily for enterprises. All routers hold network addresses (prefixes) in their routing tables. Whereas enterprise routers may have thousands of addresses, carrier routers often hold 250,000 Internet protocol (IP) addresses for customers worldwide. Core routers require complex memory to store so many network addresses. In addition, they tend to be larger, with multiple cabinets (chassis) seamlessly connected to each other and operating as a single router.

Routers geared to the carrier market often operate at *terabit* speeds, trillions of bits per second (1,000,000,000,000). The switching fabric is often made up of super computing platforms with hundreds of routers in a single device. If any one of the computers associated with a router fails, the router still functions and uses the input/output ports associated with the remaining computers.

Individual ports, each supporting one connection, often operate at OC-192, which equals 10,000 million bits per second (10 gigabits per second). Juniper Network has plans to introduce routers that support OC-768, 40 billion bits per second (40 gigabits) ports.

Juniper Network core routers are based on application-specific integrated circuit (ASIC) processors for high performance. ASICs are specialized chips built with the capability of many chips integrated within them. Advances in computers, such as memory and connectors, have benefited routers that need to check addresses and forward packets at consistently high speeds.

Implications of More Voice and Video

With more voice and video now on carriers' backbones, routers are required to differentiate between different types of traffic. They do this via protocols such as multiprotocol label switching (MPLS). There is also development and interoperability with asynchronous transfer mode (ATM) traffic. This enables IP networks to carry this traffic while preserving quality of service specified in ATM for traffic such as voice and video. (See Chapter 6 for information on ATM.)

Carrying voice and video has implications on reliability and speed. To ensure reliability and speed, Cisco is introducing a router based on a massively parallel computer and chips with 188 32-bit processors. All of these requirements plus the need to meet stringent reliability and redundancy specifications in the event of disasters such as fire and earthquakes result in higher router prices. The large research and development investments needed to support these efforts also add to higher per-port costs compared to routers made for the enterprise market.

Carrier Edge Routers—Security, Billing, and Filtering

Edge routers connect enterprises to carriers' networks. They are located at the edge of carrier networks. Edge routers aggregate large numbers of relatively slow circuits from end users at T-1 (1.54 megabits per second), T-3 (44 megabits per second), and OC-3 (155 megabits per second) speeds and send them to core routers at higher speeds of OC-12 (622 megabits), OC-48 (2.5 gigabits), and OC-192 (10 gigabits). See Figure 1.7. Connections between core and edge routers are hierarchical in nature, similar to connections between Layer 2 and Layer 3 switches in LANs.

Edge Routers—Slower, More Services Provided

Edge routers are slower than core routers. They also provide more services because they connect directly to customers as opposed to core routers that transmit to other

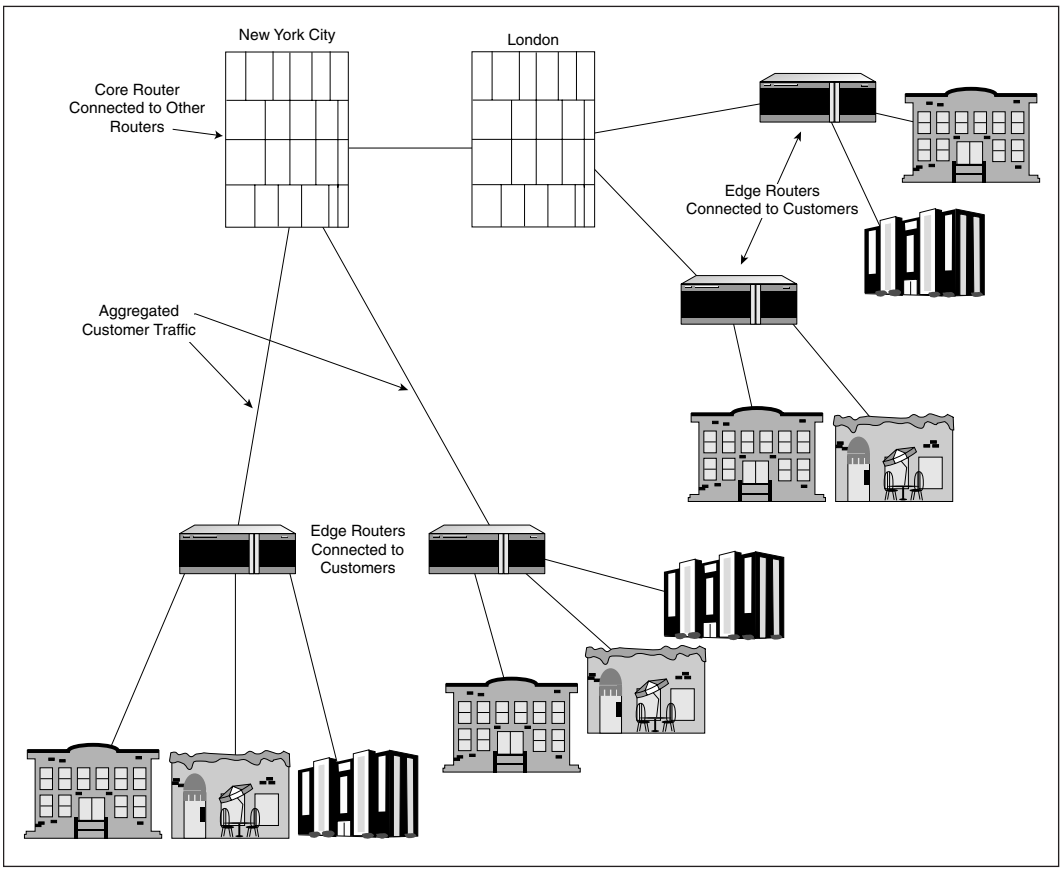


Figure 1.7
Edge and core routers.

core routers and to edge routers. Edge routers furnish services such as filtering, billing, VPN service, rate limiting, and traffic shaping.

- *Filters* are used to block traffic to sites such as those that are pornographic, music peering, or possibly personal shopping related for enterprises that don't want their employees to use the Internet for personal use.
- Rate limiting enables carriers to equip their routers with T-3, 44.5-megabit ports but to sell services of more than 44.5 megabits because it assumes that not everyone will use the service to its full capacity. To illustrate, it might sell 36 T-1s, which equals 55.44 megabits (36×1.54), 10.9 megabits more than the port's capacity of 44.5 megabits.
- VPN service furnishes security and remote access to enterprise customers. (See Chapter 5 for VPNs.)
- *Traffic classification* enables routers to distinguish between voice and data. This enables voice to be prioritized so that people don't hear delays, which impairs the quality of their calls.

Security—The Biggest Challenge

Security is the biggest challenge for edge routers. Edge routers block spam and monitor networks to keep them free from attacks. Routers keep lists that need frequent updates of sites used to launch attacks against carriers' networks. They can shut off residential customers who unknowingly download a worm and can send the customers to an Internet site that explains what has occurred and how to fix their computer so that it does not infect the carrier's network.

APPENDIX

Table 1.3 *Appendix: Compression Standards and Their Descriptions*

Compression Standard	Description
MNP 5	Microcom Network Protocol compression protocol developed by Microcom for modems. Provides 2:1 compression.
V.42bis	Data compression protocol for modems. Provides 4:1 compression.

Table 1.3 *Appendix: Compression Standards and Their Descriptions (continued)*

Compression Standard	Description
H.320	A family of standards for video adopted by the ITU (International Telecommunications Union). Quality is not as high as proprietary video compression algorithms. Most video codecs employ both proprietary and standard compression algorithms. The proprietary compression is used to transmit to another "like" video units, and the standard algorithm is used when conferencing between differing brands.
H.323	A family of standards for video adopted by the ITU for sending video over packet networks. Microsoft Corporation and Intel Corporation adopted the standard in 1996 for sending voice over packet networks. It is installed on Windows-based PCs and is used to packetize and compress voice when callers with PCs make calls from their computers over the Internet. See Chapter 5.
G.726	A family of standards for video adopted by the ITU (International Telecommunications Union). Quality is not as high as proprietary video compression algorithms. Most video codecs employ both proprietary and standard compression algorithms. The proprietary compression is used to transmit to another "like" video units, and the standard algorithm is used when conferencing between differing brands.
IBOC	In-band on-channel broadcasting uses airwaves within the current AM and FM spectrum to broadcast digital programming. IBOC is based on the Perceptual Audio Coder (PAC). There are many sounds that the ear cannot discern because they are masked by louder sounds. PAC discerns and discards these sounds that the ear cannot hear and that are not necessary to retain the quality of the transmission. This results in transmission with 15 times fewer bits. PAC, the Perceptual Audio Coder, was first developed at Bell Labs in the 1930s.
JPEG	Joint Photographic Experts Group is a compression standard used mainly for photographs. The International Standards Organizations (ISO) and the International Telecommunications Union (ITU) developed JPEG.

Table 1.3 *Appendix: Compression Standards and Their Descriptions (continued)*

Compression Standard	Description
MPEG-2	A Moving Picture Experts Group standard approved in 1993 for coding and decoding video and television images. MPEG2 uses past images to predict future images and color, and it transmits only the changed image. For example, the first in a series of frames is sent in a compressed form. The ensuing frames send only the changes. A frame is a group of bits representing a portion of a picture, text, or audio section.
MPEG-3	Moving Picture Experts Group 3 is Layer 3 of MPEG1. MPEG-3, also referred to as MP3, is a compression standard for streaming audio. MPEG3 is the compression algorithm used to download audio files from the Internet. For example, some Internet e-commerce sites allow people with compression software to download samples of music so that they can decide if they want to purchase a particular CD.
MPEG-4	Moving Picture Experts Group 4 is a standard used mainly for streaming and downloading compressed video and television. It is four times more efficient than MPEG-2.

Table 1.4 *Appendix: OSI Layers*

OSI Layer Name and Number	Layer Function
Layer 1: Physical Layer	*Layer 1* is the most basic layer. Layer 1 defines the type of media—for example, copper, wireless, or fiber optics and how devices access media. Repeaters used to extend signals over fiber, wireless, and copper are Layer 1 devices. Repeaters in cellular networks extend and boost signals inside buildings and in subways so that people can use their cellular devices in these locations. In tall buildings, antennas on rooftops transmit signals over fiber or copper to small repeaters with antennas on each floor.

Table 1.4 Appendix: OSI Layers (continued)

OSI Layer Name and Number	Layer Function
Layer 2: Data Link Layer	Ethernet, also known as 802.3, is a *Layer 2* protocol. It provides rules for error correction and access to LANs. Layer 2 devices have addressing information analogous to social security numbers. They are random but specific to individuals. Frame relay is a Layer 2 protocol used to access carrier networks from enterprises.
Layer 3: Network Layer	*Layer 3* is known as the routing layer. It is responsible for routing traffic between networks using IP (Internet protocol) network addresses, and it has error-control functions. Layer 3 is analogous to a local post office routing an out-of-town letter by ZIP code, not looking at the street address. Once an e-mail message is received at the distant network, a Layer 2 device looks at the address and delivers the message.
Layer 4: Transport Layer	*Layer 4* protocols enable networks to differentiate between types of content. Layer 4 devices route by content. They are also known as content switches. For example, video or voice transmissions over data networks might receive a higher priority or quality of service than e-mail, which can tolerate delay. TCP (transmission control protocol) is a Layer 4 protocol. Filters in routers that check for computer viruses by looking at additional bits in packets perform a Layer 4 function.
Layer 5: Session Layer	*Layer 5* manages the actual dialog of sessions. Encryption that scrambles signals to ensure privacy occurs in Layer 5. H.323 is a Layer 5 protocol that sends signals in packet networks to set up and tear down, for example, video and audio conferences.
Layer 6: Presentation Layer	*Layer 6* controls the format or how the information looks on the user's screen. Hypertext Markup Language (HTML) used to format Web pages and some e-mail messages is a Layer 6 standard.

Table 1.4 Appendix: OSI Layers (continued)

OSI Layer Name and Number	Layer Function
Layer 7: Application Layer	*Layer 7* includes the application itself plus specialized services such as file transfers or print services. Hypertext transfer protocol (HTTP) is a Layer 7 protocol.

Table 1.5 Appendix: LAN, MAN, and WAN Terms and Devices

LANs, MANs, WANs, and More	Definition
LAN (local area network)	A group of devices, such as computers, printers, and scanners, that can communicate with each other within a limited geographic area such as a floor, department, or small cluster of buildings.
MAN (metropolitan area network)	Networks that can communicate with each other within a city or a large campus area covering many city blocks.
WAN (wide area network)	A group of data devices, usually LANs, that communicate with each other between multiple cities.
Hub	The wiring center to which all devices, printers, scanners, PCs, and so forth are connected within a segment of a LAN. Hubs enable LANs to be connected to twisted pair cabling instead of coaxial cable. Only one device at a time can transmit via a hub. Higher-speed switches have replaced hubs in most organizations.
Backbone	Wiring running from floor to floor in single buildings and from building to building within campuses. A backbone connects switches in different wiring closets to each other. Backbones support high concentrations of traffic in carrier and enterprise networks.
Bridge	Bridges usually connect LANs using the same type of protocol together. They have limited intelligence and generally only connect a few LANs together. Bridges were in limited use as of the early 1990s when the price of routers dropped.

Table 1.5 *Appendix: LAN, MAN, and WAN Terms and Devices (continued)*

LANs, MANs, WANs, and More	Definition
Layer 2 switch (also called switching hub)	Layer 2 switches, located in wiring closets, are bridges that allow multiple simultaneous transmissions within a single LAN. Layer 2 switches provide a dedicated connection during an entire transmission.
Layer 3 switch (also known as routing switch)	Layer 3 switches have the capability to route traffic across the LAN backbone. They are more complex to manage than Layer 2 switches, but they can use alternate paths if one path is out of service. They are located in data centers and link wiring closets and buildings within a campus.
Layer 4 switch (also known as content switches)	Layer 4 switches are located at hosting sites and corporate and government sites that host their own Web pages. Layer 4 switches connect Web traffic to the desired Web pages by looking at the universal resource locator (URL), the Web address from which each packet was transferred to their site.
Router	Routers carry traffic between LANs, from enterprises to the Internet, and across the Internet. They are more complex than switches because they have routing tables with addresses and perform other functions. Routers select the best available path over which to send data.
Server	A centrally located computer with common departmental or organizational files such as personnel records, e-mails, sales data, price lists, student information, and medical records. Servers are connected to Layer 2 or 3 switches. Access to servers can be restricted to authorized users only.
VLAN (virtual local area network)	A virtual local area network is made up of devices, usually personal computers or Voice over IP devices, whose addresses are programmed as a group in Layer 2 switches. This segregates them from the rest of the corporate network so that all devices in the same VLAN can be give a higher priority or level of security. They are programmed as a separate LAN but are physically connected to the same switch as other devices.