CHAPTER 1

First Things First

Telecommunications, like all highly visible and interesting fields, is full of apocryphal stories, technical myths, and fascinating legends. Everyone in the field seems to know someone who knows the outside plant repair person who found the poisonous snake in the equipment box in the manhole[1], the person who was on the cable-laying ship when they pulled up the cable that had been bitten through by some species of deep water shark, some collection of seriously evil hackers, or the backhoe driver who cut the cable that put Los Angeles off the air for 12 hours.

There is also a collection of techno-jargon that pervades the telecommnications industry and often gets in the way of the relatively straightforward task of learning how all this stuff actually works. To ensure that such things don't get in the way of absorbing what's in this book, I'd like to begin with a discussion of some of them.

This is a book about telecommunications, which is the science of communicating over distance (tēle-, from the Greek tēle, "far off"). It is, however, fundamentally dependent upon *data communications,* the science of moving traffic between computing devices so that the traffic can be manipulated in some way to make it useful. Data, in and of itself, is not particularly useful, consisting as it does of a stream of ones and zeroes that is only meaningful to the computing device that will receive and manipulate those ones and zeroes. The data does not really become useful until it is converted by some application into *information*, because a human can generally understand information. The human then acts upon the information using a series of intuitive processes that further convert the information into *knowledge*, at which point it becomes truly useful. Here's an example: A computer generates a steady stream of ones and zeroes in response to a series of business activities involving the computer that generates the ones and zeroes. Those ones and zeroes are fed into another computer, where an application converts them into a spreadsheet of sales figures (information) for the store from which they originated. A financial analyst studies the spreadsheet, calculates a few ratios, examines some historical data (including not only sales numbers but demographics, weather patterns, and political trends), and makes an informed prediction about future stocking requirements and advertising focal points for the store based on the knowledge that the analyst was able to create from the distilled information.

Data communications rely on a carefully designed set of rules that governs the manner in which computers exchange data. These rules are called *protocols*, and they are centrally important to the study of data

[1]I realize that this term has fallen out of favor today, but I use it here for historical accuracy.

First Things First

communications. Dictionaries define protocol as "a code of correct conduct." From the perspective of data communications, they define it as "a standard procedure for regulating the transmission of data between computers," which is itself "a code of correct conduct." These protocols, which will be discussed in detail later in this book, provide a widely accepted methodology for everything from the pin assignments on physical connectors to the sublime encoding techniques used in secure transmission systems. Simply put, they represent the many rule sets that govern the game. Many countries play football, for example, but the rules are all slightly different. In the United States, players are required to weigh more than a car, yet be able to run faster than one. In Australian Rules football, the game is declared forfeit if it fails to produce at least one body part amputation on the field or if at least one player doesn't eat another. They are both football, however. In data communications, the problem is similar; there are many protocols out there that accomplish the same thing. Data, for example, can be transmitted from one side of the world to the other in a variety of ways including T1, E1, microwave, optical fiber, satellite, coaxial cable, and even through the water. The end result is identical: the data arrives at its intended destination. Different protocols, however, govern the process in each case.

A discussion of protocols would be incomplete without a simultaneous discussion of *standards*. If protocols are the various sets of rules by which the game is played, standards govern which set of rules will be applied for a particular game. For example, let's assume that we need to move traffic between a PC and a printer. We agree that in order for the PC to be able to transmit a printable file to the printer, both sides must agree on a common representation for the zeroes and ones that make up the transmitted data. They agree, for example (and this is *only* an example) that they will both rely on a protocol that represents a zero as the absence of voltage and a one as the presence of a three-volt pulse on the line, as shown in Figure 1-1. Because they agree on the representation, the printer knows when the PC is sending a one and when the PC is sending a zero. Imagine what would happen if they failed to agree on such a simple thing beforehand. If the transmitting PC decides to represent a one as a 300-volt pulse and the printer is expecting a three-volt

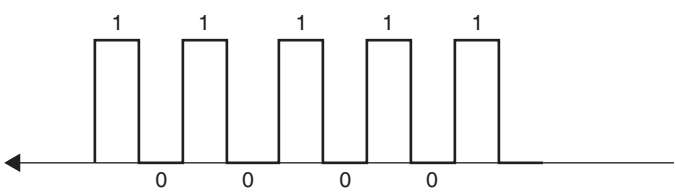


Figure 1-1 Voltage representations of data.

pulse, the two devices will have a brief (but inspired) conversation, the ultimate result of which will be the release of a small puff of silicon smoke from the printer.

Now they have to decide on a standard that they will use for actually originating and terminating the data that they will exchange. They are connected by a cable (see Figure 1-2) that has nine pins on one end and nine jacks on the other. Logically, the internal wiring of the cable would look like Figure 1-3. However, when we stop to think about it, this one-to-one correspondence of pin-to-socket will not work. If the PC transmits on pin 2, which in our example is identified as the send data lead, it will arrive at the printer on pin 2—the send data lead. This would be analogous to holding two telephone handsets together so that two communicating parties can talk. It won't work without a great deal of hollering. Instead, some agreement has to be forged to ensure that the traffic placed on the send-data lead somehow arrives on the receive data lead and vice versa. Similarly, the other leads must be able to convey information to the other end so that normal transmission can be started and stopped. For example, if the printer is ready to receive the print file, it might put voltage on the *data terminal ready* (DTR) lead, which signals to the PC that it is ready to receive traffic. The PC might respond by setting its own DTR lead high as a form of acknowledgment, followed by

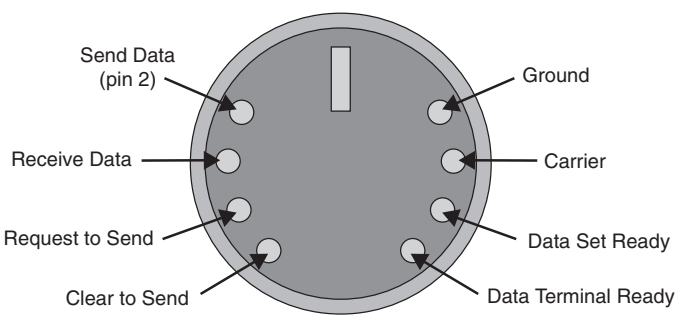


Figure 1-2 Pin assignments on a cable connector.

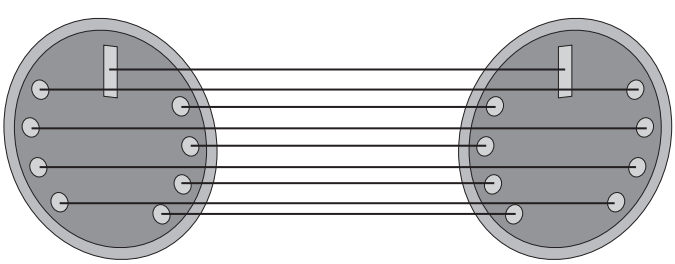


Figure 1-3 Logical wiring scheme.

transmission of the file that is to be printed. The printer will keep its DTR lead high until it wants the PC to stop sending. For example, if the printer senses that it is running out of buffer space because the PC is transmitting faster than the slower printer can print, it will drop the DTR lead, causing the PC to temporarily halt its transmission of the print file. As soon as the printer is ready to receive again, it sets the DTR lead high once again, and printing resumes. As long as both the transmitter and the receiver abide by this standard set of rules, data communications will work properly. This process of swapping the data on the various leads of a cable, incidentally, is done by the modem—or by a null modem cable that makes the communicating devices think they are talking to a modem. The null modem cable is wired so that the send-data lead on one end is connected to the receive data lead on the other end and vice-versa; similarly, a number of control leads such as the carrier detect lead, the DTR lead, and the *data set ready* (DSR) leads are wired together so that they give false indications to each other to indicate that they are ready to proceed with the transmission, when in fact no response from the far end modem has been received.

Standards: Where Do They Come From?

Physicists, electrical engineers, and computer scientists generally design data communications protocols. For example, the *Transmission Control Protocol* (TCP) and the *Internet Protocol* (IP) were written during the heady days of the Internet back in the 1960s by such early pioneers as Vinton Cerf and the late John Postel. (I want to say "back in the last century" to make them seem like *real* pioneers.) Standards, on the other hand, are created as the result of a consensus-building process that can take years to complete. By design, standards must meet the requirements of the entire data and telecommunications industry, which is of course global. It makes sense, therefore, that some international body is responsible for overseeing the creation of international standards. One such body is the United Nations. Its 150 plus member nations work together in an attempt to harmonize whatever differences they have at various levels of interaction, one of which is international telecommunications. The *International Telecommunications Union* (ITU), a suborganization of the UN, is responsible for not only coordinating the

creation of worldwide standards but also publishing them under the auspices of its own sub-organizations. These include the *Telecommunications Standardization Sector* (TSS, sometimes called the ITU-T, and formerly the *Consultative Committee on International Telegraphy and Telephony*, the CCITT), the *Telecommunications Development Sector* (TDS), and the *Radio Communication Sector* (RCS, formerly the *Consultative Committee on International Radio*, the CCIR). The organizational structure is shown in Figure 1-4.

Of course, the UN and its sub-organizations cannot perform this task alone, nor should they. Instead, they rely upon the input of hundreds of industry-specific organizations as well as local, regional, national, and international standards bodies that feed information, perspectives, observations, and technical direction to the ITU, which serves as the coordination entity for the overall international standards creation process. These include the *American National Standards Institute* (ANSI), the *European Telecommunications Standards Institute* (ETSI, formerly the *Conference on European Post and Telegraph*, CEPT), Telcordia (formerly Bellcore, now part of SAIC), the *International Electrotechnical Commission* (IEC), the *European Computer Manufacturers Association* (ECMA), and a host of others.

It is worthwhile to mention a bit about the ITU as a representative standards body. Founded in 1947 as part of the United Nations, it descended from a much older body called the Union Telegraphique, founded in 1865 and chartered to develop standards for the emerging telegraph industry. Over the years since its creation, the ITU and its three principal member bodies have developed three principal goals:

- To maintain and extend international cooperation for the improvement and interconnectivity of equipment and systems through the establishment of technical standards.

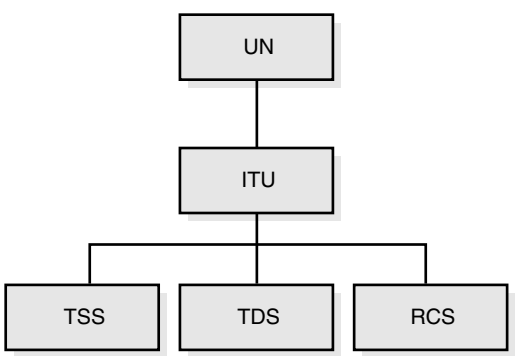


Figure 1-4
The ITU organizational structure.

- To promote the development of the technical and natural facilities (read spectrum) for most efficient applications.
- To harmonize the actions of national standards bodies to attain these common aims, and most especially to encourage the development of communications facilities in developing countries.

The Telecommunications Standardization Sector

The goals of the TSS, according to the ITU, are as follows:

- To fulfill the purposes of the union relating to telecommunication standardization by studying technical, operating, and tariff questions and adopting formal recommendations on them with a view to standardizing telecommunications on a worldwide basis.
- To maintain and strengthen its pre-eminence in international standardization by developing recommendations rapidly.
- To develop recommendations that acknowledge market and trade-related considerations.
- To play a leading role in the promotion of cooperation among international and regional standardization organizations and forums and consortia concerned with telecommunications.
- To address critical issues that relate to changes due to competition, tariff principles, and accounting practices.
- To develop recommendations for new technologies and applications such as appropriate aspects of the GII and Global multimedia and mobility.

The Telecommunications Standardization Bureau

The Telecommunication Standardization Bureau provides secretarial support for the work of the ITU-T Sector and services for the participants in ITU-T work, diffuses information on international telecommunications

worldwide, and establishes agreements with many international standards development organizations. These functions include:

- **Study group management** The management team of the study groups is composed of the chairman, vice-chairmen of the study group, chairmen of the working parties, and the TSB counselor/engineer.
- **Secretarial support and meeting organization** TSB provides secretariat services for ITU-T assemblies and study group meetings. TSB counselors and engineers coordinate the work of their study group meetings, and their assistants ensure the flow of meeting document production.
- **Logistics services** The TSB provides services, such as meeting room allocation, registration of participants, document distribution, and facilities for meeting participants.
- **Approval of recommendations and other texts** The TSB organizes and coordinates the approval process of recommendations.
- **Access to ITU-T documents for ITU-T members** The TSB organizes and controls the dispatch of documents in paper form to participants in ITU-T work and provides *Electronic Document Handling* services (EDH) that enable easy and rapid exchange of documents, information, and ideas among ITU-T participants in order to facilitate the work of standards development. The ITU-T participants can have electronic access, via TIES, to study group documents such as reports, contributions, delayed contributions, temporary and liaison documents, and so on.

The TSB also provides the following services:

- Maintenance of the ITU-T Website and distribution of information about the activities of the sector including the schedule of meetings, TSB circulars, collective letters, and all working documents.
- Update services for the list of ITU-T recommendations, the ITU-T work programmer database, the ITU-T patent statements database, and the ITU-T terms and definitions database Sector Abbreviations and Definitions for a Telecommunications Thesaurus-Oriented Database (SANCHO), as well as update services for other databases as required.
- Country code number assignment for telephone, data, and other services.
- Registrar services for *Universal International Freephone Numbers* (UIFN).

- Technical information on international telecommunications and collaborates closely with the ITU radio communication sector and with the ITU telecommunication development sector for matters of interest to developing countries.
- Provides administrative and operational information through the ITU *Operational Bulletin*.
- Coordinates the editing, publication, and posting of the recommendations.

The Radio Bureau

The functions of the radio bureau include:

- Administrative and technical support to radio communication conferences, radio communication assemblies and study groups, including working parties and task groups.
- Application of the provisions of the Radio Regulations and various regional agreements.
- Recording and registration of frequency assignments and also orbital characteristics of space services and maintenance of the master international frequency register.
- Consulting services to member states on the equitable, effective, and economical use of the radio-frequency spectrum and satellite orbits, and investigates and assists in resolving cases of harmful interference.
- Preparation, editing, and dispatch of circulars, documents, and publications developed within the sector.
- Delivers technical information and seminars on national frequency management and radio communications, and works closely with the telecommunication development bureau to assist developing countries.

The Standards

A word about the publications of the ITU. First of all, they are referred to as *recommendations* because the ITU has no enforcement authority over the member nations that use them. Its strongest influence is exactly that—the ability to *influence* its member telecommunications authorities to use the standards because it makes sense to do so on a global basis.

The standards are published every four years, following enormous effort on the part of the representatives that sit on the organization's task forces. These representatives hail from all corners of the industry; most countries designate their national telecommunications company (where they still exist) as the representative to the ITU-T, while others designate an alternate, known as a *Recognized Private Operating Agency* (RPOA). The United States, for example, has designated the Department of State as its duly elected representative body. Other representatives may include manufacturers (Lucent, Cisco, Nortel, and Fujitsu), research and development organizations (Bell Northern Research, Bell Laboratories, and Xerox PARC), and other international standards bodies.

At any rate, the efforts of these organizations, companies, governments, and individuals result in the creation of a collection of new and revised standards recommendations published on a four-year cycle. Historically, the standards are color-coded, published in a series of large format soft-cover books, differently colored on a rotating basis. For example, the 1984 books were red; the 1988 books, blue; the 1992 books, white. It is common to hear network people talking about "going to the blue book." They are referring (typically) to the generic standards published by the ITU for that particular year. It is also common to hear people talk about the CCITT. Old habits die hard: The organization ceased to exist in the early 1990s, replaced by the ITU-T. The name is still commonly used, however.

The activities of the ITU-T are parceled out according to a cleverly constructed division of labor. Three efforts result: study groups, which create the actual recommendations for telecom equipment, systems, networks, and services (there are currently 15 study groups), plan committees, which develop plans for the intelligent deployment and evolution of networks and network services, and specialized autonomous groups (three currently) that produce resources that support the efforts of developing nations. The study groups are listed in the following:

- **SG 2** Operational aspects of service provision, networks, and performance
- **SG 3** Tariff and accounting principles, including related telecommunications economic and policy issues
- **SG 4** Telecommunication management, including TMN
- **SG 5** Protection against electromagnetic environment effects
- **SG 6** Outside plant
- **SG 7** Data networks and open system communications

- **SG 9** Integrated broadband cable networks and television and sound transmission
- **SG 10** Languages and general software aspects for telecommunication systems
- **SG 11** Signaling requirements and protocols
- **SG 12** End-to-end transmission performance of networks and terminals
- **SG 13** Multi-protocol and IP-based networks and their internetworking
- **SG 15** Optical and other transport networks
- **SG 16** Multimedia services, systems, and terminals
- **SSG** Special Study Group "IMT-2000 and beyond"

Structure of Standards Documents

The standards are published in a series of alphabetically arranged documents, available as books, online resources, and CDs. They are functionally arranged according to the alphabetical designator of the standard as follows:

A Organization of the work of ITU-T

B Means of expression: definitions, symbols, and classification

C General telecommunication statistics

D General tariff principles

E Overall network operation, telephone service, service operation, and human factors

F Non-telephone telecommunication services

G Transmission systems and media, digital systems, and networks

H Audiovisual and multimedia systems

I Integrated services digital network

J Transmission of television, sound programs, and other multimedia signals

K Protection against interference

L Construction, installation, and protection of cables and other elements of outside plant

M TMN and network maintenance: international transmission systems, telephone circuits, telegraphy, facsimile, and leased circuits

N Maintenance: international sound program and television transmission circuits

O Specifications of measuring equipment

P Telephone transmission quality, telephone installations, local line networks

Q Switching and signaling

R Telegraph transmission

S Telegraph services terminal equipment

T Terminals for telematic services

U Telegraph switching

V Data communication over the telephone network

X Data networks and open-system communication

Y Global information infrastructure and Internet protocol aspects

Z Languages and general software aspects for telecommunication systems

Within each letter designator can be found specific, numbered recommendations. For example, recommendation number 25 in the "X" book contains the specifications for transporting packet-based data across a public network operating in packet mode. This, of course, is the now-famous X.25 packet switching standard. Similarly, Q.931 provides the standard for signaling in ISDN networks, and so on. The documents are remarkably easy to read and contain vast amounts of information. I am always surprised to discover how many people who work in telecommunications have never read the ITU standards. Take this, then, as *my* recommendation: Find some of them and flip through them. They can be very useful.

I spent some time writing about the ITU and its standards activities simply to explain the vagaries of the process (one of my favorite telecom jokes goes like this: "There are two things you never want to watch being made. One of them is sausage; the other is standards.") and the role of these bodies. The ITU is representative of the manner in which all standards are developed, although the frequency of update, the cycle time, the relative levels of involvement of the various players, and the breadth of coverage of the documents vary dramatically.

The Network

For years now, communications networks have been functionally depicted as shown in Figure 1-5: a big, fluffy, opaque cloud, into which disappear lines representing circuits that magically reappear on the other side of the cloud. I'm not sure why we use clouds to represent networks; knowing what I know about their complex innards and how they work, a hairball would be a far more accurate representation.

In truth, clouds are pretty good representations of networks from the point of view of the customers that use them. Internally, networks are remarkably complex assemblages of hardware and software as you will see in the chapter on telephony. Functionally, however, they are straightforward: customer traffic goes into the network on the *Gozinta;* the traffic then emerges, unchanged, on the *Gozouta.* How it happens is unimportant to the customer; all they care about is that the network receives, interprets, transports, and delivers their voice/video/images/data/music to the destination in a correct, timely, and cost-effective fashion. Later in the book we will discuss the various technologies that live within the network, but for now suffice it to say that its responsibilities fall into two categories: access and transport, as illustrated in Figure 1-6.

Network Access

As the illustration shows, network access is exactly that: the collection of technologies that support connectivity between the customer and the

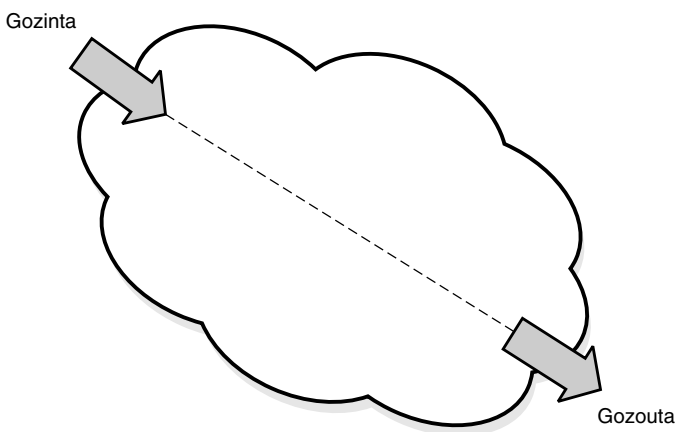


Figure 1-5 The network cloud.

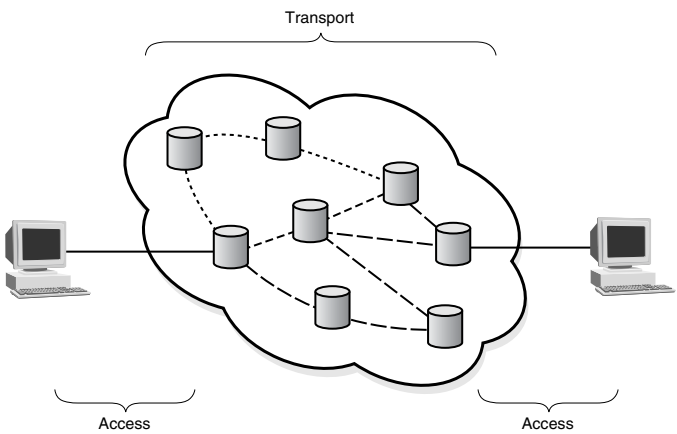


Figure 1-6 Access vs. transport regions of the network.

transport resources of the network. At its most common level, access is the local loop, the two-wire circuit that connects a customer's telephone to the local switch that provides telephony service to that customer. As the network has become more data-aware, other solutions have emerged that provide greater bandwidth as well as multiservice capability. ISDN, which uses the two-wire local loop, provides greater bandwidth than the traditional analog local loop through digitization and time-division multiplexing (both explained shortly). *Digital Subscriber Line*, or DSL, is also a local loop-based service, but offers even more diverse service than ISDN in the areas where it is available. Cable modem service, which does *not* use the telephony local loop, offers high downstream (toward the customer) bandwidth and smaller upstream (from the customer) capacity. Wireless services, including LMDS, MMDS, satellite, cellular, and others, represent another option for access connectivity. All of these will be discussed in greater detail later in the book.

Miscellaneous Additional Terms A number of other terms need to be introduced here as well, the first of which are *Data Terminal Equipment* (DTE) and *Data Circuit Terminating Equipment* (DCE). DTE is exactly that—it is the device that a user employs to gain access to the network. A DCE is the device that actually terminates the circuit at the customer's premises, typically a modem. One important point: because the bulk of the usage is over the *Public Switched Telephone Network* (PSTN), which is optimized for the transport of voice, the primary role of the DCE is to make the customer's DTE look and smell and taste and feel like a telephone to the network. For example, if the DTE is a PC, then

the modem's job is to collect the high-frequency digital signals being produced by the PC and modulate them into a range of frequencies that are acceptable to the bandwidth-limited voiceband of the telephone network. That's where the name comes from, incidentally—modulate/demodulate (mo-dem).

Another pair of terms that must be introduced here is *parallel* and *serial*. You have undoubtedly seen the ribbon cables that are used to transport data inside a PC, or the parallel wires etched into the motherboard inside the PC. These parallel conductors are called a *bus*, and are used for the high-speed transport of multiple simultaneous bits in parallel fashion from one device inside the computer to another. Serial transmission, on the other hand, is used for the single-file transport of multiple bits, one after the other, usually deployed *outside* a computer.

Finally, we offer *simplex, half-duplex,* and *full-duplex transmission.* Simplex transmission means one-way only, like a radio broadcast. Half-duplex transmission means two-way, but only one way at a time, like CB radio. Finally, full-duplex means two-way simultaneous transmission, like telephony or two-way data transmission.

Network Transport

The fabric of the network cloud is a rich and unbelievably complex collection of hardware and software that moves customer traffic from an ingress point to an egress point, essentially anywhere in the world. It's a function that we take entirely for granted because it is so ingrained in day-to-day life, but stop for a moment to think about what the network actually does. Not only does it deliver voice and data traffic between end points, but it does so easily and seamlessly, with various levels of service quality as required to any point on the globe (and in fact beyond) in a matter of seconds—and with *zero* human involvement. It is the largest fully automated machine on the planet and represents one of the greatest technological accomplishments of all time. Think about that: I can pick up a handset here in Vermont, dial a handful of numbers, and seconds later a telephone rings in Ouagadougou, Burkina Faso, in North Central Africa. How that happens borders on the miraculous. We will explore it in considerably greater detail later in the book.

Transport technologies within the network cloud fall into two categories: fixed transport and switched transport. Fixed transport, sometimes called private line or dedicated facilities, includes such technologies as T-1, E-1, DS-3, SONET, SDH, dedicated optical channels,

and microwave. Switched technologies include modem-based telephone transport, X.25 packet switching, frame relay, and *Asynchronous Transfer Mode* (ATM). Together with the access technologies described previously and customer premises technologies such as Ethernet, transport technologies offer the infrastructure components required to craft an end-to-end solution for the transport of customer information.

The Many Flavors of Transport

Over the last few years the network has been functionally segmented into a collection of loosely defined regions that define unique service types. These include the local area, the metropolitan area, and the wide area, sometimes known as the core. Local area networking has historically defined a network that provides services to an office, a building, or even a campus. Metro networks generally provide connectivity within a city, particularly to multiple physical locations of the same company. They are usually deployed across a ring architecture. Wide area networks, often called core, provide long distance transport and are typically deployed using a mesh networking model.

Transport Channels

The physical circuit over which the customer is transported in a network is often referred to as a *facility.* Facilities are characterized by a number of qualities such as distance, quality (signal level, noise, and distortion coefficients), and bandwidth. Distance is an important criterion because it places certain design limitations on the network, making it more expensive as the circuit length increases. Over distance, signals tend to weaken and become noisy, and specialized devices (amplifiers, repeaters, and regenerators) are required to periodically clean up the signal quality and maintain the proper level of loudness to ensure intelligibility and recognizability at the receiving end.

Quality is related to distance in the sense that they share many of the same affecting factors. Signal level is clearly important, as is noise, both of which were just discussed. Distortion is a slightly different beast and must be taken care of equally carefully. Noise is a random event in networks caused by lightning, fluorescent lights, electric motors, sunspot activity, and squirrels chewing on wires and is unpredictable and largely random. Noise, therefore, cannot be anticipated with any degree of accuracy; its effects can only be recovered from.

Distortion, on the other hand, is a measurable, unchanging characteristic of a transmission channel and is usually frequency-dependent. For example, certain frequencies transmitted over a particular channel will be weakened, or attenuated, more than other frequencies. If we can measure this, then we can condition the channel to equalize the treatment that all frequencies receive as they are transmitted down that channel. This process is indeed known as *conditioning* and is part of the higher cost involved in buying a dedicated circuit for data transmission.

Bandwidth is the last characteristic that we will discuss here, and the quest for more of it is one of the Holy Grails of telecommunications. Bandwidth is a measure of the number of bits that can be transmitted down a facility in any one-second period. In most cases it is a fixed characteristic of the facility and is the characteristic that most customers pay for. The measure of bandwidth is bits-per-second, although today the measure is more typically thousands (kilobits), millions (megabits) or billions (gigabits) per second.

Facilities are often called channels, because physical facilities are often used to carry multiple streams of user data through a process called *multiplexing*. Multiplexing is the process of enabling multiple users to share access to a transport facility either by taking turns or using separate frequencies within the channel. If the users take turns, as shown in Figure 1-7, the multiplexing process is known as *time division multiplexing* because time is the variable that determines when each user gets to transmit through the channel. If the users share the channel by occupying different frequencies, as shown in Figure 1-8, the process is called *frequency division multiplexing* because frequency is the variable that determines who can use the channel. It is often said that in time division multiplexing, users of the facility are given *all* of the

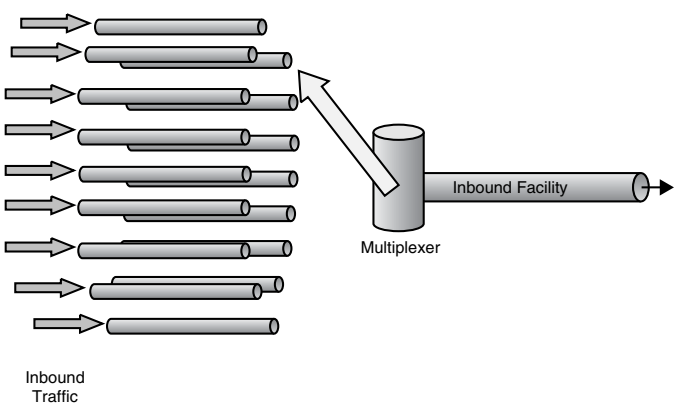


Figure 1-7
Time division multiplexing (TDM).

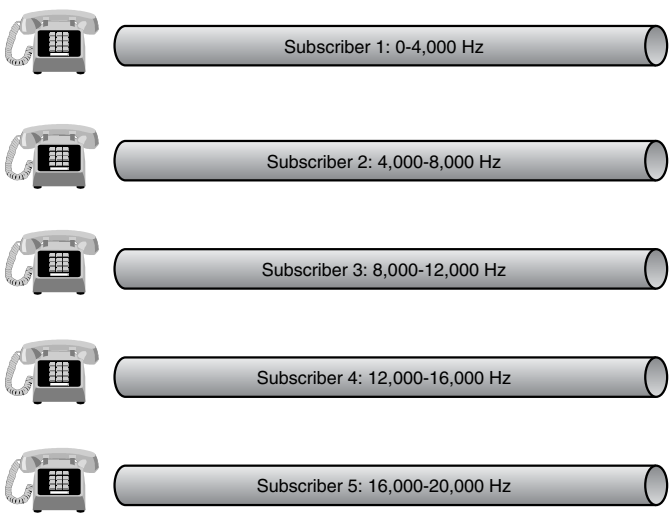


Figure 1-8 Frequency division multiplexing (FDM).

frequency *some* of the time, because they are the only ones using the channel during their timeslot. In frequency division multiplexing, users are given *some* of the frequency *all* of the time because they are the only ones using their particular frequency band at any point.

Analog versus Digital Signaling: Dispensing with Myths

Frequency division multiplexing is normally considered to be an *analog technology,* while time division multiplexing is a *digital technology.* The word *analog* means something that bears a similarity to something else, while the word *digital* means discrete. Analog data, for example, typically illustrated as some form of sine wave such as that shown in Figure 1-9, is an exact representation of the values of the data being transmitted. The process of using manipulated characteristics of a signal to represent data is called *signaling.*

We should also introduce a few terms here just to keep things marginally confusing. When speaking of signaling, the proper term for digital is *baseband,* while the term for analog signaling is *broadband.* When talking about data (not signaling), the term broadband means big channel.

The sine wave, undulating along in real time in response to changes in one or more parameters that control its shape, represents the exact value of each of those parameters at any point in time. The parameters are

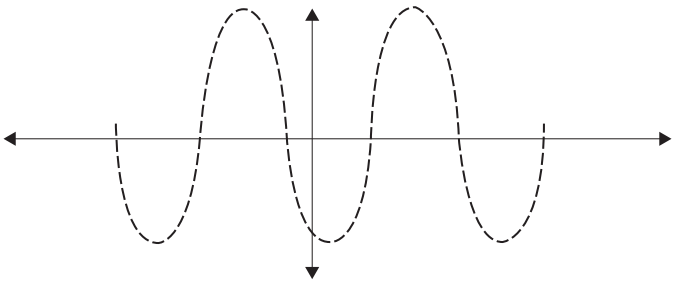


Figure 1-9
Sine wave.

amplitude, frequency, and phase. We will discuss each in turn. Before we do, though, let's relate analog waves to the geometry of a circle. Trust me—this helps.

Consider the diagram shown in Figure 1-10. As the circle rolls along the flat surface, the dot will trace the shape shown by the line. This shape is called a sine wave. If we examine this waveform carefully, we notice some interesting things about it. First of all, every time the circle completes a full revolution (360 degrees), it draws the shape shown in Figure 1-11. Thus halfway through its path, indicated by the zero point on the graph, the circle has passed through 180 degrees of travel. This makes sense, because a circle circumscribes 360 degrees.

The reason this is important is because we can manipulate the characteristics of the wave created in this fashion to cause it to carry varying amounts of information. Those characteristics, amplitude, frequency, and phase, can be manipulated as follows.

Amplitude Modulation

Amplitude is a measure of the loudness of a signal. A loud signal, such as that currently thumping through the ceiling of my office from my 16 year-old son's upstairs bedroom, has high-amplitude components, while lower volume signals are lower in amplitude. Examples are shown in Figure 1-12. The dashed line represents a high-amplitude signal, while the solid line represents a lower-amplitude signal. How could this be used in the data communications realm? Simple: Let's let high amplitude represent a digital zero, and low amplitude represent a digital one. If I then send four high amplitude waves followed by four low-amplitude waves, I have actually transmitted the series 00001111. This technique is called *amplitude modulation* (AM); modulation simply means "vary."

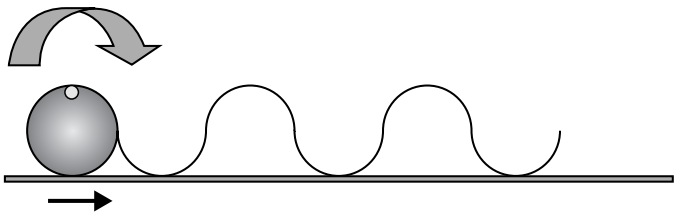


Figure 1-10
Creating a sine wave.

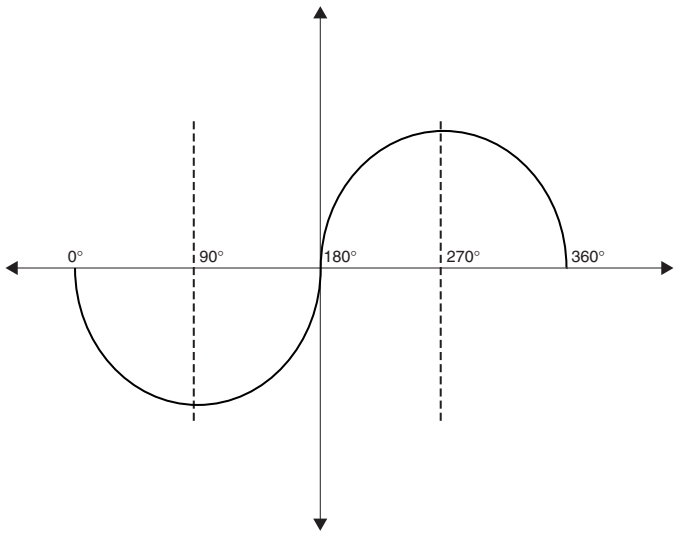


Figure 1-11
Sine wave.

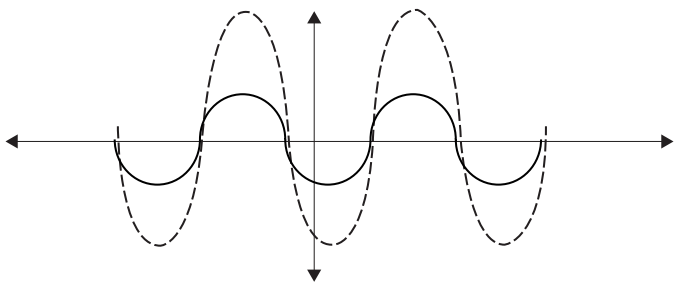


Figure 1-12
Amplitude modulation.

Frequency Modulation

Frequency modulation (FM) is similar to amplitude modulation, except that instead of changing the loudness of the signal, we change the number of signals that pass a point in a given second, illustrated in Fig-

ure 1-13. The left side of the graph contains a lower frequency signal component, while a higher frequency component appears to its right. We can use this technique in the same way we used AM: If we let a high-frequency component represent a zero, and a low-frequency component represent a one, then I can transmit our 00001111 series by transmitting four high-frequency signals followed by four low-frequency signals.

An interesting historical point about FM: The technique was invented by radio pioneer Edwin Armstrong in 1933. Armstrong, shown in Figure 1-14, created FM as a way to overcome the problem of noisy radio transmission. Prior to FM's arrival, AM was the only technique available and it relied on modulation of the loudness of the signal *and* the inherent noise to make it stronger. FM did not rely on amplitude, but rather on frequency modulation, and was therefore much cleaner and offered significantly higher fidelity than AM radio.

Many technical historians of World War II believe that Armstrong's invention of FM transmission played a pivotal role in the winning of the war. When WW II was in full swing, FM technology was only available to Allied forces. AM radio, the basis for most military

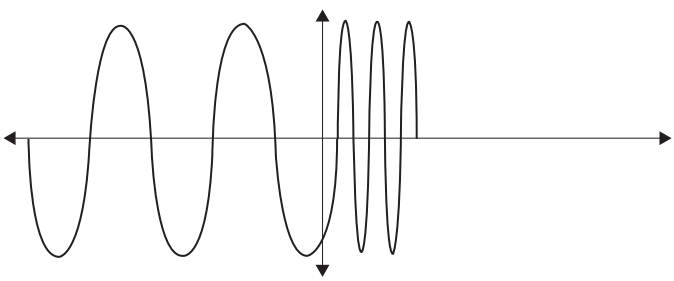


Figure 1-13 Frequency modulation.

Figure 1-14 Edwin Armstrong (photo courtesy Lucent Bell Laboratories).

communications at the time, could be jammed by simply transmitting a powerful signal that overloaded the transmissions of military radios. FM, however, was not available to the Axis powers and, therefore, could not be jammed as easily.

Phase Modulation

Phase modulation (PM) is a little more difficult to understand than the other two modulation techniques. Phase is defined mathematically as "the fraction of a complete cycle elapsed as measured from a particular reference point." Consider the drawing shown in Figure 1-15. The two waves shown in the diagram are exactly 90 degrees "out of phase" of each other because they do not share a common start point—wave B begins 90 degrees later than wave A. In the same way that we used amplitude and frequency to represent zeroes and ones, we can manipulate the phase of the wave to represent digital data.

Digital Signaling

Data can be transmitted in a digital fashion as well. Instead of a smoothly undulating wave crashing on the computer beach, we can use

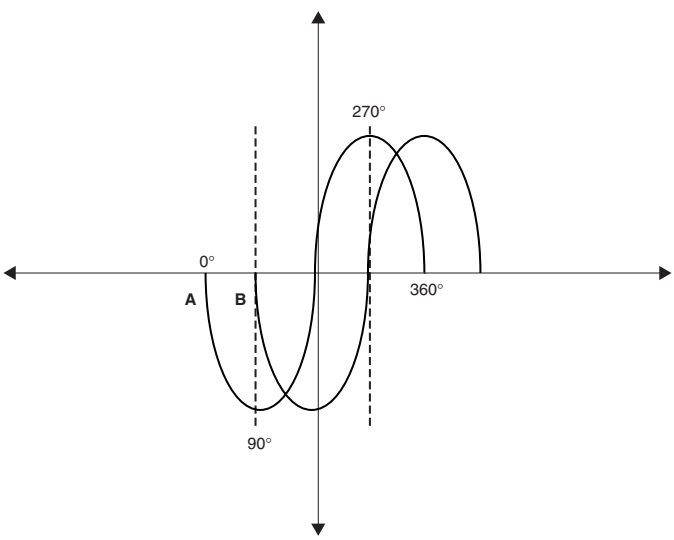


Figure 1-15 Phase modulation.

an approximation of the wave to represent the data. This technique is called *digital signaling*. In digital signaling, an interesting mathematical phenomenon, called the Fourier Series, is called into play to create what most people call a *square wave*, shown in Figure 1-16. In the case of digital signaling, the Fourier Series is used to approximate the square nature of the waveform. The details of how the series actually works are beyond the scope of this book, but suffice it to say that by mathematically combining the infinite series of odd harmonics of a fundamental wave, the ultimate result is a squared off shape that approximates the square wave that commonly depicts data transmission. This technique is called digital signaling, as opposed to the amplitude, frequency, and phase-dependent signaling techniques used in analog systems.

In digital signaling, zeroes and ones are represented as either the absence or presence of voltage on the line, and in some cases by either positive or negative voltage—or both. Figure 1-17, for example, shows a technique in which a zero is represented by the presence of positive voltage, while a one is represented as zero voltage. This is called a *unipolar signaling* scheme. Figure 1-18 shows a different technique, in which a zero is represented as positive voltage, while a one is represented as negative voltage. This is called a *non-return to zero signaling* scheme, because zero voltage has no value in this technique. Finally, Figure 1-19 demonstrates a bipolar system. In this technique, the presence of voltage represents a one, but notice that every other one is opposite in polarity from the one that preceded it and the one that follows it. Zeroes, meanwhile, are represented as zero voltage. This technique, called *Alternate Mark Inversion*, or AMI, is commonly used in T- and E-Carrier systems for reasons that will be discussed later.

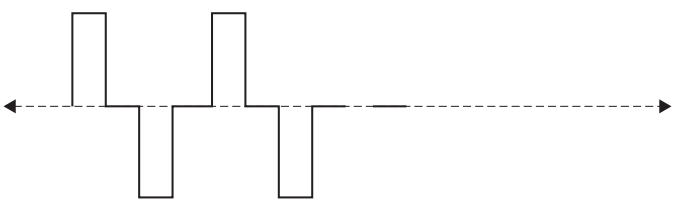


Figure 1-16
Square wave.

Figure 1-17
Unipolar signaling scheme.

Figure 1-18
Non-Return to Zero (NRZI) signaling scheme.

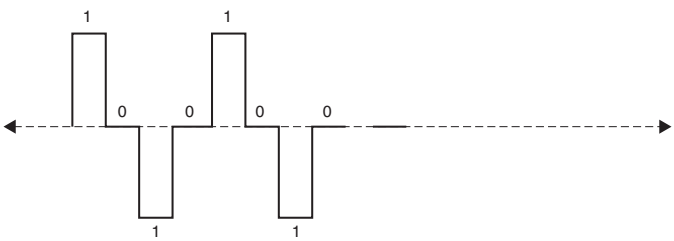


Figure 1-19
Bipolar signaling scheme.

There are other techniques in use, but these are among the most common.

Clearly, both analog and digital signaling schemes can be used to represent digital data depending upon the nature of the underlying transmission system. It is important to keep the difference between *data* and *signaling techniques* clearly separate. Data is the information that is being transported, and it can be either analog or digital in nature. For example, music is a purely analog signal because its values constantly vary over time. It can be represented, however, using either analog or digital signaling techniques. The zeroes and ones that spew forth from a computer are clearly digital information, but they too can be represented either analogically or digitally. For example, the broadband access technology known as *Digital Subscriber Line* (DSL) is not digital at all: there are analog modems at each end of the line, which means that *analog signaling techniques* are used to represent the *digital data* that is being transmitted over the local loop.

Combining Signaling Techniques for Higher Bit Rates

Let's assume that we are operating in an analog network. Under the standard rules of the analog road, one signaling event represents one bit. For example, a high-amplitude signal represents a one, and a low ampli-

tude signal represents a zero. But what happens if we want to increase our bit rate? One way is to simply signal faster. Unfortunately, the rules of physics limit the degree to which we can do that. In the 1920s, a senior researcher at Bell Laboratories who has now become something of a legend in the field of communications came to the realization that the bandwidth of the channel over which the information is being transmitted has a direct bearing on the speed at which signaling can be done across that channel. According to Harry Nyquist, the broader the channel, the faster the signaling rate can be. In fact, put another way, the signaling rate can never be faster than two times the highest frequency that a given channel can accommodate. Unfortunately, the telephone local loop was historically engineered to support the limited bandwidth requirements of voice transmission. The traditional voice network was engineered to deliver 4 kHz of bandwidth to each local loop[2], which means that the fastest signaling rate achievable over a telephony local loop is 8,000 baud. Yet during the late 1980s and the early 1990s, it was common to see advertisements for 9,600 baud modems. This is where the confusion of terms becomes obvious: as it turns out, these were *9,600 bit-per-second modems* —a big difference. This, however, introduces a whole new problem: How do we create higher bit rates over signal rate-limited (and therefore bandwidth limited) channels?

To achieve higher signaling rates, one of two things must be done: either broaden the channel, which is not always feasible, or figure out a way to have a single signaling event convey more than a single bit.

Consider the following example. We know from our earlier discussion that we can represent two bits by sending a high-amplitude signal followed by a low-amplitude signal (high-amplitude signal represents a zero, low- amplitude signal represents a one). What would happen, though, if we were to combine amplitude modulation with frequency modulation? Consider the four waveforms shown in Figure 1-20. By combining the two possible values of each characteristic (high and low frequency or amplitude), we create four possible states, each of which can actually represent two bits as shown in Figure 1-21. Consider what we have just done. We have created a system in which each signaling event represents two bits, which means that our bit rate is twice our signaling rate.

It's time to introduce a new word: *Baud*.

---

[2] One way in which this was done was through the use of load coils. Load coils are electrical traps that tune the local loop to a particular frequency range, only allowing certain frequencies to be carried. This created a problem later for digital technologies, as we will discuss.

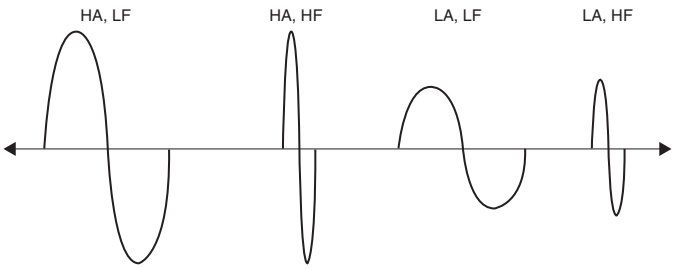


Figure 1-20
Di-bit encoding scheme.

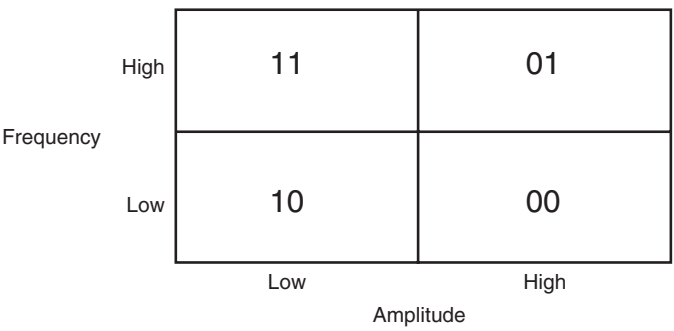


Figure 1-21
Di-bit values.

Baud is the signaling rate. It may or may not be the same as the bit rate, depending on the scheme being used.

Figure X shows a system in which we are encoding four bits for each signal, a technique known as *quad-bit encoding*. This scheme, sometimes called *Quadrature Amplitude Modulation*, or QAM (pronounced Kwăm), permits a single signal to represent four bits, which means that there is a 4:1 ratio between the bit rate and the signaling rate. Thus, it is possible to achieve higher bit rates in the bandwidth-limited telephony local loop by using multi-bit encoding techniques such as QAM. The first "high bit rate modems (9,600 bits-per-second) used this technique of a variation of it to overcome the design limitations of the network. In fact, these multi-bit schemes are also used by the cable industry to achieve the high bit rates they need to operate their multimedia broadband networks.

There is one other limitation that must be mentioned: noise. Look at Figure 1-22. Here we have a typical QAM graph, but now we have added noise, in the form of additional points on the graph that have no implied value. When a receiver sees them, however, how does it know which points are noise and which are data? Similarly, the oscilloscope trace shown in Figure 1-23 of a high-speed transmission would be difficult to interpret if there were noise spikes intermingled with the data. There is, therefore, a well-known relationship between the noise level in a circuit

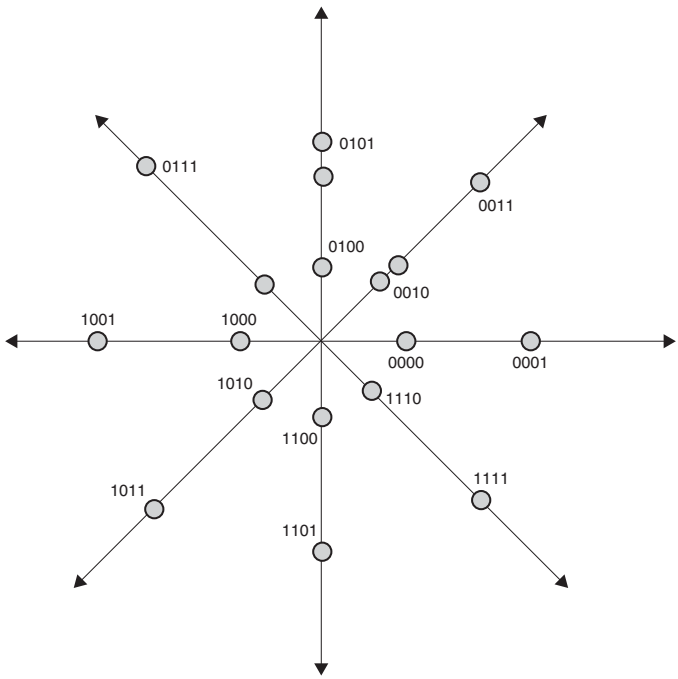


Figure 1-22
Quadrature amplitude modulation (QAM)

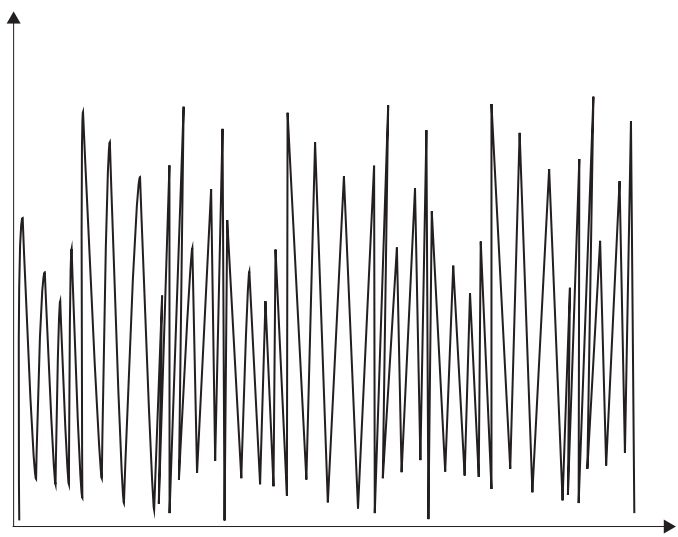


Figure 1-23
Oscilloscope trace.

and the maximum bit rate that is achievable over that circuit, a relationship that was first described by Bell Labs researcher Claude Shannon, shown in Figure 1-24 and widely known as the father of information theory. In 1948 Shannon published *A Mathematical Theory of*

Communication, which is now universally accepted as the framework for modern communications. We won't delve into the complex (but fascinating) mathematics that underlie Shannon's Theorem, but suffice it to say that his conclusions are seminal: the higher the noise level in a circuit, the lower the achievable bandwidth. The bottom line? *Noise matters.* It matters so much, in fact, that network designers and engineers make its elimination the first order of business in their overall strategies for creating high-bandwidth networks. This is one of the reasons that optical fiber-based networks have become so critically important in modern transport systems—they are far less subject to noise and absolutely immune to the electromagnetic interference that plagues copper-based networks. Cable companies that now offer data services have the same issues and concerns. Every time a customer decides to play installer by adding a cable spur for a new television set in their home and crimping the connector on the end of the cable with a pair of pliers instead of a tool specifically designed for the purpose, they create a point where noise can leak into the system, causing problems for everyone.

It gets even more melodramatic than that: According to John Judson, a cable systems maintenance manager in the Midwest, unauthorized connection to the cable network can cause problems that go way beyond unauthorized access to service. "Cable networks are high-frequency systems," he observes. "Some of the harmonics created in cable networks just happen to fall within the range of frequencies used in avionics, and therefore have the potential to affect aviation communications and nav-

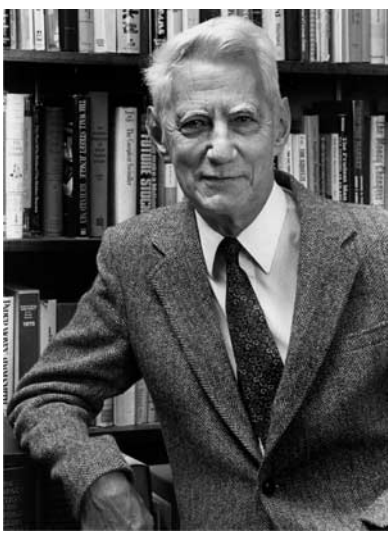


Figure 1-24 Claude Shannon (Photo courtesy Lucent Bell Laboratories).

igation. So, when you see the cable truck that looks like a commercial fishing boat cruising the neighborhood with all the antennas on top, they're looking for signal leakage from unauthorized taps. They *will* find them and they *will* come in and fix them, and you *will* get a bill for it. So, if you want to add a connection in the house, call us."

That completes our introduction of common terms, with one exception: The Internet.

The Internet: What Is It?

The Internet is a vast network of networks, recognized as the fastest growing phenomenon in human history. In the words of Douglas Adams, author of *A Hitchhiker's Guide to the Galaxy,* the Internet is "Big. Really big. Vastly, hugely, mind-bogglingly big." It is getting bigger: the Internet doubles in size roughly every 10 months, and that growth rate is expected to continue.

Not only is the Internet global in physical scope, it is universally recognized. *Everybody* knows about the Internet. In 1993, it came booming into the public consciousness, put down roots, spread like a biological virus, and flourished. Like other famous public figures, it has been on the cover of every major magazine in the world, has been the star of books, articles, TV shows, and movies, has been praised as the most significant social force in centuries, and debased as the source of a plethora of worldwide ills. Yet, for all this fame and notoriety, little is actually known about the Internet itself—at least, its private side. It is known to be a vast network of interconnected networks, with new appendages connecting approximately every 10 minutes. According to the Network Wizards' Internet Domain Survey **http://www.nw.com**, it connects approximately 110 million host computers, provides services to approximately 350 million users, and comprises roughly 500,000 interconnected networks worldwide.

The World Wide Web (WWW)

The World Wide Web was first conceived by Tim Berners-Lee, considered to be the "Father of the World Wide Web." A physicist by training, Berners-Lee began his career in the computer and telecommunications

industries following graduation from Oxford, before accepting a consulting position as a software engineer with the *European Organization for Nuclear Research* (CERN) during the late 1970s.

During his stint in Geneva, Berners-Lee observed that CERN suffers from the problems that plague most major organizations: information location, management, and retrieval. CERN is a research organization with large numbers of simultaneous ongoing projects, a plethora of internally published documentation, and significant turnover of people. Much of the work conducted at CERN revolves around large-scale, high-energy physics collaborations that demand instantaneous information sharing between physicists all over the world. Berners-Lee found that his ability to quickly locate and retrieve specific information was seriously impaired by the lack of a single common search capability and the necessarily dispersed nature of the organization. To satisfy this need, he collaborated with Robert Cailliau to write the first WWW client, a search and archive program that they called *Enquire.* Enquire was never published as a product, although Berners-Lee, Cailliau, and the CERN staff used it extensively. It did, however, prove to be the foundation for the WWW.

In May of 1990, Berners-Lee published *Information Management: A Proposal*, in which he described his experiences with hypertext systems and the rationale for Enquire. He described the system's layout, feel, and function as being similar to Apple's Hypercard, or the old Adventure game in which players moved from page to page as they navigated through the game. Remember this? Some of you will:

>YOU FIND YOURSELF IN A SMALL ROOM. THERE IS A DOOR TO THE LEFT.
>>OPEN DOOR

Enquire had no graphics, and was therefore rudimentary compared to modern Web browsers. To its credit, the system ran on a multiuser platform and could therefore be accessed simultaneously by multiple users. To satisfy the rigorous demands of the CERN staff, Berners-Lee and Cailliau designed the system around the following parameters:

- It had to offer remote access from across a diversity of networks.
- It had to be system and protocol independent, because CERN was home to a wide variety of system types—VM/CMS, Mac, VAX/VMS, and Unix.
- It had to run in a distributed processing environment.
- It had to offer access to all existing data types as well as to new types that would follow.

- It had to support the creation of personal, private links to new data sources as each user saw fit to create them.
- It had to support, in the future, diverse graphics types.
- It (ideally) had to support a certain amount of content and data analysis.

In November 1990, Berners-Lee wrote and published, with Robert Cailliau, *WorldWide Web: A Proposal for a HyperText Project*. In it, the authors described an information retrieval system in which large and diverse compendia of information could be searched, accessed, and reviewed freely, using a standard user interface based on an open, platform-independent design. This paper relied heavily on Berners-Lee's earlier paper.

In *WorldWide Web: A Proposal for a HyperText Project*, Berners-Lee and Cailliau proposed the creation of a "World Wide Web" of information that would enable the various CERN entities to access the information they needed based on a common and universal set of protocols, file exchange formats, and keyword indices. The system would also serve as a central (although architecturally distributed) repository of information and would be totally platform-independent. Furthermore, the software would be available to all and distributed free of charge.

Once the paper had been circulated for a time, the development of what we know today as the WWW occurred with remarkable speed. The first system was developed on a NeXT platform. The first general release of the WWW inside CERN occurred in May of 1991, and in December, the world was notified of the existence of the WWW (known then as W3) thanks to an article in the CERN computer newsletter.

Over the course of the next few months, browsers began to emerge. Erwise, a GUI client, was announced in Finland, and Viola was released in 1992 by Pei Wei of O'Reilly & Associates. NCSA joined the W3 consortium, but didn't announce their Mosaic browser until February of 1993.

Throughout all of this development activity, W3 servers, based on the newly released *Hypertext Transfer Protocol* (HTTP) that enabled diverse sites to exchange information, continued to proliferate. By January of 1993, there were 50 known HTTP servers; by October there were over 200, and WWW traffic comprised 1 percent of aggregate NSF backbone traffic. Very quietly, the juggernaut had begun.

In May 1994, the first international WWW conference was held at CERN in Geneva, and from that point on they were organized routinely, always to packed houses and always with a disappointed cadre of oversubscribed would-be attendees left out in the cold.

From that point on, the lines that clearly define "what happened when" begin to blur. NCSA's Mosaic product, developed largely by Marc Andreessen at the University of Illinois in Chicago, hit the mainstream and brought the WWW to the masses. Andreessen, together with Jim Clark, would go on to found Netscape Corporation shortly thereafter.

The following timeline shows the highlights of the Internet's colorful history (as well as a few other great unrelated moments). Thanks to PBS for helping to put this together.

Internet Timeline (1960–1997)

1960	There is no Internet . . .
1961	Still no Internet . . .
1962	The RAND Corporation begins research into robust, distributed communication networks for military command and control.
1962–1969	The Internet is first conceived in the early 60s. Under the leadership of the Department of Defense's *Advanced Research Project Agency* (ARPA), it grows from a paper architecture into a small network (ARPANET) intended to promote the sharing of supercomputers among researchers in the United States.
1963	Beatles play for the Queen of England.
1964	*Dr. Strangelove* portrays nuclear holocaust, which new networks must survive.
1965	The DOD's Advanced Research Project Association begins work on ARPANET. ARPA sponsors research into a cooperative network of time-sharing computers.
1966	U.S. Surveyor probe lands safely on moon.
1967	First ARPANET papers presented at Association for Computing Machinery Symposium. Delegates at a symposium for the Association for Computing Machinery in Gatlinburg, TN discuss the first plans for the ARPANET.
1968	First generation of networking hardware and software designed.
1969	ARPANET connects first four universities in the United States. Researchers at four U.S. campuses create the first hosts of the ARPANET, connecting

	Stanford Research Institute, UCLA, UC Santa Barbara, and the University of Utah.
1970	ALOHANET developed at the University of Hawaii.
1970–1973	The ARPANET is a success from the very beginning. Although originally designed to enable scientists to share data and access remote computers, e-mail quickly becomes the most popular application. The ARPANET becomes a high-speed digital post office as people use it to collaborate on research projects and discuss topics of various interests.
1971	The ARPANET grows to 23 hosts connecting universities and government research centers around the country.
1972	The InterNetworking Working Group becomes the first of several standards-setting entities to govern the growing network. Vinton Cerf is elected the first chairman of the INWG, and later becomes known as a "Father of the Internet."
1973	The ARPANET goes international with connections to University College in London, England and the Royal Radar Establishment in Norway.
1974–1981	Bolt, Beranek & Newman opens Telenet, the first commercial version of the ARPANET. The general public gets its first vague hint of how networked computers can be used in daily life as the commercial version of the ARPANET goes online. The ARPANET starts to move away from its military/research roots.
1975	Internet operations transferred to the Defense Communications Agency.
1976	Queen Elizabeth goes online with the first royal e-mail message.
1977	UUCP provides e-mail on THEORYNET.
1978	TCP checksum design finalized.
1979	Tom Truscott and Jim Ellis, two grad students at Duke University, and Steve Bellovin at the University of North Carolina establish the first USENET newsgroups. Users from all over the world join these discussion groups to talk about the Net, politics, religion, and thousands of other subjects.

1980 Mark Andreessen turns eight. In 14 more years he will revolutionize the Web with the creation of Mosaic.

1981 ARPANET has 213 hosts. A new host is added approximately once every 20 days.

1982–1987 The term Internet is used for the first time. Bob Kahn and Vinton Cerf are key members of a team that creates TCP/IP, the common language of all Internet computers. For the first time the loose collection of networks that made up the ARPANET is seen as an internet, and the Internet as we know it today is born. The mid-1980s mark a boom in the personal computer and super-minicomputer industries. The combination of inexpensive desktop machines and powerful, network-ready servers enables many companies to join the Internet for the first time. Corporations begin to use the Internet to communicate with each other and with their customers.

1983 TCP/IP becomes the universal language of the Internet.

1984 William Gibson coins the term cyberspace in his novel *Neuromancer*. The number of Internet hosts exceeds 1,000.

1985 Internet e-mail and newsgroups now part of life at many universities.

1986 Case Western Reserve University in Cleveland, Ohio creates the first Freenet for the Society for Public Access Computing.

1987 The number of Internet hosts exceeds 10,000.

1988–1990 Internet worm unleashed. The *Computer Emergency Response Team* (CERT) is formed to address security concerns raised by the Worm. By 1988 the Internet is an essential tool for communications, however it also begins to create concerns about privacy and security in the digital world. New words, such as hacker, cracker, and electronic break-in, are created. These new worries are dramatically demonstrated on Nov. 1, 1988 when a malicious program called the “Internet Worm”

temporarily disables approximately 6,000 of the 60,000 Internet hosts. System administrator turned author, Clifford Stoll, catches a group of cyberspies, and writes the best-seller *The Cuckoo's Egg*. The number of Internet hosts exceeds 100,000. A happy victim of its own unplanned, unexpected success, the ARPANET is decommissioned, leaving only the vast network-of-networks called the Internet. The number of hosts exceeds 300,000.

1991 The World Wide Web is born!

1991–1993 Corporations wishing to use the Internet face a serious problem: Commercial network traffic is banned from the National Science Foundation's NSFNET, the backbone of the Internet. In 1991 the NSF lifts the restriction on commercial use, clearing the way for the age of electronic commerce. At the University of Minnesota, a team led by computer programmer Mark MaCahill releases gopher, the first point-and-click way of navigating the files of the Internet in 1991. Originally designed to ease campus communications, gopher is freely distributed on the Internet. MaCahill calls it "the first Internet application my mom can use." 1991 is also the year in which Tim Berners-Lee, working at CERN in Switzerland, posts the first computer code of the WWW in a relatively innocuous newsgroup, "alt.hypertext." The ability to combine words, pictures, and sounds on Web pages excites many computer programmers who see the potential for publishing information on the Internet in a way that can be as easy as using a word processor. Marc Andreessen and a group of student programmers at NCSA (the *National Center for Supercomputing Applications* located on the campus of University of Illinois at Urbana Champaign) will eventually develop a graphical browser for the WWW called *Mosaic*. Traffic on the NSF backbone network exceeds 1 trillion bytes per month. One million hosts have multi-media access to the Internet over the MBone. The first audio

and video broadcasts take place over a portion of the Internet known as the "MBone." More than 1,000,000 hosts are part of the Internet. Mosaic, the first graphics-based Web browser, becomes available. Traffic on the Internet expands at a 341,634 percent annual growth rate.

1994 The Rolling Stones broadcast the Voodoo Lounge tour over the M-Bone. Marc Andreessen and Jim Clark form Netscape Communications Corp. Pizza Hut accepts orders for a mushroom, pepperoni with extra cheese over the Net, and Japan's Prime Minister goes online at **www.kantei.go.jp**. Backbone traffic exceeds 10 trillion bytes per month.

1995 NSFNET reverts back to a research project, leaving the Internet in commercial hands. The Web now comprises the bulk of Internet traffic. The Vatican launches **www.vatican.va**. James Gosling and a team of programmers at Sun Microsystems release an Internet programming language called Java, which radically alters the way applications and information can be retrieved, displayed, and used over the Internet.

1996 Nearly 10 million hosts online. The Internet covers the globe. As the Internet celebrates its 25th anniversary, the military strategies that influenced its birth become historical footnotes. Approximately 40 million people are connected to the Internet. More than $1 billion per year changes hands at Internet shopping malls, and Internet related companies like Netscape are the darlings of high-tech investors. Users in almost 150 countries around the world are now connected to the Internet. The number of computer hosts approaches 10 million.

Within 30 years, the Internet has grown from a Cold War concept for controlling the tattered remains of a post-nuclear society to the Information Superhighway. Just as the railroads of the 19th century enabled the Machine Age and revolutionized the society of the time, the Internet takes us into the Information Age, and profoundly affects the world in which we live.

The Age of the Internet Arrives

1997 Today some people telecommute over the Internet, allowing them to choose where to live based on quality of life, not proximity to work. Many cities view the Internet as a solution to their clogged highways and fouled air. Schools use the Internet as a vast electronic library, with untold possibilities. Doctors use the Internet to consult with colleagues half a world away. Even as the Internet offers a single Global Village, it threatens to create a second class citizenship among those without access. As a new generation grows up as accustomed to communicating through a keyboard as in person, life on the Internet will become an increasingly important part of life on Earth.

We will discuss the Internet in greater detail later in the book. However, just for the sake of fun, consider the following few pages that present a comparison of two technographs—one of the state of telecommunications in 1994, the other in 1999. It is not intended to be inclusive, but rather a comparison of moments in time. What a difference half-a-decade makes—and how incredibly fast this industry moves. Furthermore, consider the great buildup that occurred in 1999 in the telecom industry, followed a year later by the great meltdown of 2000–2001. What will the next five years look like? We begin in 1994—a mere seven years ago.

1994

Frame Relay has been introduced, standards are in place, and service offerings are beginning to appear. At this point, Frame Relay is a data-only service and there is no concept that it could be more than that. Meanwhile, ATM is still in the conceptual mode, and in the marketplace there is a lot of discussion about whether to go with Frame Relay as a primary backbone technology or wait for ATM. SMDS is growing as a high-bandwidth solution. LAN switching is a year away. Cisco Systems has about 40 percent of the router marketplace, Synoptics and Wellfleet are still separate companies, and discussion is underway about something called fast LAN technologies. Four, 10, and 16 Mbps are still the norm, however. By some estimates, Novell owns 65–70 percent of the

server marketplace; IPX dominates the LAN and TCP/IP is about two years overdue to be terminated (at least according to the Department of Defense, which is still waiting for OSI). NT Server does not exist. There is no Windows 95; DOS and Windows 3.11 are alive and well, and the Macintosh is a powerful player in the desktop environment. Unix is still for tech weenies.

Change is in the wind on the regulatory front, and it is dawning on the telecommunications industry that the current regulatory model is not appropriate given the rumble of enhanced competition that seems to be underway. Actual changes, however, have not yet been proposed.

The Internet, thanks to the WWW, has now been in the public eye for a year. Tim Berners-Lee has quietly rolled out his CERN-based browser, and Mosaic has become the browser of choice for the bulk of the market. Netscape is a corporate upstart on the verge of revolutionizing access to the Web. The NSF has just started to fund NAPs in the Internet world, as the government is beginning to question its own role in the process. As the Internet's popularity and incursion grow, AOL bumps heads with Prodigy and Compuserve. Hundreds, if not thousands of online service providers come out of the woodwork. However, even as it enters the third year of annual doubling in size, the Internet still isn't seen as having lasting importance in corporate America; Microsoft's Encarta doesn't even have an entry for the term. Nevertheless, the *Internet Engineering Task Force* (IETF), a loose consortium of Internet techies responsible for the technology of the Internet, starts working on the *next generation Internet Protocol* (IPng). One notable feature of IPng is that it will have 128-bit addresses; predictions are that IP's current 32-bit address space will be exhausted by 1998.

Because of growing interest in the Web, access technologies are hot and everybody wants more bandwidth over the local loop. Most modem technologies in use operate at a whopping 14.4 Kbps, but 28.8 Kbps modems are on the market and work is underway to achieve 33.6. ISDN continues to wallow in uncertainty, plagued by spotty availability, conflicting implementation standards, and questions about its value.

The corporate world is undergoing its own evolution at this time. Microsoft, Cisco, and other corporations are at the elbow of their corporate development curve. There are seven RBOCs. The only significant competitive players, other than the independents, are Teleport and MFS.

SONET standards are still considered somewhat immature; OC-48 is a laughable dream. Cell phones are considered to be an innovative, "designer" technology, and most people complain about battery life. IRIDIUM shows promise as the next great wireless network.

2000 and the beginning of the next millennium—or is that 2001?—is just six years away. What a party that will be!!

1999

Five years later, Frame Relay is a mature technology, routinely carrying data, voice, and video. It has become a premier private-line replacement technology. ATM is also mature, and is not only widely deployed, it is also being considered as the core technology for the next generation network. But ATM to the desktop is dead because of Fast Ethernet and even faster Ethernet (see the following), and ATM for even campus area networks is anybody's guess.

The current regulatory environment is—well, exciting. We now have three RBOCs instead of seven, two major IXCs (assuming that the Sprint/WorldCom merger takes place), and a plethora of CLECs, DLECs, ITSPs, ISPs, and other berserkers disrupting the market model. Furthermore, we are very close to seeing true competition at both the local and long- distance levels between the IXCs and the ILECs.

Al Gore is resting comfortably after giving birth to the Internet, which has become *the* central focal point in the telecommunications industry—as well as in virtually every *other* industry. Significant spin-off technologies abound, including Voice over IP, VPNs, Web-enabled call centers, voice-enhanced Web sites, electronic commerce, and the newly emerged E-business. The term "dot-com" has entered the lexicon and become part of everyday life. Whole portfolios are built around these Cinderella companies.

Traditional modem technology now provides 56 Kbps access (well, sort of . . .), but other technologies have leapfrogged that, including cable modems at 10 Mbps, wireless options like LMDS, and a variety of DSL services that offer bandwidth levels between 9 and 52 Mbps. SMDS is, for all intents and purposes, dead, and ISDN continues to wallow in uncertainty, plagued by spotty availability, conflicting implementation standards, and questions about its value. But Internet access gave ISDN new life, at least temporarily.

Fast and gigabit Ethernet are commonplace. LAN switching is fast becoming widely embedded technology. Optical fiber is widely deployed in local networks. WDM, DWDM, and UDWDM provide massive bandwidth over optical fiber. SONET is mature, and in fact is being discussed in some venues as if it is reaching the end of its useful life with the proliferation of WDM technologies. Companies like Qwest and Level3 are

taking advantage of them to carve out niches for themselves in the bandwidth marketplace. In fact, bandwidth has become a commodity, traded on spot markets alongside soy beans and pork bellies.

A feeding frenzy is underway as the telecommunications market converges. Companies are buying each other apace as they jockey for position in the greatest game in town, and they are doing so by implementing new applications with names like "Enterprise resource planning" and "Customer relationship management."

Cellular telephony is ubiquitous, and integrated handsets are hitting the market. Iridium, once a shining star, is in receivership. AOL is a powerhouse as the biggest ISP on the planet. They now own CompuServe, and Prodigy has become invisible. Windows 2000 is on the market, and Apple's future as a real player is uncertain. Due to the popularity of Linux, Unix has entered the mindset and vocabulary of ordinary people on the street. Firewalls, still uncommon five years ago, are now finding a market as home-based computer systems obtain 24×7 access to the Internet using cable modems and DSL technologies.

IP is now ubiquitous. NetWare version 5 will run natively over IP. All 32-bit versions of Windows (Windows 95, and so on) have a built-in TCP/IP kernel. IP version 6 (IPv6) is three years old but has yet to see widespread implementation. The IETF is now an international standards organization, sanctioned by ISO. Cisco dominates the router marketplace at the high- and middle-range, and is even a force at the low-end.

2000 came and went without incident. IT professionals who planned to have a New Years Eve party in their offices waiting for the ringing telephones, lost power, crashed computers, and other unnatural disasters that would inevitably occur at 00:00:00.00 on 1/1/2000, were sorely disappointed.

Chapter Summary

This chapter is designed to acquaint the reader with the fundamental terms and concepts that characterize the data and telecommunications worlds today. Now we can move deeper into the magic. In the next chapter, we introduce the design, philosophy, structure, and use of data communications protocols.

CHAPTER 2

Protocols

Click.

One simple action kicks off a complex series of events that results in the transmission of an e-mail message, the creation of a digital medical image, or the establishment of a videoconference between a child and a grandmother. The process through which this happens is a remarkable symphony of technological complexity, and it is all governed by a collection of rules called protocols. This chapter is dedicated to them.

Data Communications Systems and Functions

If I were to walk up to you on the street and extend my hand in greeting, you would quite naturally reach your hand out, grab mine, and shake it —in most parts of the world. We agree to abide by a commonly accepted set of social rules, one of which is shaking hands as a form of greeting. It doesn't work everywhere. In Tibet, it is customary to extend one's tongue as far as it can be extended as a form of greeting (clearly a sign of a great culture!). In China, unless you are already friends with the person you are greeting, it is not customary to touch in any fashion. You, of course, have a choice when I extend my hand. You could hit it, lick it, or spit in it. But because of the accepted rules that govern western society, you would take my hand in yours and shake it. These rules that govern communication, *any form of communication,* are called protocols. And the process of using protocols to convey information is called data communications. It's no accident, incidentally, that the obnoxious racket that analog modems make when they are attempting to connect to each other is called a handshake. The noise they make is their attempt to negotiate a common set of rules that works for both of them for that particular session.

The Science of Communications

Data communication is the procedure required to collect, package, and transmit data from one computing device to another, typically (but not always) over a *wide area network* (WAN). It is a complex process with many layers of functionality. To understand data communications, we

must break it into its component parts and examine each part individually, relying on the old adage that "the only way to eat an elephant is one bite at a time." Like a Russian Matryoshka doll, such as the one shown in Figure 2-1, data communications comprises layer upon layer of operational functionality that work together to accomplish the task at hand, namely, the communication of data. These component parts are known as *protocols*, and they have one responsibility: to ensure the integrity of the data that they transport from the source device to the receiver.

This data integrity is measured in the following ways (see Figure 2-2):

- **Bit level integrity** Ensures that the bits themselves are not changed in value as they transit the network
- **Data integrity** Guarantees that the bits are recognizable as packaged entities called frames or cells
- **Network integrity** Provides for the assured delivery of those entities, now in the form of packets, from a source to a destination
- **Message integrity** Not only guarantees the delivery of the packets, but in fact their *sequenced* delivery to ensure the proper arrival of the entire message
- **Application integrity** Provides for the proper execution of the responsibilities of each application

Protocols exist in a variety of forms and are not limited to data communications applications. Military protocols define the rules of engagement that modern armies agree to abide by, diplomatic protocols define

Figure 2-1 Russian Matryoshka dolls.

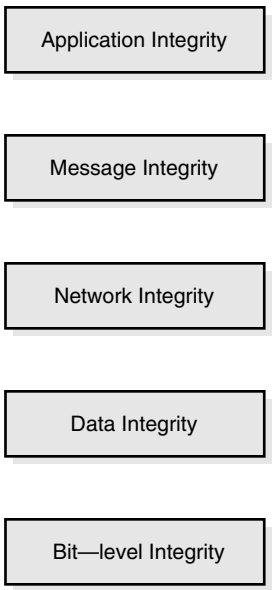


Figure 2-2 *The various integrity levels of the OSI Model.*

the manner in which nations interact and settle their political and geographic differences, and medical protocols document the manner in which medications are used to treat illness. The word *protocol* is defined as a set of rules that facilitates communication. Data communications, then, is the science built around the protocols that govern the exchange of digital data between computing systems.

Data Communications Networks

Data communications networks are often described in terms of their architectures, as are protocols. Protocol architectures are often said to be *layered* because they are carefully divided into highly related but non-overlapping functional entities. This "division of labor" not only makes it easier to understand how data communications work, but also makes the deployment of complex networks far easier.

The amount of code (lines of programming instructions) required to successfully execute the complex task of data transmission is quite large.

If the program that carries out all of the functions in that process were written as a single, large, monolithic chunk of code, then it would be difficult to make a change to the program when updates are required, because of the monolithic nature of the program. Now imagine the following: instead of a single set of code, we break the program into functional pieces, each of which handles a particular, specific function required to carry out the transmission task properly. With this model, changes to a particular module of the overall program can be accomplished in a way that only affects that particular module, making the process far more efficient. This modularity is one of the great advantages of layered protocols.

Consider the following simple scenario, shown in Figure 2-3. A PC-based e-mail user in Madrid with an account at ISP Terra Networks wants to send a large, confidential message to another user in Marseilles. The Marseilles user is attached to a mainframe-based corporate e-mail system. In order for the two systems to communicate, a complex set of challenges must first be overcome. Let's examine them a bit more closely.

The first and most obvious challenge that must be overcome is the difference between the actual user interfaces on the two systems. The PC-based system's screen presents information to the user in a *Graphical User Interface* (GUI, pronounced 'gooey') format that is carefully designed to make it intuitively easy to use. It eliminates the need to rely on the old command-line syntax that was used in DOS environments.

The mainframe system was created with intuitive ease of use in mind, but because a different company designed the interface for a mainframe host, under a different design team, it bears minimal resemblance to the PC system's interface. Both are equally capable, but completely different.

As a result of these differences, if we were to transmit a screen of information from the PC directly to the mainframe system, it would be unreadable simply because the two interfaces do not share common field names or locations.

The next problem that must be addressed is security, illustrated in Figure 2-4. We mentioned earlier that the message that is to be sent from

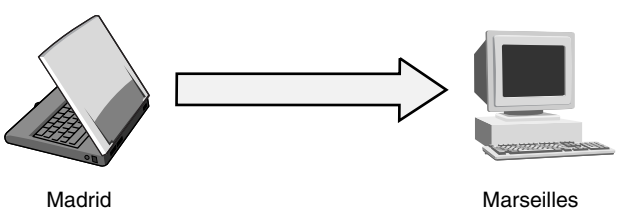


Figure 2-3 PC-to-mainframe communications.

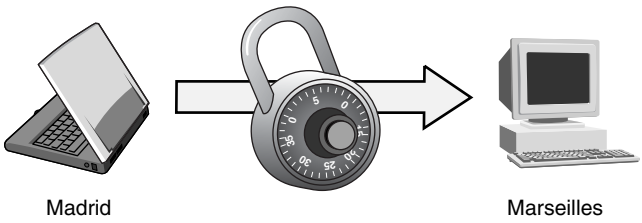


Figure 2-4
Managing security.

the user in Madrid is confidential, which means that it should probably be encrypted to protect its integrity. And because the message is large, the sender will probably compress it to reduce the time it takes to transmit it. Compression, which will be discussed in more detail later, is simply the process of eliminating redundant information from a file before it is transmitted or stored to make it easier to manage.

Another problem has to do with the manner in which the information being transmitted is represented. The PC-based Eudora message encodes its characters using a 7-bit character set, the *American Standard Code for Information Interchange* (ASCII). A sample of the ASCII codeset is shown later in Table 2-1. Mainframes, however, often use a different codeset called the *Extended Binary Coded Decimal Interchange Code* (EBCDIC). The ASCII traffic must be converted to EBCDIC if the mainframe is to understand it, and vice versa, as shown in Figure 2-5.

Binary Arithmetic Review

It's probably not a bad idea to review binary arithmetic for just a moment, since it seems to be one of the least understood details of data communications. I promise, this will not be painful. I just want to offer a quick explanation of the numbering scheme and the various codesets that result.

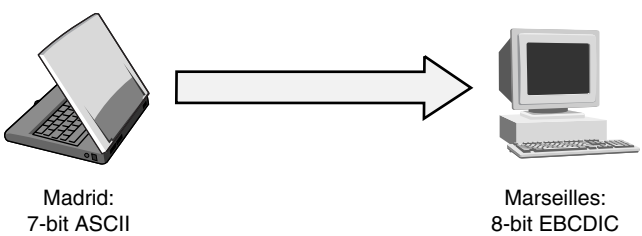


Figure 2-5
Code conversion.

Protocols

Modern computers are often referred to as digital computers because the values they use to perform their function are limited (remember, the word *digital* means discrete). Those values are nominally zero and one. In other words, a value can either be one or zero, on or off, positive or negative, presence of voltage or absence of voltage, or presence of light or absence of light. Two possible values exist for any given situation, and this type of system is called *binary*. The word means a system that comprises two distinct components or values. Computers operate using base 2 arithmetic, whereas humans use base 10. Let me take you back to second grade.

When we count, we arrange our numbers in columns that have values based on multiples of the number 10, as shown in Figure 2-6. Here we see the number 6,783, written using the decimal numbering scheme. We easily understand the number as it is written because we are taught to count in base 10 from an early age.

Computers, however, don't speak in base 10. Instead, they speak in base 2. Instead of having columns that are multiples of 10, they use columns that are multiples of two, as shown in Figure 2-7. In base 10, the columns are (reading from the right):

- Ones
- Tens
- Hundreds
- Thousands
- Ten thousands
- Hundred thousands
- Millions
- And so on

In base 2, the columns are

- Ones
- Twos

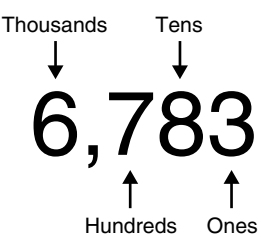


Figure 2-6 Base 10 numbering scheme.

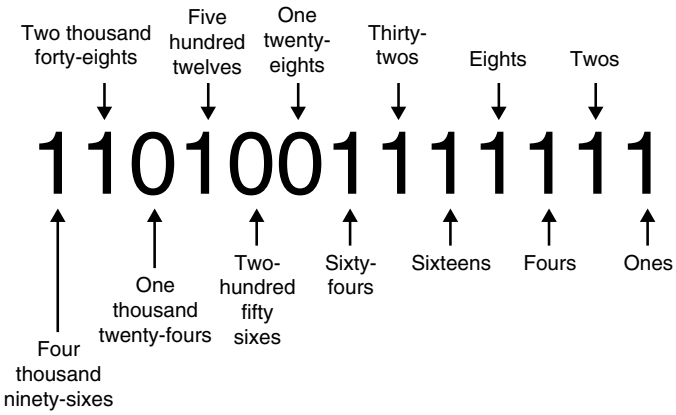


Figure 2-7 *Base 2 numbering scheme.*

- Fours
- Eights
- Sixteens
- Thirty-twos
- Sixty-fours
- One hundred twenty-eights
- Two hundred fifty-sixes
- Five hundred twelves
- One thousand twenty-fours
- And so on

So our number, 6,783, would be written as follows in base two:

1101001111111

From right to left that's one 1, one 2, one 4, one 8, one 16, one 32, one 64, no 128, no 256, one 512, no 1,024, one 2,048, and one 4,096. Add them all up (1+2+4+8+16+32+64+512+2048+4096) and you *should* get 6,783.

That's binary arithmetic. Most PCs today use the 7-bit ASCII character set shown in Table 2-1. The mainframe, however (remember the mainframe?), uses EBCDIC. What happens when a 7-bit ASCII PC sends information to an EBCDIC mainframe system that only understands 8-bit characters? Clearly, problems would result. Something therefore has to take on the responsibility of translating between the two systems so that they can intelligibly transfer data.

Table 2-1 ASCII Codeset.

Character	ASCII Value	Decimal Value
0	0110000	48
1	0110001	49
2	0110010	50
3	0110011	51
4	0110100	52
5	0110101	53
6	0110110	54
7	0110111	55
8	0111000	56
9	0111001	57
A	1000001	65
B	1000010	66
C	1000011	67
D	1000100	68
E	1000101	69
F	1000110	70
G	1000111	71
H	1001000	72
I	1001001	73
J	1001010	74
K	1001011	75
L	1001100	76
M	1001101	77
N	1001110	78
O	1001111	79
P	1010000	80
Q	1010001	81
R	1010010	82
S	1010011	83
T	1010100	84
U	1010101	85
V	1010110	86
W	1010111	87
X	1011000	88
Y	1011001	89
Z	1011010	90

Another problem that arises has to do with the logical relationship between the applications running in the two systems. Although the PC most likely supports the e-mail account of a single user, the mainframe undoubtedly hosts hundreds, perhaps thousands of accounts, and must therefore ensure that users receive their mail and *only* their mail. Some kind of user-by-user and process-by-process differentiation is required to maintain the integrity of the system and its applications. This is illustrated graphically in Figure 2-8.

The next major issue has to do with the network over which the information is to be transmitted from Madrid to Marseilles. In the past, information was either transmitted via a dedicated and very expensive point-to-point circuit, over the relatively slow public switched telephone network, or PSTN. Today, however, most modern networks are packet-based, meaning that messages are broken into small, easily routable pieces, called packets, prior to transmission. Of course, this adds an additional layer of complexity to the process. What happens if one of the packets fails to arrive at its destination? Or, what if the packets arrive at the destination out of order? Some process must be in place to manage these challenges and overcome the potentially disastrous results that could occur.

Computer networks have a lot in common with modern freeway systems, including the tendency to become congested. Congestion results in delay, which some applications do not tolerate well. What happens if some or all of the packets are badly delayed, as shown in Figure 2-9? What is the impact on the end-to-end *quality of service* (QoS)?

Another vexing problem that often occurs is errors in the bitstream. Any number of factors, including sunspot activity, the presence of electric

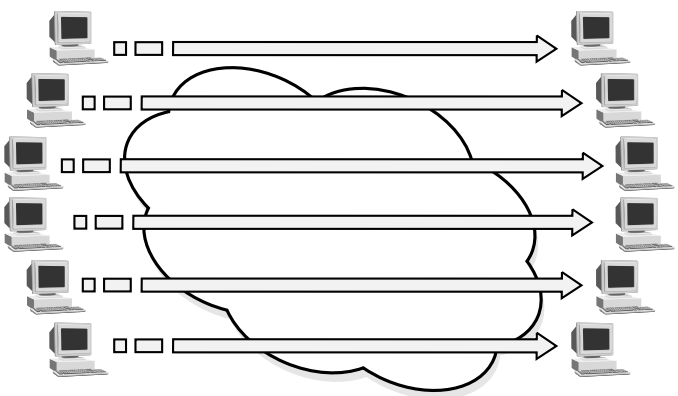


Figure 2-8
Logical session management.

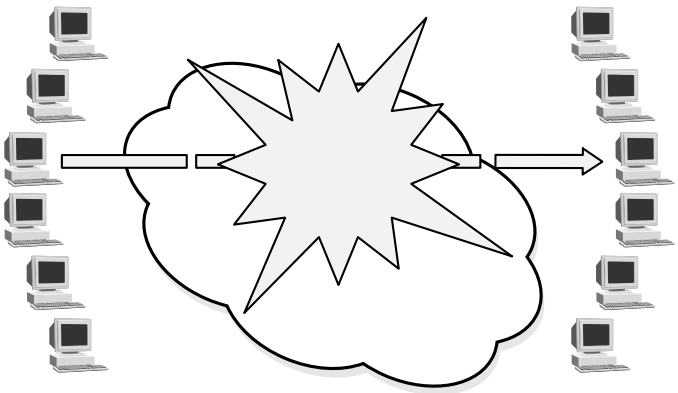


Figure 2-9
Problems in the network cause delay and lost data.

motors, and the electrical noise from fluorescent lights can result in ones being changed to zeroes and zeroes being changed to ones, as shown in Figure 2-10. Obviously, this is an undesirable problem, and a technique must be in place to detect and correct these errors when they occur.

Also, some inherent problems may be occurring in the physical medium over which the information is being transmitted. Many different media exist, including twisted copper wire pairs, optical fiber, coaxial cable, and wireless systems, to name a few. None of these are perfect transmission media; they all suffer from the vagaries of backhoes, lightning strikes, sunlight, earth movement, squirrels with sharp teeth, kids with BB guns, and other impairments far too numerous to name. When these problems occur, how are they detected? Equally important, how are the transmission impairments that they inevitably cause reported and corrected?

Also, an agreed-upon set of rules must define exactly how the information is to be physically transmitted over the selected medium. For example, if the protocol to be used dictates that information will *always* be transmitted on pin 2 of a data cable, such as that shown in Figure 2-11, then the other end will have a problem since its received signal will

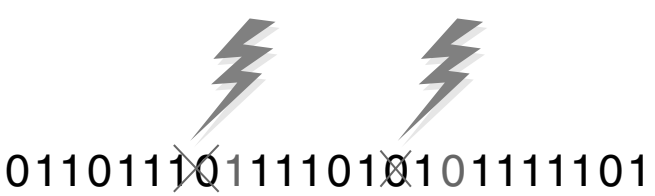


Figure 2-10
Bit errors.

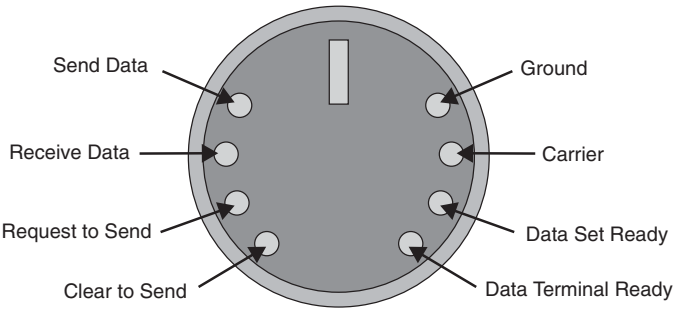


Figure 2-11 Physical agreements.

arrive on the same pin that it wants to *transmit* on. Furthermore, an agreement must be reached on how information is to be physically represented, how and when it is to be transmitted, and how it is to be acknowledged. What happens if a very fast transmitter overwhelms the receive capabilities of a slower receiver? Does the slower receiver have the capability, or even the *right,* to tell it to slow down?

Collectively, all of these problems pose what seem to be insurmountable challenges to the transmission of data from a source to a receiver. Although the process is obviously complex, steps have been taken to simplify it by breaking it into logical pieces. Those pieces, as we described earlier, are protocols. Collections of protocols, carefully selected to form functional groupings, are what make data communications work properly.

Perhaps the best-known "family" of protocols is the International Organization for Standardization's *Open Systems Interconnection Reference Model*, usually called the OSI Model for short. Shown in Figure 2-12 and comprising seven layers, it provides a logical way to study and understand data communications and is based on the following simple rules. First, each of the seven layers must perform a clearly defined set of responsibilities that are unique to that layer to guarantee the requirement of functional modularity. Second, each layer depends upon the services of the layers above and below to do its own job, as we would expect, given the modular nature of the model. Third, the layers have no idea how the layers around them do what they do; they simply know that they do it. This is called transparency.

Finally, there is nothing magic about the number seven. If the industry should decide that we need an eighth layer on the model, or that layer five is redundant, then the model will be changed. The key is functionality. An ongoing battle is taking place within the ranks of OSI Model pundits, for example, over whether *both* layers six and seven are required,

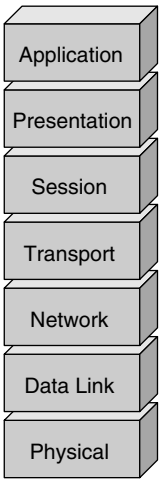


Figure 2-12
OSI Model.

because many believe them to be so similar functionally that one or the other is redundant. Others question whether layer five is needed, the functions of which are considered by many to be superfluous and redundant. Whether any changes are made is not important. The fact that changes *can* be made is what matters.

It is important to understand that the OSI Model is nothing more than a conceptual way of thinking about data communications. It isn't hardware; it isn't software. It merely simplifies and groups the processes of data transmission so that they can be easily understood and manipulated. Let's look at the OSI Model in a little more detail (please refer to Figure 2-12).

As we mentioned earlier, the model is a seven-layer construct within which each layer is tightly dependent upon the layers surrounding it. The Application layer, at the top of the model, speaks to the actual application process that creates the information to be transported by the network. It is closest to the customer and the customer's processes, and is therefore the most customizable and manipulable of all the layers. It is highly open to interpretation.

On the other end of the spectrum, the Physical layer dwells within the confines of the actual network and is totally standards-dependent. There is minimal room here for interpretation. A pulse is either a one or a zero; there's nothing in between. Physical-layer standards therefore tend to be highly commoditized, while Application-layer standards tend to be highly specialized. This becomes extremely important as the service provider model shifts from delivering commodity bandwidth to providing

customized services, even if they're mass customized, to their customer base. Service providers are clawing their way up the OSI food chain to get as close to the Application-layer end of the model as they can, because of the Willie Sutton Rule.

The Willie Sutton Rule

Willie Sutton, shown in Figure 2-13, became famous in the 1930s for a series of outrageous robberies during which he managed to outwit the police at every turn. During his career he had two nicknames, "The Actor" and "Slick Willie," because of his ingenious tendency to use a wide array of disguises during his robberies. A sucker for expensive clothes, Sutton was an immaculate dresser. Although he was a bank robber, he had the reputation of being a gentleman. In fact, people who witnessed his robberies stated he was quite polite. One teller remembers him coming into the bank dressed to the nines carrying flowers, which he presented to her in exchange for her money. Another victim said Sutton's robberies were like attending the movies, except that the usher had a gun.

On February 15, 1933, Sutton and an accomplice attempted to rob the Corn Exchange Bank and Trust Company in Philadelphia, Pennsylvania. Sutton, disguised as a mailman, entered the bank early in the morning, but a suspicious passerby caused them to abort the robbery. Roughly a year later, however, on January 15, 1934, he entered the same bank through a ceiling skylight. When the guard arrived, Sutton forced him to admit the employees, whom Sutton handcuffed and locked in a small back room.

Sutton also robbed a Broadway jewelry store in broad daylight, dressed as a telegraph messenger. His other disguises included a policeman, special delivery messenger, and maintenance man.

Figure 2-13
Willie Sutton.

Protocols

Sutton was finally caught in June of 1931 and sentenced to 30 years in prison. He escaped on December 11, 1932 by climbing a prison wall. Two years later he was recaptured and sentenced to serve 25 to 50 years in Eastern State Penitentiary, Philadelphia, for the robbery of the Corn Exchange Bank.

Sutton's career was not over yet, however. On April 3, 1945, Sutton was one of 12 convicts who escaped from Eastern State through a tunnel. He was recaptured the same day by Philadelphia police officers and sentenced to life imprisonment as a fourth-time offender. At that time, he was transferred to the Philadelphia County Prison in Homesburg, Pennsylvania to live out the rest of his days. On February 10, 1947, Sutton tired of prison life. He and several other prisoners, dressed as prison guards, carried two ladders across the prison yard to the wall shortly after dark. When the searchlights froze them in its glare, Sutton yelled, "It's okay," and no one stopped him. They climbed the wall under the watchful eye of the guards and disappeared into the night.

On March 20, 1950, Willie Sutton was added to the FBI's Ten Most Wanted list. Because of his expensive clothing habit, his photograph was given to tailors all over the country in addition to the police. On February 18, 1952, a tailor's 24-year-old son recognized Sutton on the New York subway and followed him to a local gas station. The man reported the incident to the police who later arrested him.

Sutton did not resist his arrest by New York City Police, but denied any robberies or other crimes since his 1947 escape from the Philadelphia County Prison. When he was arrested, Sutton owed one life sentence plus 105 years to the people of Pennsylvania. Because of his new transgressions (mostly making the police look remarkably incompetent), his sentence was augmented by an additional 30 years to life in New York State Prison.

Shortly after his final incarceration, a young reporter was granted a rare interview with Sutton in his prison cell. When they met, Sutton shook his hand and asked, "what can I do for you, young man?" The reporter, nervous, stammered back, "M-M-Mr. Sutton, why do you rob banks?" Sutton sat back and replied with a smile, "Because, young man, that's where the money is."

That's not the end of the story, however. In 1969, the New York State prison authority decided that Sutton did not have to serve his entire sentence of two life sentences plus 105 years, because of failing health. So, on Christmas Eve, 1969, Sutton, now 68, was released from Attica State Prison. In 1970, Sutton did a television commercial to promote the New

Britain, Connecticut Bank and Trust Company's new photo credit card program. You have to love the little ironies in life. Sutton died in 1980 in Spring Hill, Florida, at the age of 79.

So what does Willie Sutton have to do with the OSI Model and service providers? Not much, but his career does. Today's service providers are climbing the food chain because the money is up there with the customers. Yes, of course, money can be made at the Physical Layer end of the model, but the sustainable, growable revenues are up where services can be customized endlessly to meet the changing needs of customers.

Back to the Model

More now about the inner workings of the OSI Model.

The functions of the model can be broken into two pieces, as illustrated by the dashed line in Figure 2-14 between layers three and four that divide the model into the *chained layers* and the *end-to-end layers*.

The chained layers comprise layers one through three: the Physical layer, the Data Link layer, and the Network layer. They are responsible for providing a service called *connectivity*. The end-to-end layers on the other hand comprise the Transport layer, the Session layer, the Presentation layer, and the Application layer. They provide a service called *interoperability*. The difference between the two services is important.

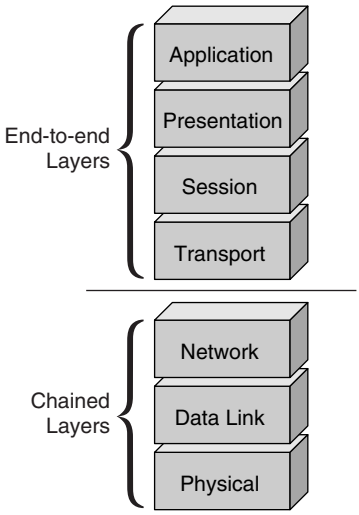


Figure 2-14 Chained vs. end-to-end layers.

Protocols

Connectivity is the process of establishing a physical connection so that electrons can flow correctly from one end of a circuit to the other. Little intelligence is involved in the process. It occurs, after all, pretty far down in the protocol ooze of the OSI Model. Connectivity is critically important to network people; it represents their lifeblood. Customers, on the other hand, are typically only aware of the criticality of connectivity when it isn't there for some reason. No dial tone? Visible connectivity. Can't connect to the ISP? Visible connectivity. Dropped call on a cell phone? Visible connectivity.

Interoperability, however, is something that customers are much more aware of. Interoperability is the process of guaranteeing *logical connectivity* between two communicating processes over a physical network. It's wonderful that the lower three layers give a user the ability to spit bits back and forth across a WAN. But what do the bits mean? Without interoperability, that question cannot be answered.

For example, the e-mail application running on the PC and the e-mail application running on the mainframe are logically incompatible with each other for any number of reasons that will be discussed shortly. They can certainly swap bits back and forth, but without some form of protocol intervention, the bits are meaningless. Think about it: if the PC shown on the left side of Figure 2-15 creates an e-mail message that is compressed, encrypted, ASCII-encoded, and shipped across logical channel 17, do the intermediate switches that create the path over which the message is transmitted care? Of course not. Only the transmitter and receiver of the message that house the applications that will have to interpret it care about such things. The intermediate switches care that they have electrical connectivity, that they can see the bits, that they can determine whether they are the *right* bits, and whether they themselves are the intended recipient or not. Therefore, the end devices, the sources and sinks of the message, must implement all seven layers of the OSI Model, because they must not only concern themselves with connectivity issues, but also with issues of interoperability. The intermediate

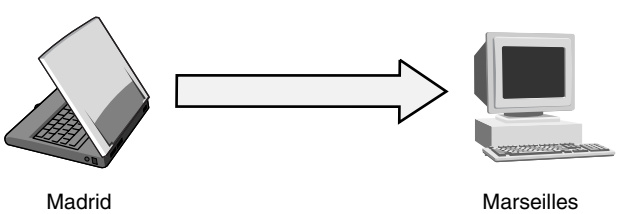


Figure 2-15
Connectivity.

devices, however, only care about the functions and responsibilities provided by the lower three layers. Interoperability, because it only has significance in the end devices, is provided by the end-to-end layers, layers four through seven. Connectivity, on the other hand, is provided by the chained layers, layers one through three, because those functions are required in every link of the network chain, hence the name.

Layer by Layer

The OSI Model relies on a process called enveloping, illustrated in Figure 2-16, to perform its tasks. If we return to our earlier e-mail example, we find that each time a layer invokes a particular protocol to perform its tasks, it wraps the user's data in an "envelope" of overhead information that tells the receiving device about the protocol used. For example, if a layer uses a particular compression technique to reduce the size of a transmitted file, and a specific encryption algorithm to disguise the content of the file, then it is important that the receiving device be made aware of the technique employed so that it knows how to decompress and decrypt the file when it receives it.

Needless to say, quite a bit of overhead must be transmitted with each piece of user data. The overhead is needed, however, if the transmission

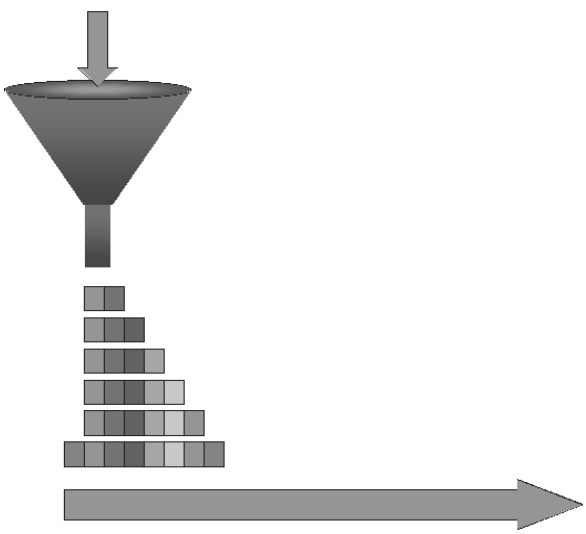


Figure 2-16
The enveloping process.

is to work properly. So, as the user's data passes down the so-called stack from layer to layer, additional information is added at each step of the way, as illustrated.

In summary then, the message to be transported is handed to layer seven, which performs Application-layer functions and then attaches a header to the beginning of the message that explains the functions performed by that layer so that the receiver can interpret the message correctly. In our illustration, that header function is represented by information written on the envelope at each layer. When the receiving device is finally handed the message at the Physical layer, each succeeding layer must open its own envelope until the kernel, the message, is exposed for the receiving application. Thus, OSI protocols really do work like a nested Russian doll. After peeling back layer after layer of the network onion, the core message is exposed.

Let's now go back to our e-mail example, but this time we'll describe it within the detailed context of OSI's layered architecture. We begin with a lesson on linguistics.

Esperanto

An old and somewhat comforting cliché observes that "wherever one goes, people speak English." In fact, less than 10 percent of the world's population speaks English, and to their credit many of them speak it as a second language.[1] Many believe there is a real need for a truly international language. In 1887, Polish physician Ludwig L. Zamenhof published a paper on the need for a universally spoken tongue. He believed that most of the world's international diplomacy disputes resulted from a communication failure between monolingual speakers and the inevitable misunderstandings of nuance that occur when one language is translated into another. Zamenhof set out to solve this "Tower-of-Babel" problem (origin of the word babble, by the way), the result of which was the creation of the international language called *Esperanto.* In Esperanto, the word Esperanto means "one who hopes."

Since its creation, Esperanto has been learned by millions and, believe it or not, is widely spoken; current estimates say that it is known by

[1]Among seasoned international travelers an old joke exists that goes likes this: "What do you call someone who speaks three languages?" *Trilingual.* "OK, what do you call someone who speaks *two* languages?" *Bilingual.* OK, what do you call someone who speaks *one* language? *American.*

approximately 2 million speakers. And its use is far from being purely academic. Meetings are held in Esperanto, advertising campaigns use it, hotels and restaurants publish literature using it, and professional communities such as health care and scientific research now use Esperanto widely as a way to universally communicate information. Second only to English, it is the *lingua franca* of the international world. It is most commonly spoken in Central and Eastern Europe, East Asia (particularly mainland China), South America, and Southwest Asia. It is less commonly spoken in North America, Africa, and the Middle East.

Esperanto's success as the language of international communication results from three advantages. It is easy to learn, it is politically neutral, and there are practical reasons to learn it. The structure of the language is so simple and straightforward that it can typically be learned in less than a quarter of the time it takes to learn a traditional language. For example, all letters have one sound and one sound *only.* Only 16 grammar rules must be learned, compared to the hundreds that pervade English and other Romance or Germanic languages. Furthermore, it has no irregular verb forms (you have to love that!). Even the vocabulary is simple to learn. Many words are instantly recognizable (and learnable), such as these:

- Telefono (telephone)
- Biciclo (bicycle)
- Masxino (machine)
- Reto (network)
- Kosmo (outer space)
- Plano (plan)

Speakers of languages other than English will recognize the roots of these words. Reto, for example, is similar to the Spanish word *red* (network). A pretty good Esperanto-English dictionary can be found at **http://www.geocities.com/Athens/Forum/1197/glossar2.htm**.

Just for fun, here's a paragraph, courtesy of the Esperanto League of North America (**http://www.esperanto-usa.org/**):

> Inteligenta persono lernas la lingvon Esperanto rapide kaj facile. Esperanto estas la moderna, kultura lingvo por la tuta mondo. Simpla, fleksebla, belsona, g`i estas la praktika solvo de la problemo de universala interkompreno. Esperanto meritas vian seriozan konsideron. Lernu la internacian lingvon Esperanto.

Here's the translation:

> An intelligent person learns the language Esperanto rapidly and easily. Esperanto is the modern, cultural language for the whole world. Simple, flexible, musical, it is the practical solution for the problem of universal mutual understanding. Esperanto deserves your serious consideration. Learn the international language Esperanto.

(I have included a short Esperanto dictionary in the Appendix as well as a list of resources on the subject for no reason other than the fact that it is interesting.)

So what does this have to do with telecommunications and the transmission of e-mail messages? Read on.

Layer 7: The Application Layer

The network user's application (Eudora, Outlook, Outlook Express, or PROFS) passes data down to the uppermost layer of the OSI Model, called the Application layer. The Application layer provides a set of highly specific services to the application above it that have to do with the *meaning* or *semantic content* of the data. These services include file transfer, remote file access, terminal emulation, network management, mail services, and data interoperability. This interoperability is what enables our PC user and our mainframe-based user to communicate. The Application Layer converts the application-specific information into a common, canonical form that can be understood by both systems. A canonical form is a form that can be understood universally. The word comes from *canon,* which refers to the body of officially established rules or laws that govern the practices of a church. The word also means an accepted set of principles of behavior that all parties in a social or functional grouping agree to abide by. Hence, the applicability of Esperanto.

Let's examine a real-world example of a network-oriented canonical form. When network hardware manufacturers build components such as switches, multiplexers, cross-connect systems, and modem pools for sale to their customers, they do so knowing that one of the most important aspects of a successful hardware sale is the inclusion of an element management system that will enable customers to manage the device within their networks. The only problem is that today most networks are made up of equipment purchased from a variety of vendors. Each vendor develops its own element managers on a device-by-device basis, which works

exceptionally well for each device. This does not become a problem until it comes time to create a management hierarchy for a large network, shown in Figure 2-17, at which time the network management center begins to look a lot like a Macy's television department. (A large network management system is shown in Figure 2-18.) Each device or set of devices requires its own display monitor, and when one device in the network fails, causing a waterfall effect, the network manager must reconstruct the entire chain of events to discover what the original causative factor was. This is sometimes called the Three-Mile-Island effect.

Back in the 1970s when the Three Mile Island nuclear power plant went critical and tried to make Pennsylvania glow in the dark, it became

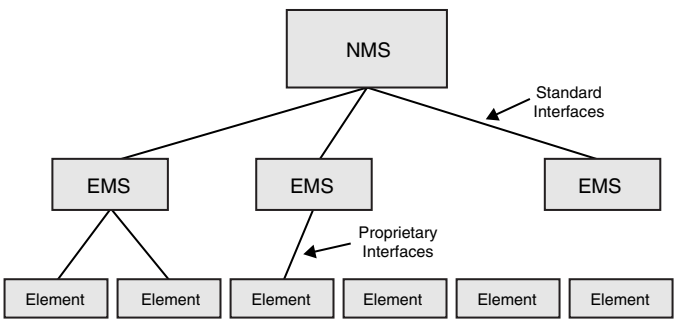


Figure 2-17 Network management hierarchy.

Figure 2-18 Network management center (Courtesy of AT&T).

clear to the Monday morning quarterbacks trying to reconstruct the event and create the "how this could have been prevented" document that all the information required to turn the critical failure of the reactor into a nonevent was in the control room, buried somewhere in the hundreds of pages of fanfold paper that came spewing out of the high-speed printers. No procedure was in place to receive the output from the many managed devices and processes involved in the complex task of managing a nuclear reactor, analyzing the output, and handing a simple, easy-to-respond-to decision to the operator.

The same problem is true in complex networks. Most of them have hundreds of managed devices with simple associated element management systems that generate primitive data about the health and welfare of each device. The information from these element managers is delivered to the network management center, where it is displayed on one of many monitors that the network managers themselves use to track and respond to the status of the network. What they *really* need is a single map of the network that shows all of the managed devices in green if they are healthy. If a device begins to approach a preestablished threshold of performance, the icon on the map that represents that device turns yellow, and if it fails entirely, it turns red, yells loudly, and automatically reports and escalates the trouble. In one of his many books on American management practices, USC Professor Emeritus Warren Bennis observes that "the business of the future will be run by a person and a dog. The person will be there to feed the dog; the dog will be there to make sure the person doesn't touch anything." Clearly, that model applies here.

So how can this ideal model of network management be achieved? Every vendor will tell you that their element management system is the best element manager ever created. None of them are willing to change the user interface that they have created so carefully. Using a canonical form, however, there is no reason to. All that has to be done is to exact an agreement from every vendor that stipulates that, although they do not have to change their user interface, they must agree to speak some form of technological Esperanto on the back side of their device. That way the users still get to use the interface they have grown accustomed to, but on the network side, every management system will talk to every other management system using a common and widely accepted form. Again, it's just like a canonical language. If people from five different language groups need to communicate, they have a choice. They can each learn everybody else's language (four additional

languages per person) or they can agree on a canonical language (Esperanto), which reduces the requirement to a single language each. An example is shown in Figure 2-19.

In network management, several canonical forms exist. The most common are the *International Organization for Standardization's* (ISO) *Common Management Information Protocol* (CMIP), the *Internet Engineering Task Force's* (IETF) *Simple Network Management Protocol* (SNMP), and the Object Management Group's *Common Object Request Brokered Architecture* (CORBA). As long as every manager device agrees to use one of these on the network side, every system can talk to every other system.

Other canonical forms found at the Application layer include ISO's X.400/X.500 Message Handling Service, the IETF's *Simple Mail Transfer Protocol* (SMTP) for e-mail applications, ISO's *File Transfer, Access, and Management* (FTAM), the IETF's *File Transfer Protocol* (FTP), and the *Hypertext Transfer Protocol* (HTTP) for file transfer, and a host of others. (Quiz: Where would you find these defined?) Note that the services provided at this layer are highly specific in nature. They perform a limited subset of tasks.

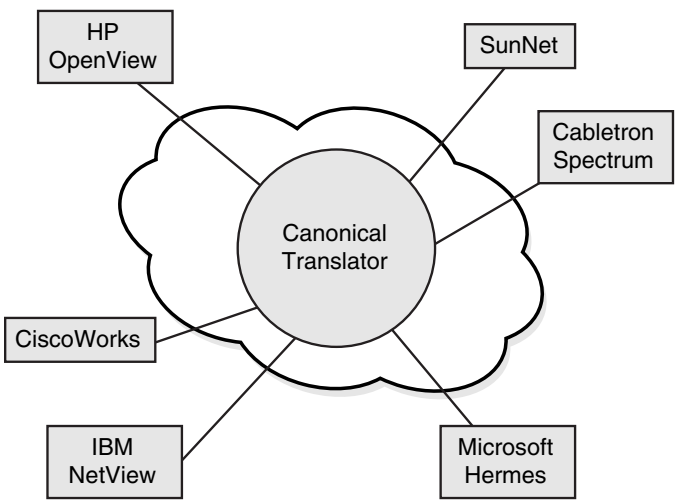


Figure 2-19
Canonical translator.

Layer 6: The Presentation Layer

For our e-mail example, let's assume that the Application layer converts the PC-specific information to X.400 format and adds a header that will tell the receiving device to look for X.400-formatted content. This is not a difficult concept. Think about the nature of the information that must be included in any e-mail encoding scheme. Every system must have a field for the following:

- Sender (From)
- Recipient (To)
- Date
- Subject
- Cc
- Bcc
- Attachment
- Copy
- Message body
- Signature (optional)
- Priority
- Various other miscellaneous fields

The point is that the number of defined fields is relatively small, and as long as each mail system knows what the fields are and where they exist in the coding scheme of the canonical standard, it will be able to map its own content to and from X.400 or SMTP. Problem solved.

Once the message has been encoded properly as an e-mail message, the Application layer passes the now slightly larger message down to the Presentation layer. It does this across a layer-to-layer interface using a simple set of commands and encoding structures called *service primitives*.

The Presentation layer provides a more general set of services concerning the structural *form* or *syntax* of the data than the Application layer does. These services include code conversion, such as 7-bit ASCII to 8-bit EBCDIC translation, as well as compression, using such services as PKZIP, British Telecom Lempel-Ziv, the various releases of the *Moving*

Picture Experts Group (MPEG), the *Joint Photographic Experts Group* (JPEG), and a variety of others. The services also feature encryption, which includes *Pretty Good Privacy* (PGP) and *Public Key Infrastructure* (PKI). Note that these services can be used on any form of data; spreadsheets, word processing documents, and rock music can all be compressed and encrypted. Compression is typically used to reduce the number of bits required to represent a file through a complex manipulative mathematical process that identifies redundant information in the image, removes it, and sends the resulting smaller file off to be transmitted or archived. To explain how compression works, let's examine JPEG.

JPEG was developed jointly by ISO and the *International Telecommunication Union Standardization Sector* (ITU-T) as a technique for the compression of still images while still retaining varying degrees of quality as required by the user's application. Here's how it works. Please refer to Figures 2-20a and 2-20b, which are photographs of my nephew, E.J.

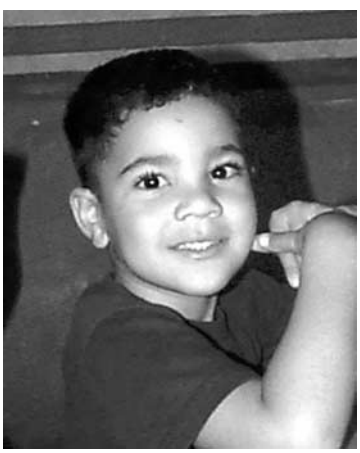


Figure 2-20a
EJ.

Figure 2-20b
EJ's eye.

Figure 2-20a shows the original photograph, a reasonably good quality picture that has in fact been substantially compressed using JPEG. Figure 2-20b comprises a small portion of the image on the left, specifically E.J.'s right eye. Notice the small boxes that make up the image. Those boxes are called *picture elements,* or pixels. Each pixel requires substantial computer memory and processing resources: 8 bits for storage of the red components of the image, 8 bits for green, and 8 bits for blue, which are the three primary colors (and the basis for the well-known RGB color scheme). That's 24-bit color, and every pixel on a computer screen requires them. Furthermore, a screen contains a lot of pixels. Even a relatively low-resolution monitor that operates at 640×480 has 307,200 pixels, with 24 bits allocated per pixel. That equates to 921,600 bytes of information, or roughly 1MB.

Just for fun, let's see what happens when we make the image move, as we will do if we're transporting video. Since typical video generates 30 frames per second, that's 221,184,000 bits that have to be allocated per second, a 222-Mbps signal. That's faster than a 155-Mbps SONET OC-3c signal! The message is that we'd better be doing *some* kind of compression.

JPEG uses an ingenious technique to reduce the bit count in still images. First, it clusters the pixels in the image (look at Figure 2-20b) into 16-pixel-by-16-pixel groups, which it then reduces to 8×8 groups by eliminating every other pixel. The JPEG software then calculates an average color, hue, and brightness value for each 8×8 block, which it encodes and transmits to the receiver. In some cases, the image can be further compressed, but the point is that the number of bits required to reconstruct a high-quality image is dramatically reduced by using JPEG.

Encryption, on the other hand, is used when the information contained in a file is deemed sensitive enough to require that it be hidden from all but those eyes with permission to view it.

Encryption is one aspect of a very old science called cryptography. Cryptography is the science of writing in code. Its first known use dates to 1900 B.C. when an Egyptian scribe used nonstandard hieroglyphs to capture the private thoughts of a customer. Some historians feel that cryptography first appeared as the natural result of the invention of the written word. Its use in diplomatic messages, business strategies, and battle plans certainly supports the theory.

In data communications and telecommunications, encryption is required any time the information to be conveyed is sensitive and the possibility exists that the transmission medium is insecure. This can occur over any network, although the Internet is most commonly cited as being the most insecure of all networks.

All secure networks require a set of specific characteristics if they are to be truly secure. The most important of them are as follows:

- **Privacy/confidentiality** The capability to guarantee that no one can read the message except the intended recipient.
- **Authentication** The guarantee that the identity of the recipient can be verified with full confidence.
- **Message integrity** Assurance that the receiver can confirm that the message has not been changed in any way during its transit across the network.
- **Nonrepudiation** A mechanism to prove that the sender really sent this message and was not sent by someone pretending to be the sender.

Cryptographic techniques, including encryption, have two responsibilities: they ensure that the transmitted information is free from theft or any form of alteration, and they provide authentication for both senders and receivers. Today, three forms of encryption are most commonly employed: secret key (or symmetric) cryptography, public-key (or asymmetric) cryptography, and hash functions. How they work is beyond the scope of this book, but numerous resources are available on the topic (see the Bibliography in the Appendix). One of the best resources is *An Overview of Cryptography* by my good friend Gary Kessler. The paper, which Gary updates routinely, is available at **http://www.garykessler.net/library/crypto.html**.

Whenever I lecture about security, I always find that people have an intense interest in computer and network hackers. Over the years, I have had the opportunity to meet and interview many of them and to learn what drives their behavior and what they *really* do. Since we are on the subject of security, and before we leave the Presentation layer, here is an essay on the topic.

An Aside: Hackers I Have Known

Late one night, long after everyone has gone home for the evening, an 18-year-old computer cracker, following weeks of fruitless attempts, finally manages to penetrate the logical firewall that protects your cor-

porate minicomputer. He logs into the system and deletes or damages critical customer contact records, accounting data, the results of months of research and development activity, and product order databases. On a whim, he unleashes a virus on the operating system that is designed to awaken weeks or months from now and wreak havoc on the system's hard drive array. As a capstone to his efforts, he uploads the access information for your system to electronic cracker bulletin boards all over the country.

Like a frog on a wax dissecting tray, you have been cut open, violated, and displayed to the world. To understand why hackers do what they do, it is first important to know who a hacker really is. The classic image that leaps to mind at the mention of the word is that of a dark and mysterious figure, hunched over a networked computer in the dead of night, wreaking untold digital havoc upon an unsuspecting, sleeping public.

This is certainly the image that Hollywood moviemakers have created for the hacker community, and although there may be some truth to it, the reality is far more complex. Hackers certainly share certain social and behavioral characteristics, but they are as difficult a segment of the population to stereotype as any other.

History of Hackers

The term hacker originated long before it was applied to the world of computers. According to Phil Agre of MIT[2], the term really has only two meanings, regardless of the context in which it is used. First, it is "an appropriate application of ingenuity." Second, it is "a creative practical joke."

Two of the earliest and best-known examples of hacking occurred at college sports events. In 1961, Caltech students from Pasadena hacked the annual Rose Bowl game by replacing three sets of cards (2,300 cards in each set, a nontrivial achievement) that would be used by students in the stands to perform card stunts. The results were predictable. Instead of displaying WASHINGTON, one set of replaced cards displayed CALTECH. Another displayed HUSKIES, but spelled it backwards. A final stunt portrayed a beaver (Caltech's mascot) instead of the Washington husky.

[2] Brian Leibowitz: *The Journal of the Institute for Hacks, Tomfoolery and Pranks*. MIT Museum, 1990.

A second hack occurred in November of 1982, when MIT hacked the Harvard-Yale football game. Following Harvard's second touchdown against Yale in the first quarter, a small black balloon emerged from the ground on the 40-yard line and began to expand. On it was printed MIT in large letters. When the balloon reached a diameter of about six feet, it popped with a bang and a cloud of white smoke. The *Boston Globe* later reported that the winner of the Harvard-Yale game was in fact MIT, and MIT's president was quoted as saying, "There is absolutely no truth to the rumor that I had anything to do with it, but I wish there were."[3]

Both of these stunts required enormous ingenuity, planning skills, stealth, patience, and moxie. In keeping with Agre's earlier definition, they were certainly creative applications of ingenuity, as well as terrific practical jokes. Although they were harmless stunts, they exhibited a less desirable characteristic that is all too often shared with computer hacks: they disrupted the smooth operation of carefully planned systems and events. A practical joke that momentarily disrupts a football game is one thing; disruption of a computer system upon which people depend for critical societal services is another thing entirely.

Enter the Computer

As computer technology found its way onto the college campus in the 1960s, the term hacker began to take on a new meaning. First applied to computer students at MIT, Stanford, and other universities with burgeoning computer science departments, it was used to describe people who were smitten with interconnected computers and driven to discover everything they could about their inner workings and capabilities. These students soon formed a loosely connected community within which they freely shared information about operating system flaws, physical and logical security loopholes that could be exploited, and techniques for exploring the telephone network and hacking free service from AT&T (a practice that came to be known as *phreaking*). Some of these early hackers went on to achieve significant success. Witness Steve Wozniak and Steve Jobs, the founders of Apple Computer Corporation, who funded their early careers by making and selling blue boxes, 2600-Hz tone generators used to eke free service from the telephone company.

---

[3] Op. Cit.

Today the word *hacker* has taken on a more nefarious connotation. It is globally used to describe those individuals who engage in criminal activity that involves unauthorized access to computers, databases, and networks. They are invariably described as delinquents, computer criminals, vandals, or worse. But in reality, who are these people? And how, if at all, do they differ from the hackers of the 1960s who started it all?

A Hacker Profile

Max Weber, the noted anthropologist, wrote that social position or status is predicated on three key factors: the accumulation of wealth, power (and therefore the ability to control), and the achievement of an enhanced state of prestige among peers. This same model, with a few modifications, applies reasonably well to the hacker community. Although most hackers are not particularly interested in accumulating vast amounts of wealth, they *are* interested in accumulating vast amounts of information, the coin of their realm. In the hacker's universe (not unlike the modern corporate universe), information equates to power, and power quickly sublimes to prestige. It is clear that prestige within the community stems directly from technical proficiency, and therefore a certain amount of native intelligence.

This indication of intelligence has not gone unnoticed outside the community. In a speech delivered just prior to the 1990 hacking trial of Craig Neidorf, a.k.a. Knight Lightning, editor of *Phrack Magazine*, Vermont Senator Patrick Leahy observed that "we cannot unduly inhibit the inquisitive 13-year-old who, if left to experiment today, may tomorrow develop the telecommunications or computer technology to lead the United States into the twenty-first century. He represents our future and our best hope to remain a technologically competitive nation." And although Senator Leahy clearly does not advocate hacking, he is quick to point out that the degree of the punishment should be in keeping with the magnitude of the crime. One industry pundit, defending the actions of Masters of Deception hacker Phiber Optik (Mark Abene), observed that "hacking represents about as much of a threat to the newly rampant telecommunications juggernaut as shoplifting does to the future of world capitalism."[4] Public opinion of the relative "evilness" of hackers is clearly all over the map.

[4] Julian Dibbell: *The Prisoner: Phiber Optik Goes to Jail*. *Village Voice*, January 11, 1994.

Shared Characteristics

In *Information Warfare,* author Winn Schwartau observes that most hackers share several common characteristics. They tend to be male, between the ages of 12 and 28. They are often social misfits who feel ignored and misunderstood, and often come from emotionally abusive or otherwise dysfunctional families. According to Schwartau, they often suffer from clinical narcissistic personality disorder. Although typically very intelligent, they tend to not do particularly well in school, perhaps because they are often shy and introverted and therefore lack the social skills at school that so often contribute to good academic performance.

Because many hackers are raised in families where they feel that they have little control over their own lives, it is easy to understand why they would be attracted to hacking. As one hacker[5] observed, "there is a sort of technological purity to what we do. We don't try to damage systems; we just want to prove that we can get in, look around, leave our mark to show that we've been there, and get out, undetected. There's an incredible sense of power that comes from being able to do that." Another hacker interviewed during the preparation of this book[6] said that his lawyer (an ex-hacker) described the feeling as being similar to the euphoria achieved during sexual intercourse, a similarly "invasive" act.

In spite of the melodramatic images painted by Hollywood, hackers rarely use information garnered during online expeditions to financially enrich themselves. Although exceptions to this aren't hard to find (as evidenced by recent online thefts of bank credit card and telephone company calling card data), most hackers eschew this sort of activity, concentrating instead on the thrill of reaching forbidden information rather than the use of the information itself.

Countless articles, letters, and personal testimonials speak of this "hacker ethic." Even Chris Goggans, better known as Legion of Doom hacker Erik Bloodaxe, claimed repeatedly to be adamantly opposed to destructive hacking:[7]

> "Malicious hacking pretty much stands against everything that I adhere to. You always hear people talking about this so-called hacker ethic and I really do believe that. I would never wipe anything out. I would never take a system down and delete anything off of a system. Any time I was ever in

---

[5] From author's personal interview with a San Francisco Bay Area hacker (name withheld by request).

[6] E-mail interview with ice9, January 1996.

[7] From an interview with Netta Gilboa of *Gray Areas Magazine*, Fall 1994.

> a system, I'd look around the system, I'd see how the system was architectured [sic], see how the directory structures differed from different types of other operating systems, make notes about this command being similar to that command on a different type of system, so it made it easier for me to learn that operating system. Because back then you couldn't just walk down the street to your university and jump right on these different computer systems, because they didn't have them and if they did have them only several classes would allow you access to them. Given the fact that I was certainly not of college age, it wasn't really an option. You didn't have public access to systems . . . So, the whole idea of doing anything destructive or malicious . . . just goes against the grain of anything that's me. I find it pretty repulsive and disgusting. I am certainly not blind to the fact that there are people out there that do it, but obviously these people have a sh—ty upbringing or they are just bad people."

Although most hackers are young white males, a significant (15 to 20 percent) female contingent also exists among the hacker elite, scattered across the United States. As for the ethnic mix, there appear to be statistically significant inclusions of Jewish hackers in the east and Asian hackers in the west.

What, then, does the personality profile of the typical hacker look like? Although in reality there is no such thing as a typical hacker, certain oft-repeated characteristics become obvious.

Physical Appearance Considering the number of hours that hackers sit sedentary in front of their computers, they tend to be remarkably thin, although there are certainly overweight hackers. They rarely have tans and tend to dress in T-shirts, jeans, running shoes, or Birkenstocks. They often have long hair and/or mustaches, eschew briefcases for backpacks, and strongly dislike business attire, often to the point of quitting a job rather than conforming to a dress code. The overall look is one of "casual scruffiness."

Education Teen hackers tend to be something of an educational mixed bag. They are usually extraordinarily bright, yet often exhibit the traits of poor students. Some are diagnosed with *Attention Deficit Disorder* (ADD) because of their inability to concentrate. According to statistics gathered from various sources,[8] they are often simply bored and feel unchallenged by traditional scholastic activities.

[8] These sources consist of a combination of personal interviews conducted by the author, published works, and various online resources (cited in bibliography).

Beyond their teen years, hackers tend to either have college degrees or an equivalent level of self-education. Those that go on to college often study electrical or mechanical engineering, management information systems, computer science, software engineering, data processing, or physics. A reasonable number of them study math, philosophy, philology, linguistics, and history.

Hackers who are self-educated tend to be highly intelligent and inordinately curious about the things that interest them. They tend to be able to absorb large quantities of seemingly unrelated facts, and to dredge them up at some later time.

In spite of the image that has emerged of them, hackers tend to be interested in many different subjects and are far from intellectually limited. They tend to be capable of maintaining an intense interest in subjects that interest them, and less so with subjects that bore or frustrate them. As a result, their online world tends to be immaculately organized, their real world a chaotic mess.

Hacker Demographics

Hacker activity in the United States has two primary geographic focal points. One is Berkeley, California; the other, Cambridge, Massachusetts. Usenet studies that have been conducted over the years indicate that 50 to 60 percent of the hackers in the United States are concentrated around those two cities, with the bulk of the remainder found in Seattle, Los Angeles, Research Triangle Park (Raleigh-Durham), Washington D.C., Princeton, Austin, and New York City. These are clearly university towns. The large hacker presence there may reflect the presence of current and former students.

As noted earlier, the hacker community is predominantly white male, although the percentages of females and minorities in their midst are growing. By and large, prejudice is nonexistent in the hacker community and is in fact despised by most hackers. One reason for this, suggested during an interview with a young hacker in Minneapolis, is interesting. Because the bulk of hacker communications are executed online, race and gender have no meaning in their world. The now-famous *New Yorker* cartoon of the Internet dogs comes to mind: "isn't it great? On the Internet nobody knows you're a dog."

Other Traits

Many hackers tend to be intellectually intolerant of others, often considering those who do not share their technical prowess or interest to be intellectually inferior (hearkening back to the aforementioned Clinical Narcissistic Personality Disorder). They often have trouble interacting with nonhackers and may have trouble forming and keeping strong emotional relationships. In spite of the fact that hackers are often very precise and accurate in their use of language, they often have poor interpersonal communication skills and difficulty identifying with nonhackers. In spite of all this, many hackers are extremely skillful social engineers, capable of engaging in chatty conversations with unsuspecting people to extract sensitive information from them. Some of the best known (and devastating) hacks were accomplished via social engineering.

How does this work? Consider the following. Data centers tend to be 24-hour operations, staffed around the clock by computer operators, software support personnel, and network managers. The least senior people will always be found on the night shift, because (1) they have the lowest seniority, and (2) they can't hurt anything at night (the machines are usually offline running backups and the like).

Now imagine the following scenario. It is 3 A.M. Sitting in front of the main system console is a new operator, still learning the idiosyncrasies of the machine. Suddenly, the phone beside the console rings. She answers it.

> Operator: Um . . . Online Operations, this is Sandra.
>
> Hacker: Hey, Sandra, how you doing? This is Bill down in Ops support and we've got a big problem. Remember that DSQL30 job that we just ran? Well, it bombed off and I have to get it restarted. I've been on the phone for the last two hours with Jim Nye down in Application Support and he's really ripped because I woke him up, but hey, that's why he makes the big bucks, right? Anyway, Sandra, I need you to spool up P000366 on tape drive C so I can get this puppy humming again. Can you do that for me? If we get this started in the next five minutes, I'll be able to do a restore and have the onlines up on time, which means you get to be a hero."

Sandra, of course, *should* call Jim Nye down in Application Support and risk his wrath before complying with the request. However, the obvious authority in the voice of the person on the other end of the line con-

vinces Sandra that she should do what she is being asked to do. She does, and a hacker makes off with whatever information is stored on that tape. This is social engineering at its best.

In *Old Hackers, New Hackers: What's the Difference?*,[9] hacker Steve Mizrach (a.k.a. Seeker1) takes umbrage with Steven Levy, author of the seminal 1984 work *Hackers,* over his perception of the differences between the hackers of the 1960s and those of the 1990s. According to Levy, the differences between the two are quite clear. The 1960s hackers were a creative lot who loved having control over their computers and who were always seeking to improve and simplify the way they worked and interfaced with people. Early hackers hacked because of a feeling of "truth and beauty" in their activities, and always shared what they learned freely within the community. They were, according to Levy, computer wizards.

1990s hackers, on the other hand, were often perceived as driven by a desire to destroy and tamper with computers and the information they housed to gain control over people. They exploited and manipulated, hacked for profit and status, and were paranoid, isolated, and secretive. They were computer terrorists, always searching for new forms of electronic vandalism or maliciousness with little concern for the consequences.

In the final analysis, little difference exists between the two groups of people. However, a dramatic difference is apparent in their targets, and it is largely a social one. In the early days of hacking, computers were primarily used by universities, R&D organizations, and very large, monolithic corporations. The impact of hackers went largely unnoticed by the general public, because by and large, the activity was restricted to a small universe that the general public knew very little about. Generally speaking, they simply weren't affected.

Today, however, two factors have changed that. The first is the pervasive infiltration of computers throughout all facets of society; the second is the relatively high level of technological sophistication that the general public possesses. Computers and the networks that interconnect them have become intrinsic and critical elements throughout modern society. They control hospital life support devices, aircraft approaches and reservation systems, telephony networks, heating and cooling subsystems, and the world's ability to buy and sell commodities. No longer does a hacker-initiated computer disruption pose an annoyance to a small and eclectic group of researchers. Today it stands to affect the public at large in profound and potentially injurious ways.

---

[9] Steve Mizrach. *Old Hackers, New Hackers: What's the Difference?*

Like any societal subset, the hacker community is a complex mix of personalities, motivations, and talents. Some hack for the thrill of the hunt; others do so with criminal intent, planning personal gain from the information they access. Although network, system, and law enforcement professionals argue over the relative level of criminal damage that hackers inflict, there is only one truth: all hackers are motivated to penetrate system security, and if there is a weakness, they *will* find and exploit it. The personnel responsible for system security should operate under the assumption that *all* systems have weaknesses and should therefore take steps to put into place robust physical and logical firewalls, as well as routine audit procedures.

Where Do We Go From Here?

The movie *Sneakers* revolved around a group of hackers who reformed their ways, repackaged their technical skills, and created a consulting firm to help organizations like the *National Security Agency* (NSA) protect themselves from attacks by the very people they used to be. This is a nice model, but how close to reality is it? Do corporations really knowingly hire hackers as security consultants? After all, when the U.S. Leasing Corporation was hacked by Kevin Mitnick (recently released after serving a five-year prison term for malicious hacking) in 1980, one executive suggested to the MIS department that perhaps "we should hire the kid." The reply from MIS was, "OK, but how many people will we have to hire to watch him?"

As the generalized use of the Internet as a tactical business tool becomes more pervasive, corporate security professionals have good reason to be concerned. In a study conducted jointly by consultancy Ernst & Young and *InformationWeek Magazine*, more than half of all chief information officers questioned reported security-related losses in the previous business year. Of those who use the Internet as an external business tool, 20 percent claimed to have been hacked at least once during the same time frame. Losses from these security-related events ranged from $100,000 to more than 1 million dollars from a single penetration.

Clearly, some sort of robust and immediate action is needed to forestall repeated security violations. Most corporations today have designed and installed effective firewall technology on their critical systems. It has been repeatedly proven, however, that one of the weakest links in any secure system is not the hardware or software, but rather the people who run the system. Many hackers exploit logic faults,

Internet Protocol (IP) holes, and sloppy programming to penetrate systems. Just as many, however, use social engineering, the process described earlier of conning people in computer rooms and central offices into being unwitting accomplices for the same purpose. For this reason, some security professionals believe that the best way to implement a corporate anti-hacker security program is to bring hackers into the corporation to fill the role. Is this a viable model?

Popular Myths

Hackers have enjoyed a veil of technological mystery for some time that often portrays them differently than reality. The press would have the world believe that hackers are routinely arrested and sent away to enjoy long jail terms. In fact, arrests have been relatively rare, and convictions rarer still. Even more rare are instances in which hackers are hired on the courthouse steps to oversee security within a corporation.

Another common belief is that hackers often pool their resources when they "see the error of their ways" and form security consultancies. In the late 1980s, Chris Goggans (Erik Bloodaxe) and other members of the now defunct Legion of Doom decided to abandon hacking and form a security consulting firm called Comsec. The business, firmly ensconced in a modern office suite in Houston with high ceilings and skylights, opened its doors in May of 1991. They had no clients, but they quickly took steps to remedy that problem. They printed fliers and press releases advertising their services, and then compiled a list of companies that had been penetrated by hackers. This last was easy; they simply scanned the postings on any number of hacker *Bulletin Board Services* (BBSs), and sent press releases to the companies that appeared there.

Soon after they began their mailings, both *Newsweek* and *Time* came out with stories about Comsec, referring to them as "the hackers who turned anti-hackers." That was all it took. The phone began to ring, and soon Comsec had business. Unfortunately, things did not continue smoothly. Rival hackers from spin-off group Masters of Deception hacked into Comsec's systems and phone lines, prompting Chris Goggans to contact the FBI. The Secret Service got involved, and before long, most members of the Masters of Deception were under indictment and on their way to serve time for their actions.

Comsec soon went out of business. According to Goggans in an interview conducted with *Gray Areas Magazine* in the Fall of 1994, the company folded largely because of bad treatment from the press:

> "We were basically blacklisted by the security community. They wouldn't allow me a forum to publish any of my articles. [The trade magazines] were told by certain members of large accounting firms that they would pull their advertising if they associated with us . . . I had speaking engagements pulled. A head of a very large security association promised me a speaking engagement and then decided to cancel it and didn't bother to tell me until a month before the conference. I talked to him and he said, 'Oh, well, I should have called you.' . . . We had that kind of treatment."

Most hackers point out that although the *Sneakers* model is perhaps more Hollywood than it is reality, success stories have certainly occurred. One hacker interviewed in Munich, Germany summed it up this way:

> "Most of us were pretty young when we started hacking, and we did it more for the thrill than anything else. Eventually, though, we grew up, took on responsibilities, and got real jobs. This doesn't mean we all stop hacking; it just means that some of us take what we know and sell it for a paycheck. For example, I work for the help desk organization of a big computer manufacturer. What I know about computers and networks goes well beyond what other people in the organization know; I'm good at it, and my employer knows it. As long as I continue to do a good job and get commendation letters from big customers, he doesn't care that I was a hacker. And yes, he does know."

It should be noted that most of the hackers involved in the Legion of Doom and Masters of Deception debacle learned from their experiences and went on to secure jobs that use their skills productively in one way or another. Some went on to college, whereas others didn't, but most of them now use their skills legitimately. They work for computer companies, research institutions, and telecommunications service providers. Other publish books and magazines or make films.

Hiring Hackers: Pros

"I wish I had known who he was, because I would have hired him on the spot." That was the assessment of one hacker's abilities by a former computer operations manager at one of the seven *Incumbent Local Exchange Carriers* (ILECs). "This guy used to call the console three or four times a week, bragging about how he was going to get into 'the system' again tonight. The operators would challenge him, but sure enough, almost without exception, sometime during the graveyard shift a message would

appear on the main OPS console from the guy. He was in the system. It's also important to note that he was a hacker in the classical sense of the term. He never hurt anything; he just wanted to prove that he could get in. It was the thrill of the chase. In fact, his messages would always consist of three parts. He'd say, "I'm back, in spite of your security; here's how I got in; and here's what you have to do to fix the hole. In a few days, I'll come back and find another one for you." And he'd be gone.

"Now, there were three options I could have pursued. I could have shut down the network, denying the guy access—along with everybody else trying to get into the system. I could have called security, who *might* have caught him. Of course, if I had done that, he'd have gotten a slap on the wrist and come back with a vengeance. This was not a guy I wanted mad at me, given the facility with which he jumped in and out of our critical systems.

"Finally, I had a third option, and that was to do what I did: stroke the guy's ego, and let him wander around the system while watching him closely. After all, in the four years I had that job, he never did any damage, and in fact provided a valuable service. Of course, if security had known about it, there'd have been hell to pay. One day he just disappeared. I don't know if he got caught, found all the holes, got bored, or discovered girls. All I know is that one day he just quit calling. On the one hand I was relieved; on the other, I felt like I had lost a staff member."

There is no question that some hackers have valuable skills that could be used by corporate security organizations to their advantage. However, like any prospective employee, hackers must be carefully screened to determine their motivation, their relative technical skill level, and whatever unique qualities they have that, combined with the first two items, would cause an employer to consider hiring them. *If* proper screening procedures are employed, and *if* the hiring manager is comfortable with the prospective employee, then they can be placed in the pool along with other potential candidates.

Employers should be aware of the fact that within the general hacker community, three recognizably distinct motivational subgroups exist. The first group comprises legitimate hackers, who for the most part subscribe to the hacker ethic that says "break in, look around, don't touch anything, leave a mark, and get out." They have no intention of causing damage or disrupting service.

The second group are called *phreakers*. Phreakers use their skills to secure free telephone service (phreaking), usually by hacking their way into privately owned *Private Branch Exchanges* (PBXs) or by manipulating the public telephone network.

Crackers make up the final group. Crackers are legitimate thieves who manipulate networks and computer resources to defraud banks, insurance companies, and the like. Cracking often involves electronic funds transfers and the manipulation of automatic teller machines. Some spectacular incidents of cracked bank systems have occurred in the last few years, but thankfully the success rate is low.

Hackers and phreakers pose the least threat to potential employers. They are often young and, according to the general community, are often more technically astute than crackers. They also lack criminal baggage.

So what are the advantages of hiring a hacker? First, if the corporation has done its assessment of the candidate properly, then it stands to turn a technically astute opponent into an ally. Second, the learning curve for the hacker-turned-professional can be far less steep than that for traditional new hires, although the hacker's knowledge coming in the door must be carefully assessed.[10]

Third, the corporate security organization benefits because it now has a behind-the-scenes entree into the hacker community, as well as the capability of an accomplished hacker on staff. After all, the Federal Government hired a hacker informant to help them capture Kevin Mitnick.

Within the data security world, organizations (again, the *Sneakers* model) called *Tiger Teams* make their living as "hackers for hire," breaking into systems for a fee in order to uncover weaknesses. Many security experts observe, however, often correctly, that hackers are far more imaginative than professional Tiger Teams.[11]

Thus, hiring hackers as employees has its advantages. Of course, like anything else, there is also a downside.

Hiring Hackers: Cons

It can be argued that hackers do what they do because of a lack of judgment. They are young; they don't sense the "wrongness" of what they're doing. They succumb to peer pressure, or they are psychologically flawed because of family problems and aren't capable of sensing the difference between right and wrong.

---

[10] Knowledge claimed and knowledge held are often quite different. The author reviewed one legitimately published book that claimed to be an authority on the telecommunications and computer technology behind hacking. It was rife with errors. Hence, a careful assessment of a hacker's actual knowledge base is in order.

[11] Gary C. Kessler: "*Computer and Network Security.*" June 1995.

It can also be argued that although some hackers mature and recognize that what they do may be wrong, others do not. This implies a serious lack of ethical propriety and should be a consideration for prospective employers.

Countless examples of system penetrations have occurred because hackers were hired, knowingly or not, as system operators, maintenance personnel, or even janitors. It is incumbent upon the hiring manager to determine whether hiring a hacker into a sensitive position is worth the potential risk to corporate systems. Managers as a rule are not psychologists, but the question of whether a hacker has been "rehabilitated" to the point of being a valuable and nonthreatening employee should be in the forefront of the consideration process. There is no question that many hackers do mature, do outgrow the thrill of the illicit hack, and do go on to become responsible contributors to the telecommunications industry and beyond. It is critical, however, that managers properly assess their motivation for employment.

Although hackers, former or otherwise, may prove to be valuable employees in a company, it is incumbent upon the employer to assess the possible threat of a hacker on the payroll. If the decision is made to hire the individual, management must take steps to observe their actions during the first few months of employment. In many companies, this comes in the form of a probationary period, during which the employee is carefully scrutinized. Any infraction can then be dealt with quickly and professionally.

Hacker: Villain or Hero?

In most computer-literate circles, the mere mention of the word *hacker* conjures up a mental kaleidoscope of dark and brooding images. A being of consummate evil, the hacker has made a wholesale commitment to the dark side, forever intent on wreaking untold digital destruction upon the computers that have massed their forces behind the featureless stone walls of the data center keep.

Although that is a nice image, and it serves to rally the data defenders to a common defensive cry, in the real world it's not that simple. Hackers cannot be pigeonholed into a stereotypical image any more than other societal groups can. Hacking is, at best, socially questionable, and at worst, mildly illegal (assuming that no damage is done). Hackers themselves are often seen as social outcasts, even pariahs. Does this, however, make them criminals?

Protocols

Most true hackers commit themselves to some sort of hacker ethic, a set of rules that by and large says the following: "Get in, look around, leave your mark, get out. Don't touch data, don't gerrymander file structures, and don't trash hardware." In essence, "Do No Harm."

"We represent the Lewis and Clark of Cyberspace," says Climber, one of many hackers who agreed to be interviewed for this chapter. "We're out there pushing the envelope, trying to learn as much about this new frontier as we can. To us, the challenges of security systems are like the challenges of the wilderness. They are there to be overcome, and in the same way the early explorers overcame the forces of nature, we strive to overcome the challenges of system security. Lewis and Clark did no damage to nature when they crossed the country; in the same spirit, we mean no harm to the systems we penetrate."

Consider the term *hero*. The *American Heritage Dictionary* defines a hero as "a person noted for feats of courage or nobility of purpose, especially one who has risked or sacrificed his or her life." Although hackers don't generally risk their lives in their pursuits, they do put themselves at a considerable legal risk. The hacker community recognizes significant accomplishments among their members and rewards them with special titles that indicate the degree of their accomplishments. The highest level is called Elite status and is striven for by all. Within the hacker circle, those who accomplish particularly skillful hacks are viewed as heroes, particularly by neophytes.

Social groups tend to differentiate themselves according to clearly defined and accepted guidelines. In early societies, lines of differentiation were drawn between groups that provided levels of service to the community, such as hunting, building, gathering, farming, and so on. In the hacker community, as in many businesses, these differentiation lines are drawn between subgroups that exhibit various hacking skill levels.

Chris Goggans, the leader of the Legion of Doom in the 1980s, was clearly a hero to members of the up-and-coming hacker ranks. Goggans believed in the do-no-harm hacker ethic, going so far as to convert the Legion of Doom into the legitimate ComSec organization. His thirst for knowledge about the inner workings of computer systems was a model of behavior for both hackers and hacker wannabes, and although his activities, like those of all hackers, were clearly on the fuzzy edge of legal, they were admired and emulated. To his followers, Erik Bloodaxe was a hero.

Who, then, is the villain in this story? In literature, the villain is typically the character that is at odds with the story's hero. Within the hierarchy of the Legion of Doom, that character might well have been Mark Abene, better know to his peers as hacker Phiber Optik. Although

Goggans and Abene started out as colleagues in the Legion of Doom, they eventually found themselves at odds with each other, locked in a philosophical battle over the direction and guiding principles of the organization. Abene left the Legion of Doom to found the Masters of Deception, a rival hacker organization that routinely "attacked" the Legion, which by that time had been converted to ComSec.

Of course, one could also argue that the police were the villains in this technodrama. The Legion of Doom was an organization of highly intelligent young people engaged in an activity that was considered to be patently illegal. However, they had made the decision to "go straight" by converting their organization into a computer security consultancy. They created a business plan, rented office space, advertised their services, and even lined up a few clients. Even so, because of their prior activities, the police worked closely with AT&T and eventually issued search warrants for several members' residences. Villain or hero? Again, it isn't that simple. The police were doing their jobs, protecting the public from a perceived threat. The hackers were, to their way of thinking, committing no crime.

Paul Hind (a pseudonym at the request of the interviewee) is the computer operations manager for a large multinational bank in the San Francisco Bay area. For him, hackers straddle the fence between hero and villain. "On the one hand," he says, "Hackers make my job infinitely more difficult. Sometimes I feel that I spend the bulk of my time throwing up barriers, trying to keep them out of our systems. In those instances, I really resent their intrusions because it feels like a violation of some kind of trust.

"On the other hand, hacking represents a sort of perverse challenge to me and my staff. It's a sort of 'us against them' activity where our skills are pitted against theirs. And let me be the first to tell you, these people have talent. Some of them know more about the inner workings of our systems than my best people. I'd love to have them on my staff."

In one interview, Hind described a situation that developed that made him realize that hackers, while not necessarily heroes, are not always villains either: "we were doing a major install of an application update, and we had applications support staff dialing in from all over the place. Some of them were in centers as far away as Texas. Anyway, we finished the install around three in the morning, and in the confusion [Operations] forgot to shut down the dial network, leaving a huge system absolutely wide open to intrusion. The only reason we found out about it was a message that appeared on the system console about a half-hour after we finished. It said, "Congratulations on a successful install. However, you left

your front-end dial lines up. Better knock them down before somebody less charitable than me gets in." It was signed, SYS_HACK.

"We had always suspected that there were hackers playing around in the system, but until that time we never had any direct evidence of it. For all I know, he's in there now, but if he is, I can't find him. And since he's never hurt anything—and in fact, has done me at least one favor—I'm not inclined to tell anyone about it. I suppose there's a risk with that, but I'm willing to take it."

Paul Hind's opinion of hackers is perhaps the most accurate and is in fact somewhat widely shared. Clearly, hackers with malicious intents are out there, just as malign individuals make up any subgroup of society. They do not, however, fall into neatly crafted stereotypes, in spite of what the popular press would like to think.

Ice9 is a longtime hacker who agreed to be interviewed via the Internet. He believes strongly in the hacker "do no harm" ethic and is amused by the efforts of the press to paint all hackers as misguided ne'er-do-wells. "I sometimes find it entertaining the way we (hackers) are portrayed in the media. We must keep in mind, as we read these stories, that sensationalism sells.

"The plain and honest truth is that most of us are sensible people that do get away from the keyboard from time to time. Most of us have careers and are reasonably productive members of society. True, if you go to a hacker convention, you'll find all kinds of people with purple hair wearing studded leather and rags, as if they came right out of a [William] Gibson or [Neal] Stephenson novel. Most of what you'd see would not be hackers, but hacker fans or people who just know each other.

"There are always a few maladjusted, chemically imbalanced kids out there that live just to cause trouble, but most of us are just regular people that got computers when we were young and never lost our curiosity about them.

"I'm sorry if my reply is a bit long, but it would not be accurate to generalize hackers, as with any group of people, to be good or evil. I will say that we contribute a great deal to everyone on the net, since we make it necessary for software vendors to ensure proper security and privacy for their users." Clearly, ice9's perspective mirrors Hind's rather closely.

So, when are hackers villains? As before, this is a gray area. Most individuals interviewed for this chapter, however, including the hackers themselves, agreed that the villains are those who step over the unspoken line of ethical behavior. It is interesting to note that many of the hackers were quick to point out that as many villains can be found in the ranks of law enforcement as in the hacker community. According to many

of them, often an unspoken level of mutual respect exists between the hacker and the law enforcement agent. In some cases, however, the relationship is much more predatory, and law enforcement agents will sometimes "overstep the bounds" of the relationship. But what defines the location of the line?

Gary Kessler is an assistant professor of computer science at Champlain College in Burlington, Vermont. A widely recognized authority on computer and network security, he believes that ethically any unauthorized penetration of a private system is a violation, regardless of the intent. "Suppose someone finds a key to your house while you are on vacation," he posits. "They unlock the door, go inside, and close the door behind them. They then systematically go through your closets, drawers, photo albums, medicine chest, and kitchen cabinets. They don't take anything, you understand, nor do they do any damage. They just look around. When they're finished, they leave, closing the door behind them.

"The person who found the key and used it might argue that they did nothing wrong. They damaged nothing, nor did they take anything that wasn't theirs. Most people, however, will argue that the mere presence of that person in their house without prior knowledge or permission is a violation of the highest order, one that they might very well call the police about.

"In my mind, the same rule applies with computers. Whether the person does damage or not, or steals information or not, is immaterial. They're in a system without the permission of the owner, and that violates a trust. It's wrong and amounts to criminal trespass."

So: villain or hero? Obviously, the question has no absolute answer. Hackers argue quite convincingly (and many computer security employees will agree) that they provide a valuable service to the computer community as a whole.

"Oil companies hate organizations like Greenpeace," says Climber. "Well, we're sort of like the Greenpeace of cyberspace. We force computer security organizations, hardware and software manufacturers, and users to always be on their toes, and to always manufacture and manage the best and most secure products possible. We're sort of like a catalyst, and they should appreciate what we do."

The other sides of the argument are equally compelling. Law enforcement officials may (and sometimes do) harbor a grudging admiration for the "cleverness" exhibited by their hacker quarries, but in the final analysis, their job is to enforce the law. There is little room for interpretation, and for the most part, the law today says that unauthorized use of a network or access to a computer is a violation of that law. Although

some computer professionals like Paul Hind respect and even find value in hacker activities, others view those same activities as a base violation.

During an early interview with one of the hackers mentioned previously, the hacker described the act of penetrating a machine's security wall as being similar to sex. Using that analogy, one could argue that unlawful computer and network access is a form of rape, a crime that deserves no quarter. A melodramatic interpretation? Perhaps. Privacy, however, and the protection of personal property are rights that most individuals in a society value and protect vociferously. When it comes to interpretation of the law, most people find little room for charity when they are the victim of the violation.

Let's turn our attention now back to our e-mail message.

The Session Layer

We have now left the Presentation layer. Our e-mail message is encrypted and compressed, and may have gone through an ASCII-to-EBCDIC code conversion before descending into the complexity of the Session layer. As before, the Presentation layer adds a header containing information about the services it employs.

For being such an innocuous layer, the Session layer certainly engenders a lot of attention. Some believe that the Session layer could be eliminated by incorporating its functions into the layer above or the layer below, thus simplifying the OSI model. Whatever. The bottom line is that it *does* perform a set of critical functions that cannot be ignored.

First of all, the Session layer ensures that a logical relationship is created between the transmitting and receiving applications. It guarantees, for example, that our PC user in Madrid receives his or her mail and *only* his or her mail from the mainframe, which is undoubtedly hosting large numbers of other e-mail users. This requires the creation and assignment of a logical session identifier.

Many years ago, I recall an instance when I logged into my e-mail account and found to my horror that I was actually logged into my Vice-President's account. Needless to say, I backpedalled out of there as fast as I could. Today I know that this occurred because of an execution glitch in the Session layer.

Layer five also shares the responsibility for security with the Presentation layer. You may have noticed that when you log in to your e-mail application, the first thing the system does is ask for a login ID, which

you dutifully enter. The ID appears in the appropriate field on the screen. When the system asks for your password, however, the password does not appear on the screen. The field remains blank or is filled with stars, shown graphically in Figure 2-21. This is because the Session layer knows that the information should not be displayed. When it receives the correct login ID, it sends a command to the terminal (your PC) asking you to enter your password. It then immediately sends a second message to the terminal, telling it to turn off "local echo" so that your keystrokes are not echoed back on to the screen. As soon as the password has been transmitted, the Session layer issues a command to turn local echo back on again, enabling you to once again see what you type.

Another responsibility of the Session layer that is particularly important in mainframe environments is a process called *checkpoint restart.* This is a process that is analogous to the autosave function available on many PC-based applications today. I call it the Hansel and Gretel function. As the mainframe performs its many tasks during the online day, the Session layer keeps track of everything that has been done, scattering a trail of digital bread crumbs along the way as processing is performed. Should the mainframe fail for some reason (the dreaded ABEND), the Session layer will provide a series of recovery checkpoints. As soon as the machine has been rebooted, the Session layer performs the digital equivalent of walking back along its trail of bread crumbs. It finds the most recent checkpoint, and the machine uses that point as its most recent recovery data, thus eliminating the possibility of losing huge amounts of recently processed information.

So, the Session layer may not be the most glamorous of the seven layers, but its functions are clearly important. As far as standards go, the list is fairly sparse. See the ITU-T's X.225 standard for the most comprehensive document on the subject.

After adding a header, layer five hands the steadily growing *Protocol Data Unit* (PDU) down to the Transport layer. This is the point where we first enter the network. Until now, all functions have been software-based and, in many cases, a function of the operating system.

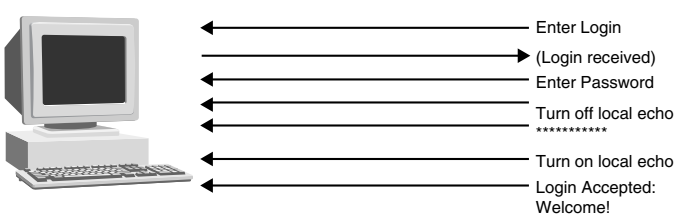


Figure 2-21
Session Layer turns off echo to protect user.

Protocols

The Transport layer's job is simple: to guarantee end-to-end, error-free delivery of the entire transmitted message. Not bits, not frames or cells, not packets, but the entire message. It does this by taking into account the nature and robustness of the underlying physical network over which the message is being transmitted, including the following characteristics:

- Class-of-service required
- Data transfer requirements
- User interface characteristics
- Connection management requirements
- Specific security concerns
- Network management and reporting status data

Two basic network types are available: *dedicated* and *switched*. We will examine each in turn before discussing Transport-layer protocols.

Dedicated networks are exactly what the name implies, an always-on network resource, often dedicated to a specific customer, which provides a high-quality transport service. That's the good news. The bad news is that dedicated facilities tend to be expensive, particularly because the customer pays for them whether they use the facility or not. Unless they are literally using it 100 percent of the time, the network is costing them money. The other downside of a dedicated facility is susceptibility to failure. Should a terrorist backhoe driver decide to take the cable out, there is no alternative route for the traffic to take. It requires some sort of intervention on the part of the service provider that is largely manual. Furthermore, dedicated circuits tend to be inflexible, because again, they are dedicated.

Switched resources, on the other hand, work in a different fashion and have their own set of advantages and disadvantages to consider. First and foremost, they require an understanding of the word virtual.

When a customer purchases a dedicated facility, he or she literally "owns" the resources between the two communicating entities, as shown in Figure 2-22. Either the circuit itself is physically dedicated to them (common in the 1980s), or a timeslot on a shared physical resource such

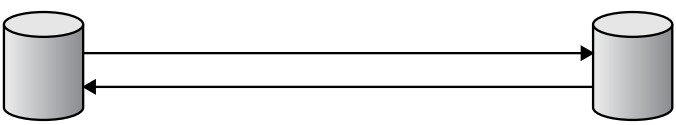


Figure 2-22 Point-to-point circuit.

as T-Carrier is dedicated to them. Data is placed on the timeslot or the circuit and it travels to the other end of the established facility, very simple and straightforward. No possibility of a misdelivered message exists, because the message only has a single possible destination. Imagine turning on the faucet in your front yard to water the plants and having water pour out of your neighbor's hose. It would be about that ridiculous.

In a switched environment, things work quite differently. In switched networks, the only thing that is actually dedicated is a timeslot, because everything in the network that is physical is shared among many different users. Imagine what a wonderful boon to the service providers this technology is. It gives them the ability to properly support the transport requirements of large numbers of customers while selling the same physical resources to them, over and over and over again. Imagine!

To understand how this technology works, please examine Figure 2-23. In this example, device D on the left needs to transmit data to device K on the right. Notice that access to the network resources (the switches in the cloud) is shared with three other machines. In order for this to work, each device must have a unique identifier so that the switches in the network can distinguish among all the traffic streams that are flowing through them. This identifier, often called a *virtual circuit identifier,* is assigned by the Transport layer as one of its many responsibilities. As examples, X.25, frame relay, and ATM are all switched network technologies that rely on this technique. In X.25, the identifier is called a virtual circuit identifier; in frame relay, it is called a *data link connection identifier* (DLCI, pronounced "Delsey"); and in ATM, it is called a virtual circuit identifier as well. Each of these will be described in greater detail later in the book.

When device D generates its message to device K for transport across the network, the transport layer "packages" the data for transmission. Among other things, it assigns a logical channel that the ingress switch

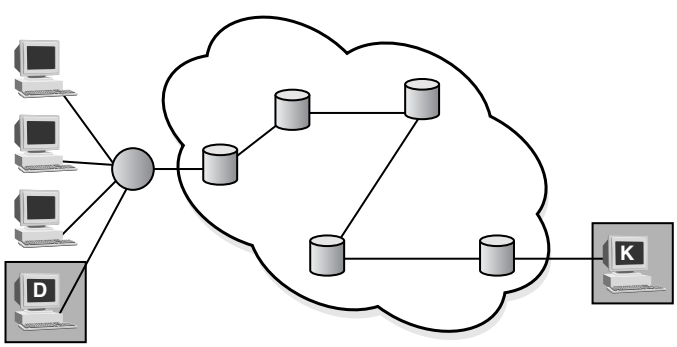


Figure 2-23
A switched network.

uses to uniquely identify the incoming data. It does this by creating a unique combination of the unique logical address with the shared physical port to create an entirely unique virtual circuit identifier.

When the message arrives at the first switch, the switch enters the logical channel information in a routing table that it uses to manage incoming and outgoing data. There can be other information in the routing table as well such as QoS indicators. These details will be covered later when we discuss the Network layer (layer three).

The technology that a customer uses in a switched network is clearly not dedicated, but it gives the appearance that it is. This is called *virtual circuit service,* because it gives the appearance of being there when in fact it isn't. *Virtual Private Networks* (VPNs), for example, give a customer the appearance that they are buying private network service. In a sense, they are; they do have a dedicated logical facility. The difference is that they share the physical facilities with many other users, which enables the service provider to offer the transport service for a lower cost. Furthermore, secure protocols protect each customer's traffic from interception. VPNs are illustrated in Figure 2-24.

As you may have intuited by now, the degree of involvement that the Transport layer has varies with the type of network. For example, if the network consists of a single, dedicated, point-to-point circuit, then very little could happen to the data during the transmission because the data would consist of an uninterrupted, "single-hop" stream. No switches along the way could cause pieces of the message to go awry. The Transport layer therefore would have little to do to guarantee the delivery of the message.

However, what if the architecture of the network is not as robust as a private line circuit? What if this is a packet network, in which case the message is broken into segments by the Transport layer which are independently routed through the fabric of the network? Furthermore, what

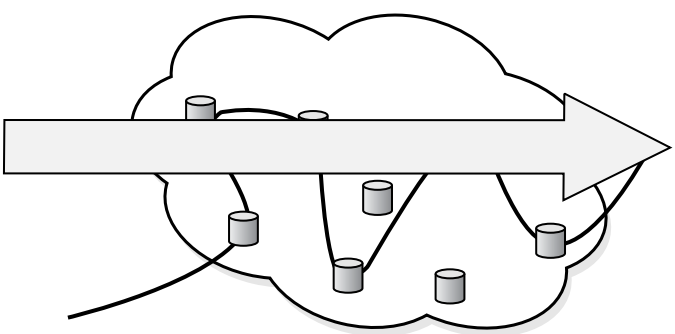


Figure 2-24
VPN.

if there is no guarantee that all of the packets will take the same route through the network wilderness? In that case, the route actually consists of a *series* of routes between the switches, like a string of sausage links. In this situation, the components of the message are not guaranteed to arrive in sequence. In fact, there is no guarantee that they will arrive at all! The Transport layer therefore has a major responsibility to ensure that all of the message components arrive, and that they carry enough additional information in the form of yet another header, this time on each packet, to enable them to be properly resequenced at the destination. The header, for example, contains sequence numbers that the receiving Transport layer can use to reassemble the original message from the stream of random packets.

Consider the following scenario. A transmitter fires a message into the network, where it passes through each of the upper layers until it reaches the originating Transport layer, which segments the message into a series of five packets, labeled one of five, two of five, three of five, and so on. The packets enter the network and proceed to make their way across the wilderness of the network fabric. Packets one, two, three, and five arrive without incident, although they do arrive out of order. Packet four unfortunately gets caught in a routing loop in New Mexico. The receive Transport layer, tasked with delivering a complete, correct message to the layers above, puts everything on hold while it awaits the arrival of the errant packet. The layer, however, will only wait so long. It has no idea where the packet is. It does, however, know where it is *not*. After some predetermined period of time, the receive Transport layer assumes that the packet isn't going to make it and initiates recovery procedures that result in the retransmission of the missing packet.

Meanwhile, the lost packet has finally stopped and asked for directions, extricated itself from the traffic jams of Albuquerque, and made its way to the destination. It arrives, covered with dust, an "I've Seen Crystal Caverns" bumper sticker on its trailer, expecting to be incorporated into the original message. By this time, however, the packet has been replaced with the resent packet. Clearly, some kind of process must be in place to handle duplicate packet situations, which happen rather frequently. The Transport layer then becomes the center point of message integrity.

Transport-layer standards are diverse and numerous. ISO, the ITU-T, and the IETF publish recommendations for layer four. The ITU-T publishes X.224 and X.234, which detail the functions of both connection-oriented and connectionless networks. ISO publishes ISO 8073, which defines a Transport protocol with five layers of functionality ranging from TP0 through TP4:

- **Class 0 (TP0)** Simple class
- **Class 1 (TP1)** Basic error recovery class
- **Class 2 (TP2)** Multiplexing class
- **Class 3 (TP3)** Error recovery and multiplexing class
- **Class 4 (TP4)** Error detection and recovery class

TP0 has the least capability. It is roughly equivalent to the IETF's *User Datagram Protocol* (UDP), which will be discussed a bit later. TP4 is the most common ISO Transport layer protocol and is equivalent in capability to the IETF's *Transmission Control Protocol* (TCP). It provides an iron-clad transport function and operates under the assumption that the network is wholly unreliable and must therefore take extraordinary steps to safeguard the user's data.

Switching and Routing

Before we descend into the wilds of the Network layer, let's introduce the concepts of switching and routing.

Modern networks are often represented as a cloud filled with boxes representing switches or routers. Depending upon such factors as congestion, cost, number of hops between routers and other considerations, the network selects the optimal end-to-end path for the stream of packets created by the Transport layer. Depending upon the nature of the Network layer protocol that is in use, the network will take one of two actions. It will either establish a single path over which all the packets will travel in sequence, or the network will simply be handed the packets and told to deliver them as it sees fit. The first technique, which establishes a seemingly dedicated path, is called *connection-oriented service*; the other technique, which does *not* dedicate a path, is called *connectionless service*. We will discuss each of these in turn. Before we do, however, let's discuss the evolution of switched networks.

Switched Networks

Modern switched networks typically fall into one of two major categories: *circuit-switched*, in which the network preestablishes a path for the transport of traffic from a source to a destination, as is done in the traditional telephone network, or *store-and-forward networks*, where the traffic is handed from one switch to the next as it makes its way

across the network fabric. When traffic arrives at a switch in a store-and-forward network, it is stored, examined for errors and destination information, and forwarded to the next hop along the path, hence the name, store and forward. Packet switching is one form of store-and-forward technology.

Store-and-Forward Switching

> *Thus, from some far-away and beleaguered island, where all day long the men have fought a desperate battle from their city walls, the smoke goes up to heaven; but no sooner has the sun gone down than the light from the line of beacons blazes up and shoots into the sky to warn the neighboring islanders and bring them to the rescue in their ships.*
>
> *The Iliad* by Homer, circa 700 B.C.

The first store-and-forward networks were invented and used . . . by the early Greeks and Romans. Indeed, Mycenae learned of the fall of Troy because of a line of signal towers between the two cities that used fire in each tower to transmit information from tower to tower. An opening on the side of each tower could be alternately opened and blocked, and using a rudimentary signaling code, short messages could be sent between them in a short period of time. A message could be conveyed across a large country such as France in a matter of hours, as Napoleon discovered and used to his great advantage.

The earliest *modern* store-and-forward networks were the telegraph networks. When a customer handed over a message in the form of a yellow paper flimsy that was to be transmitted, the operator would transmit the message in code over the open wire telegraph lines to the next office, where the message printed out on a streaming paper tape. On the tape would appear a sequence of alternating pencil marks and gaps, or spaces, combinations of which represented characters. A mark represented a one, while a space represented a zero. A point of historical interest is that the terms "mark" and "space" are common in modern networks. In T-Carrier, the encoding scheme is called *Alternate Mark Inversion* (AMI), because every other one alternates in polarity from the ones that surround it. Similarly, *Alternate Space Inversion* (ASI) is used in signaling schemes such as on the *Integrated Services Digital Network* (ISDN) D-Channel.

At any rate, the entire message would be delivered in this fashion, from office to office to office, ultimately arriving at its final destination,

a technique called *message switching*. Over time, of course, the process became fully mechanized and the telegraph operators disappeared.

This technique had one major problem. What happened if the message, upon arrival, was found to be corrupt, or if it simply did not arrive for some odd reason? In that case, the entire message would have to be resent at the request of the receiver. This added overall delays in the system and was awfully inefficient since in most cases only a few characters were corrupted. Nevertheless, the entire message was retransmitted. Once the system was fully mechanized, it meant that the switches had to have hard drives on which to store the incoming messages, which added yet more delay since hard drives are mechanical devices and by their very nature relatively slow. Improvements didn't come along until the advent of *packet switching*.

Packet Switching

With the arrival of low-cost, high-speed, solid-state microelectronics in the 1970s, it became possible to take significant steps forward in switching technology. One of the first innovative steps was *packet switching*. In packet switching, the message that was transmitted in its entirety over the earlier message-switched store-and-forward networks is now broken into smaller, more manageable pieces that are numbered by the Transport layer before being passed into the network for routing and delivery.

This innovation offers several advantages. First, it eliminates the need for the mechanical, switch-based hard drive, because the small packets can now be handled blindingly fast by solid-state memory. Second, should a packet arrive with errors, it and it alone can be discarded and replaced. In message-switched environments, an unrecoverable bit error resulted in the inevitable retransmission of the entire message, not a particularly elegant solution. Packet switching, then, offers a number of distinct advantages.

As before, of course, packet switching also has disadvantages. A physically or logically dedicated path no longer (necessarily) exists from the source to the destination, which means that the capability to guarantee QoS on an end-to-end basis is severely restricted. There are ways to work around this, as you will see in the section that follows, but they are often costly and *always* complex.

This QoS problem is one of the reasons that IP telephony is having a difficult time achieving widespread deployment. It works fine in controlled, relatively small corporate environments where traffic patterns

can be scrutinized and throttled as required to maintain QoS. In the public IP environment, however (read *the Internet*), no means exists to ensure that degree of control. Will it work? Of course. Is it dependable? Absolutely not. A customer might be willing to call a friend with it, but they would be less inclined to use the service for a business call—not because it's bad, but because it's not dependable or predictable. Until it is, the old circuit-switched telephone network will continue to enjoy its century (or two) in the sun. The day will certainly come, but for now it isn't ready for prime time.

Packet switching can be implemented in two very different ways. We'll discuss them now.

Connection-Oriented Networks

Capt. Lewis is brave, prudent, habituated to the woods, & familiar with Indian manners & character. He is not regularly educated, but he possesses a great mass of accurate observation on all the subjects of nature which present themselves here, & will therefore readily select those only in his new route which shall be new. He has qualified himself for those observations of longitude & latitude necessary to fix the line he will go over.

Thomas Jefferson to Dr. Benjamin Rush of Philadelphia on why he picked Meriwether Lewis for the Corps of Discovery

Six papers of ink powder; sets of pencils; "Creyons," two hundred pounds of "best rifle powder;" four hundred pounds of lead; 4 Groce fishing Hooks assorted; twenty-five axes; woolen overalls and other clothing items, including 30 yds. Common flannel; one hundred flints; 30 Steels for striking or making fire; six large needles and six dozen large awls; three bushels of salt.

Partial list of items purchased by Lewis for the trip

When Meriwether Lewis (see Figure 2-25) and William Clark left St. Louis with the Corps of Discovery in 1803 to travel up the Missouri and Columbia Rivers to the Pacific Ocean, they had no idea how to get where they were going. They traveled with and relied on a massive collection of maps, instruments, transcripts of interviews with trappers and Native American guides, an awful lot of courage, and the knowledge of Saca-

Figure 2-25
Meriwether Lewis.

jawea, the wife of independent French-Canadian trader Toussaint Charbonneau, who accompanied them on their journey. As they made their way across the wilderness of the northwest, they marked trees every few hundred feet by cutting away a large and highly visible swath of bark, a process known as "blazing," shown in Figure 2-26. By blazing their trail, others could easily follow them without the need for maps, trapper lore, or guides. They did not need to bring compasses, sextants, chronometers, or to hire local guides; they simply followed the well-marked trail.

If you understand this concept, then you also understand the concept of connection-oriented switching, sometimes called *virtual circuit switching,* one of the two principal forms of switching technologies. When a device sends packets into a connection-oriented network, the first packet, often called a *call setup packet* or *discovery packet*, carries embedded in it the final destination address that it is searching for. Upon arrival at the first switch in the network, the switch examines the packet, looks at the destination address, and selects an outgoing port that will get the packet closer to its destination. It has the capability to do this because presumably, somewhere in the recent past, it has recorded the "port of arrival" of a packet from the destination machine, and concludes that if a packet arrived on that port from the destination host, then a good way

Figure 2-26
Blazing the trail.

to get closer to the destination is to go out the same port that the arriving packet came in on. The switch then records in its routing tables an entry that dictates that all packets originating from the same source (the source being a virtual circuit address/physical port address combination that identifies the logical source of the packets) should be transmitted out the same switch port. This process is then followed by every switch in the path, from the source to the destination. Each switch makes table entries, similar to the blazes left by the Corps of Discovery.[12]

With this technique, the only packet that requires a complete address is the initial one that blazes the trail through the network wilderness. All subsequent packets carry nothing more than a short identifier, a virtual circuit address, that instructs each switch that they pass through how to handle them. Thus, all the packets with the same origin will follow the same path through the network. Consequently, they will arrive in order and will all be delayed the same amount of time as they traverse the

[12] The alternative is to have a network administrator manually preconfigure the routes from the source to destination. This guarantees a great deal of control, but it also obviates the need for an intelligent network.

network. The service provided by connection-oriented networks is called a *virtual circuit service*, because it simulates the service provided by a dedicated network. The technique is called connection-oriented because the switches perceive that a relationship, or connection, exists between all of the packets that derive from the same source.

As with most technologies, a connection-oriented transmission has a downside. In the event of a network failure or heavy congestion somewhere along the predetermined path, the circuit is interrupted and will require some form of intervention to correct the problem because the network is not self-healing from a protocol point of view. Certainly, network management schemes and stopgap measures are in place to reduce the possibility that a network failure might cause a service interruption, but in a connection-oriented network, these measures are external. Nevertheless, because of its ability to emulate the service provided by a dedicated network, connection-oriented services are widely deployed and very successful. Examples include Frame Relay, X.25 packet-based service, and ATM. All will be discussed in detail later in the book.

Connectionless Networks

The alternative to connection-oriented switching is *connectionless switching*, sometimes called *datagram service.* In connectionless networks, no predetermined path goes from the source to the destination. Also, no call setup packet exists; all data packets are treated independently, and the switches perceive no relationship between them as they arrive—hence the name "connectionless." Every packet carries a complete destination address, since it cannot rely on the existence of a preestablished path created by a call setup packet.

When a packet arrives at the ingress switch of a connectionless network, the switch examines the packet's destination address. Based on what it knows about the topology of the network, congestion, the cost of individual routes, distance (sometimes called *hop count*), and other factors that affect routing decisions, the switch will select an outbound route that optimizes whatever parameters the switch has been instructed to concern itself with. Each switch along the path does the same thing.

For example, let's assume that the first packet of a message, upon arrival at the ingress switch, would normally be directed out physical

port number seven, because, based upon current known network conditions, that port provides the shortest path (lowest hop count) to the destination. However, upon closer examination, the switch realizes that although port seven provides the shortest hop count, the route beyond the port is severely congested. As a result, the packet is routed out port 13, which results in a longer path but avoids the congestion. Because no preordained route through the network is used, the packet will simply have to get directions when it arrives at the next switch.

Now the second packet of the message arrives. Because this is a connectionless environment, however, the switch does not realize that the packet is related to the packet that preceded it. The switch examines the destination address on the second packet and then proceeds to route the packet as it did with the preceding one. This time, however, upon examination of the network, the switch finds that port seven, the shortest path from the source to the destination, is no longer congested. It therefore transmits the packet on port 7, ensuring that packet two will in all likelihood arrive before packet one. Clearly, this poses a problem for message integrity and illustrates the criticality of the transport layer, which, you will recall, provides end-to-end message integrity by reassembling the message from a collection of out-of-order packets that arrive with varying degrees of delay because of the vagaries of connectionless networks.

Connectionless service is often called *unreliable* because it fails to guarantee delay minimums, sequential deliveries, or, for that matter, any kind of delivery. This causes many people to question why network designers would rely on a technology that guarantees so little. The answer lies within the layered protocol model. Although connectionless networks do not guarantee sequential delivery or limits on delay, they *will* ultimately deliver the packets. Because they are not required to transmit along a fixed path, the switches in a connectionless network have the freedom to route around trouble spots by dynamically selecting alternate pathways, thus ensuring delivery, albeit somewhat unpredictably. If this process results in an out-of-order delivery, no problem: that's what the transport layer is for. Data communications is a team effort and requires the capabilities of many different layers to ensure the integrity and delivery of a message from the transmitter to the receiver. Thus, even an "unreliable" protocol has distinct advantages.

An example of a well-known connectionless protocol is the *Internet Protocol* (IP). It relies on the *Transmission Control Protocol* (TCP), a transport layer protocol, to guarantee end-to-end correctness of the delivered message. Times will occur, however, when the foolproof capabilities of TCP and TCP-like protocols are considered overkill. For exam-

ple, network management systems tend to generate large volumes of small messages on a regularly scheduled basis. These messages carry information about the health and welfare of the network and about topological changes that routing protocols need to know about if they are to maintain accurate routing tables in the switches. The problem with these messages is that they (1) are numerous, and (2) often carry information that hasn't changed since the *last* time the message was generated, 30 seconds ago.

TCP and TP4 protocols are extremely overhead-heavy compared to their lighter-weight cousins UDP and TP0. Otherwise, they would not be able to absolutely, positively guarantee the delivery of the message. In some cases, however, there may not be a need to absolutely, positively guarantee delivery. After all, if I lose one of those status messages, no problem; it will be generated again in 30 seconds anyway. The result of this is that some networks choose not to employ the robust and capable protocols available to them, simply because the marginal advantage they provide doesn't merit the transport and processing overhead they create in the network. Thus, connectionless networks are extremely widely deployed. After all, those 500 million (or so) Internet users must be reasonably happy with the technology.

Let's now examine the Network layer. Please note that we are now entering the realm of the chained layers, which you will recall are used by all devices in the path—end-user devices as well as the switches or routers themselves.

The Network Layer

The Network layer, which is the uppermost of the three chained layers, has two key responsibilities: routing and congestion control. We will also briefly discuss switching at this layer, even though many books consider it to be a layer-two process. So, for the purists in the audience, please bear with me—there's a method to my madness.

When the telephone network first started its remarkable growth path at the sunrise of the twentieth century, no concept of switching existed. If a customer wanted to be able to speak with another customer, he or she had to have a phone at home with a dedicated path to that person's home. Another person required another phone and phone line, and you quickly begin to see where this is leading. Figure 2-27 illustrates the problem; the telephone network's success would bring on the next ice

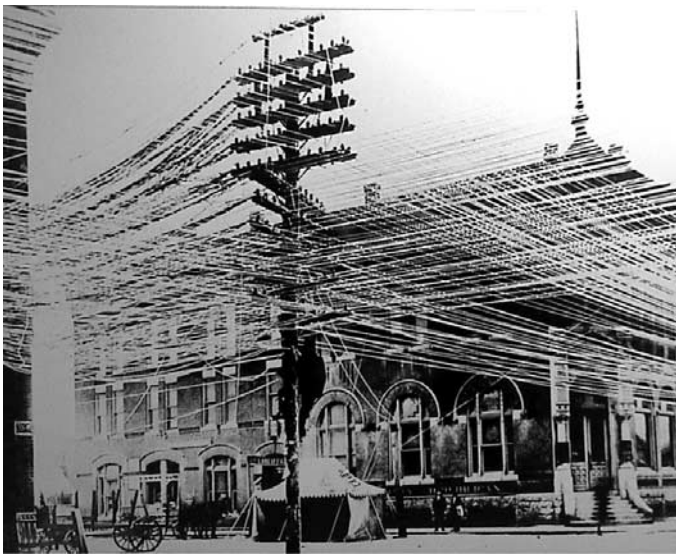


Figure 2-27 Aerial telephone wire (Courtesy Lucent Technologies).

age, blocking the sun with all the aerial wire the telephone network would be required to deploy.

Consider this simple mathematical model. In order to fully interconnect, or mesh, five customers, as shown in Figure 2-28, so that any one of them can call any other, the telephone company would have to install 10 circuits, according to the equation $n(n - 1)/2$, where n is the number of devices that want to communicate. Extrapolate that out now to the population of even a small city, say, 2,000 people. That boils down to 3,997,999 circuits that would have to be installed, all to enable 2,000 people to call each other. Obviously, some alternative solution was greatly needed. That solution was the switch.

The first switches did not arrive until 1878 with the near-disastrous hiring of young boys to work the cord boards in the first central offices. John Brooks, author of *Telephone: The First 100 Years,* offers the following:

> *The year of 1878 was the year of male operators, who seem to have been an instant and memorable disaster. The lads, most of them in their late teens, were simply too impatient and high-spirited for the job, which, in view of the imperfections of the equipment and the inexperience of the subscribers, was one demanding above all patience and calm. According to the late reminiscences of some of them, they were given to lightening the tedium of their work by roughhousing, shouting constantly at each other, and swearing frequently at the customers. An early visitor to the Chicago exchange said of it,*

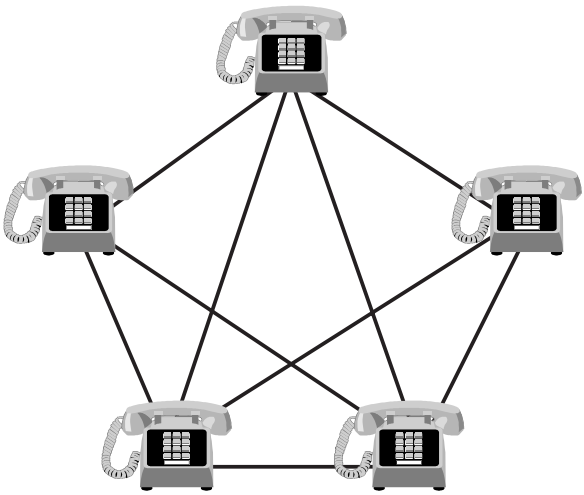


Figure 2-28
Meshed network; 5 users, 10 circuits.

"The racket is almost deafening. Boys are rushing madly hither and thither, while others are putting in or taking out pegs from a central framework as if they were lunatics engaged in a game of fox and cheese. It was a perfect bedlam."

Later in 1878, the boys were grabbed by their ears and removed from their operator positions. They were replaced quickly, to the enormous satisfaction of the customers according to a multitude of accounts, by women, shown in Figure 2-29.

These operators were, in fact, the first switches. Now, instead of needing a dedicated circuit running from every customer to every other customer, each subscriber needed a single circuit that ran into the central exchange, where it appeared on the jack field in front of an operator (each operator managed approximately 100 lines, the optimum number according to Bell System studies). When a customer wanted to make a call, they would crank the handle on their phone, generating a current that would cause a flag to drop, a light to light, or a bell to ring in front of the operator. Seeing the signal, the operator would plug a headset into the customer's jack appearance and announce that they were ready to receive the number to be dialed. The operator would then simply "cross-connect" the caller to the called party, and then wait for the receiver to be picked up on the other end. The operator would periodically monitor the call and pull the patch cord down when the call was complete.

This model meant that instead of needing 3,997,999 circuits to provide universal connectivity for a town of 2,000 people, 2,000 were needed.

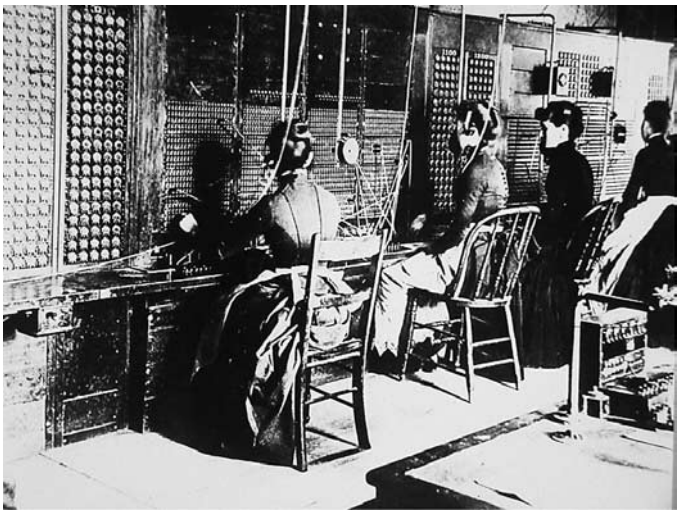


Figure 2-29 First women operators (Courtesy Lucent Technologies).

A rather *significant* reduction in capital outlay for the telephone company, wouldn't you say? Instead of looking like Figure 2-28, the network now looked like Figure 2-30.

Over time, manual switching slowly disappeared, replaced by mechanical switches followed by more modern all-electronic switches. The first true mechanical switches didn't arrive until 1892 when Almon Strowger's Step-by-Step switch was first installed by his company, Automatic Electric.

Strowger's story is worth telling, because it illustrates the serendipity that characterized so much of this industry's development. It seems that Almon Strowger was not an inventor, nor was he a telephone person. He was, in fact, an undertaker in a small town in Missouri. One day, he came to the realization that his business was (OK, I won't say dying) declining and upon closer investigation determined that the town's operator was married to his competitor. As a result, any calls that came in for the undertaker naturally went to her husband, and *not* to Strowger.

To equalize the playing field, Strowger called upon his considerable talents as a tinkerer and designed a mechanical switch and dial telephone, shown in Figure 2-31, which is still in use today in a number of developing countries.

The bottom line to all this is that switches create temporary end-to-end paths between two or more devices that want to communicate with each other, which is accomplished in a variety of ways. Circuit-switched networks create a "virtually dedicated path" between the two end points

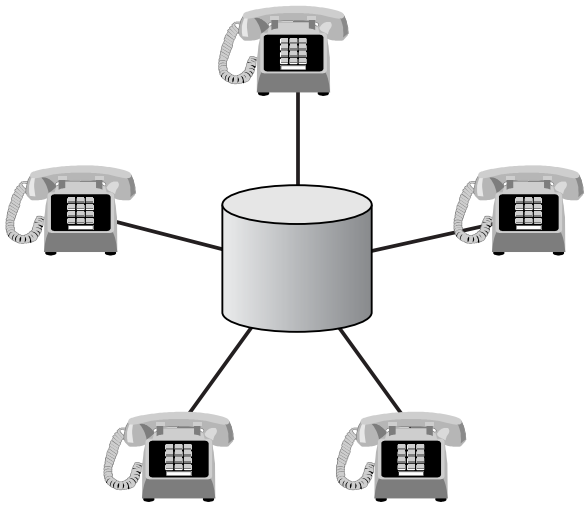


Figure 2-30
Switched network; five users, five circuits.

Figure 2-31
Strowger dial telephone.

and offer constant end-to-end delay, making them acceptable for delay-sensitive applications or connections with long hold times. Store-and-forward networks, particularly packet networks, work well for short, bursty messages with minimal delay sensitivity.

Managing all this, however, is more complicated than it would seem at first blush. First of all, the switches must have the capability to select not

only a path, but the *best* path, based on QoS parameters. This constitutes intelligent routing. Second, they should have some way of monitoring the network so that they always know its current operational conditions. Finally, should they encounter unavoidable congestion, the switches should have one or more ways to deal with it.

Routing Protocols

So, how are routing decisions made in a typical network? Whether connectionless or connection-oriented, the routers and switches in the network must take into account a variety of factors to determine the best path for the traffic they manage. These factors fall into a broad category of rule sets called *routing protocols*. For reference purposes, please refer to the "tree" shown in Figure 2-32.

Once the Transport layer has taken whatever steps are necessary to prepare the packets for their transmission across the network, they are passed to the Network layer.

The Network layer has two primary responsibilities in the name of network integrity: *routing* and *congestion control*. Routing is the process of intelligently selecting the most appropriate route through the network for the packets. Congestion control is the process that ensures that the packets are minimally delayed (or at least equally delayed) as they make their way from the source to the destination. We will begin with a discussion of routing.

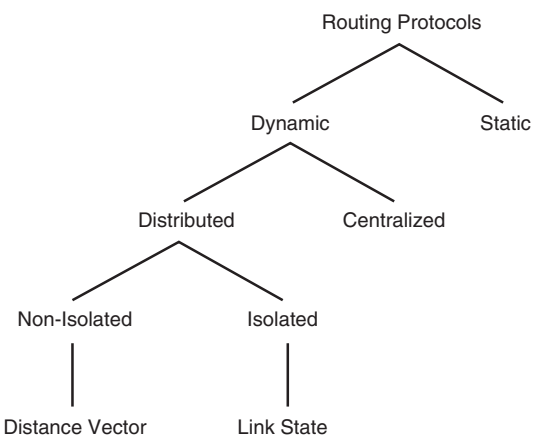


Figure 2-32 Routing Protocol Overview.

Routing Protocols

Routing protocols are divided into two main categories: *static routing protocols* and *dynamic routing protocols*. Static routing protocols are those that require a network administrator to establish and maintain them. If a routing table change is required, the network administrator must manually make the change. This ensures absolute security, but is labor-intensive and therefore less frequently used other than in highly secure environments (military or health care) or network architectures that are designed around static routing because the routes are relatively stable anyway (such as IBM's *Systems Network Architecture* [SNA] for example).

More common are dynamic routing protocols, where network devices make their own decisions about optimum route selection. They do this in the following general way: they pay attention to the network around them and collect information from their neighbors about the best routes to particular destinations based on such parameters as the least number of hops, least delay, lowest cost, or highest bandwidth. The network devices then archive those bits of information in tables and selectively flush the tables periodically to ensure that the information contained in them is always as current as possible. Because dynamic routing protocols assume intelligence in the switch and can therefore reduce the amount of human intervention required, they are commonly used and are, in fact, the most widely deployed routing protocols.

Dynamic routing protocols are further divided into two subcategories: *centralized* and *distributed*. Centralized routing protocols concentrate the route decision-making processes in a single node, thus ensuring that all nodes in the network receive the same and most current information possible. When a switch or router needs routing information that is not contained in its own table, it sends a request to the root node asking for direction. This technique has significant downsides, however; by concentrating the decision-making capability in a single node, the likelihood of a catastrophic failure is dramatically increased. If that node fails, the entire network's capability to seek optimal routing decisions fails. Second, because all nodes in the network must go to that central device for routing instructions, a significant choke point can result.

Several options can reduce the vulnerability of a single point of failure. The first, of course, is to distribute the routing function. This conflicts with the concept of centralized routing, but only somewhat. Consider the Internet, for example. It uses a sort of hybrid of centralized and distributed routing protocols in its *Domain Name Server* (DNS)

function. A limited number of devices are tasked with the responsibility of maintaining knowledge of the topology of the network and the location of domains, providing something of a AAA trip-planning service for data packets.

Another option is to designate a backup machine that takes over in the event of a failure of the primary routing machine. This technique, used in the early Tymnet packet networks, relied on the capability of the primary machine to send a "sleeping pill packet" to the backup machine, with these instructions: "Pay attention to what I do, and memorize everything I learn, but just sit in the corner and be a potted plant. Take no action, make no routing decisions—just learn. Let the sleeping pill keep you in a semi-comatose state. If, for some reason, I fail, I will stop sending the sleeping pills, at which time you will wake up and take over until I recover." An ingenious technique, but overly complex and far too failure-prone for modern network administrators. Distributed routing protocols are far more common today.

In distributed routing protocol environments, each device collects information about the topology of the network and makes independent routing decisions based upon the information it accumulates. For example, if a router sees a packet from source X arrive on port 12, it knows that somewhere out port 12 it will find destination X. It doesn't know how far out there necessarily, just that the destination is somewhere out there over the digital horizon. Thus, if a packet arrives on another port looking to be transmitted to X, the router knows that by sending the packet out port 12 it will at least get closer to its destination. It therefore makes an entry in its routing tables to that effect, so that the next time a packet arrives with the same destination, the switch can consult its table and route the packet quickly.

These routing protocols are analogous to the process of stopping and asking for directions on a road trip (or not), reputedly one of the great male-female differentiators, right after who controls the TV remote. Anthropologists must have a field day with this kind of stuff. According to apocryphal lore, women have no problem whatsoever stopping and asking for directions, while men are loathe to do it—one of those silly threats to the manhood things. Anyway, back to telecomm. If you were planning a road trip across the country, you could do so using one of two philosophies. You could go to AAA or a travel agent and have them plan out the entire route for you, or you could do the Jack Kerouac thing and simply get in the car and drive. Going to AAA seems to be the simplest option because once the route is planned, all you have to do is follow the directions—Lewis' blazed trail, as it were. The downside is that if you

make it as far as Scratch Ankle, Alabama (yes, it's a real place) and the road over which you are supposed to travel is closed, you are stuck. You have to stop and ask for directions anyway.

The alternative is to simply get in the car, drive to the nearest gas station, and tell them that you are trying to get to Dime Box, Texas. The attendant will no doubt tell you the following: "I don't know where Dime Box is, but I know that Texas is down in the southwest. So if you take this highway here to Kansas City, it'll get you closer. But you'll have to ask for better directions when you get there." The next gas station attendant may tell you, "Well, the quickest way to central Texas is along this highway, but it's rush hour and you'll be stuck for days if you go that way. I'd take the surface street. It's a little less comfortable, but there's no congestion." By stopping at a series of gas stations as you traverse the country and asking for help, you will eventually reach your destination, but the route may not be the most efficient. That's okay, though, because you will never have to worry about getting stuck with bad directions. Clearly, the first example of these is connection-oriented; the second is connectionless. Connection-oriented travel is a far more comfortable, secure way to go; connectionless is riskier, less sure, more flexible, and much more fun. Obviously, distributed routing protocols are centrally important to the traveler as well as to the gas station attendant who must give them reliable directions. They are also equally important to routers and switches in connectionless data networks.

Distributed routing protocols fall into two categories: *distance vector* and *link state*. Distance vector protocols rely on a technique called *table swapping* to exchange information about network topology with each other. This information includes destination/cost pairs that enable each device to select the least cost route from one place to another. On a scheduled basis, routers transmit their entire routing tables on all ports to all adjacent devices. Each device then adds any newly arrived information to its own tables, thus ensuring currency.

The only problem with this technique is that it results in a tremendous amount of management traffic (the tables) being sent between network devices, and if the network is relatively static—that is, changes in topology don't happen all that often—then much of the information is unnecessary and can cause serious congestion. In fact, it is not uncommon to encounter networks that have more management traffic traversing their circuits than actual user traffic. What's wrong with this picture? Distance vector works well in small networks where the number of multihop traverses is relatively low, thus minimizing the impact of its bandwidth-intensive nature.

Distance vector protocols have that name because of the way they work. Recovering physicists will remember that a vector is a measure of something that has both direction and magnitude associated with it. The name is appropriate in this case, because the routing protocol optimizes on a direction (port number) and a magnitude (hop count).

Because networks are growing larger, traffic routinely encounters route solutions with large hop counts. This reduces the effectiveness of distance vector solutions. A better solution is the link state protocol. Instead of transmitting entire routing tables on a scheduled basis, link state protocols use a technique called *flooding* to only transmit changes that occur to adjacent devices *as they occur*. This results in less congestion and a more efficient use of network resources, and it reduces the impact of multiple hops in large-scale networks.

Both distance vector and link state protocols are in widespread use today. The most common distance vector protocols are the *Routing Information Protocol* (RIP) and Cisco's *Interior Gateway Routing Protocol* (IGRP) and *Border Gateway Protocol* (BGP). Link state protocols include *Open Shortest Path First* (OSPF), commonly used on the Internet, as well as the *Netware Link Services Protocol* (NLSP), used to route *Internetwork Packet Exchange* (IPX) traffic.

Clearly, both connection-oriented and connectionless transport techniques, as well as their related routing protocols, have a place in the modern telecommunications arena. As QoS becomes such a critical component of the service offered by network providers, the importance of both routing and congestion control becomes apparent. We now turn our attention to the second area of responsibility at the network layer, *congestion control*.

Congestion Control

At its most fundamental level, congestion control is a mechanism for reducing the volume of traffic on a particular route through some form of load-balancing. No matter how large, diverse, or capable a network is, some degree of congestion is inevitable. It can result from sudden unexpectedly high utilization levels in one area of the network, from failures of network components, or from poor engineering. In the telephone network, for example, the busiest calling day of the year in the United States is Mother's Day. To reduce the probability that a caller will not be able to complete a call to Mom, network traffic engineers take extraordi-

nary steps to load-balance the network. For example, when subscribers on the East Coast are making long-distance calls at 9:00 in the morning, West Coast subscribers haven't even turned on their latte machines yet. Network resources in the West are underutilized during that period, so engineers route East Coast traffic westward and then hairpin it back to its destination to spread the load across the entire network. As the day gets later, they reduce the volume of westward-bound traffic to ensure that California has adequate network resources for its own calls.

Two terms are important in this discussion. One is congestion; the other is delay. The terms are often used interchangeably, but they are not the same thing.

Years ago I lived in the San Francisco area where traffic congestion is a way of life. I often had to drive across the many bridges that criss-cross San Francisco Bay, the Suisun Straits, or the Sacramento River. Many of those bridges require drivers to stop and pay a toll, resulting in localized delay. The time it takes to stop and pay the toll is mere seconds, yet traffic often backs up for miles as a result of this local phenomenon.

This is the relationship between the two: local delay often results in widespread congestion, and congestion is usually caused by inadequate buffer or memory space. Increase the number of buffers—the lanes of traffic on the bridge, if you will—and congestion drops off. Open another line or two at Home Depot ("No waiting on line seven!") and congestion drops off.

The various players in the fast food industry manage congestion in different ways, and with dramatically different results. Without naming them, some use a single queue with a single server to take orders, a technique that works well until the lunch rush begins. Then things back up dramatically. Others use multiple queues with multiple servers, a technique that is better except that one queue can experience serious delays should someone place an order for a nonstandard item or try to pay with a credit card. That line then experiences serious delay. The most effective restaurants stole an idea from the airlines and use a single queue with multiple servers. This keeps things moving because the instant a server is available, the next person in line is served.

Remember when Jeff Goldblum, the chaos theoretician in *Jurassic Park,* talked about the Butterfly Effect? How a butterfly flapping its wings in the Amazon Basin can kick off a chain of events that affects weather patterns in New York City? That aspect of Chaos Theory contributes greatly to the manner in which networks behave, and the degree to which their behavior is immensely difficult to predict under a load.

So how is congestion handled in data networks? The simplest technique, used by both Frame Relay and ATM, is called packet discard, shown in Figure 2-33. In the event that traffic gets too heavy based on preestablished management parameters, the switches simply discard excess packets. They can do this because of two facts: first, networks are highly capable and the switches rarely have to resort to these measures; second, the devices on the ends of the network are intelligent and will detect the loss of information and take whatever steps are required to have the discarded data resent. As drastic as this technique seems, it is not all that catastrophic. Modern networks are heavily dependent on optical fiber and highly capable digital switches. As a result, packet discard, while serious, does not pose a major problem to the network. And even when it is required, recovery techniques are fast and accurate.

Because congestion occurs primarily as the result of inadequate buffer capacity, one solution is to preallocate buffers to high-priority traffic. Another is to create multiple queues with varying priority levels. If a voice or video packet arrives that requires high-priority, low-delay treatment, it will be deposited into the highest priority queue for instantaneous transmission. This technique holds great promise for the evolving all-services Internet, because it's greatest failing is its inability to deliver multiple, dependable, sustainable grades of service quality.

Other techniques are available that are somewhat more complex than packet discard, but do not result in loss of data. For example, some devices, when informed of congestion within the network, will delay a transmission to give the network switches time to process their overload

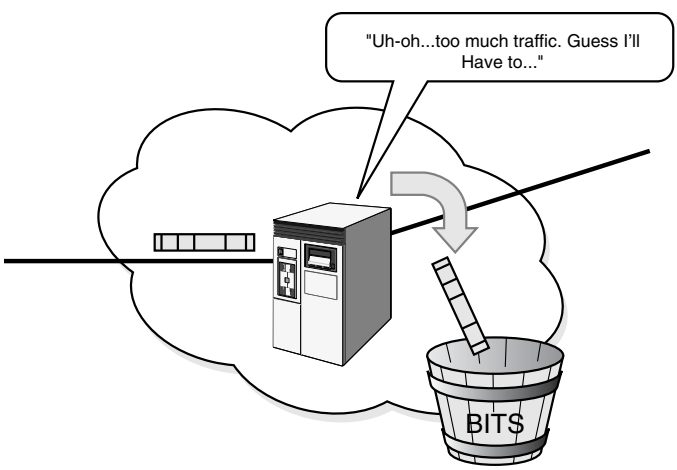


Figure 2-33 Congestion control with packet discard.

before receiving more. Others will divert traffic to alternate, less-congested routes, or "trickle" packets into the network, a process known as *choking* (see Figure 2-34). Frame relay, for example, has the capability to send what is called a *choke packet* into the network, implicitly telling the receiving device that it should throttle back to reduce congestion in the network. Whether it does or not is another story, but the point is that the network has the intelligence to invoke such a command when required. This technique is now used on freeways in large cities. Traffic lights are installed on major onramps that meter the traffic onto the roadway. This results in a dramatic reduction in congestion. Other networks have the intelligence to diversely route traffic, thus reducing the congestion that occurs in certain areas.

Clearly, the Network layer provides a set of centrally important capabilities to the network itself. Through a combination of network protocols, routing protocols, and congestion control protocols, routers and switches provide granular control over the integrity of the network.

Back to the E-Mail Message

Let us return now to our e-mail example. The message has been divided into packets by the Transport layer and delivered in pieces to the Network layer, which now takes whatever steps are necessary to ensure that the packets are properly addressed for efficient delivery to the destination. Each packet now has a header attached to it that contains routing information and a destination address. The next step is to get the packet

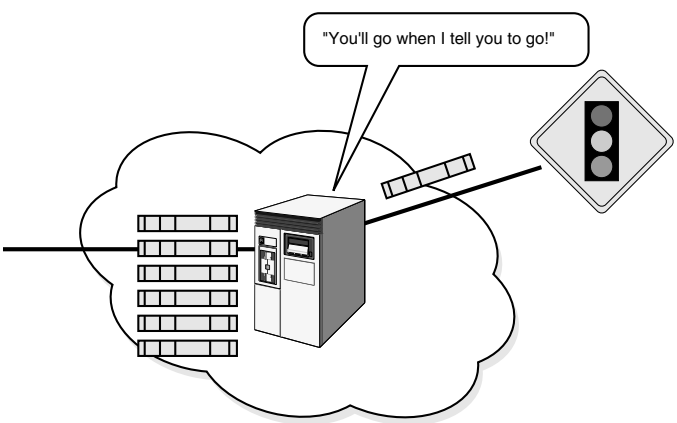


Figure 2-34 *Congestion control using throttling.*

correctly to the next link in the network chain; in this case, it is the next switch or router along the way. This is the responsibility of the Data Link layer.

The Data Link Layer

The Data Link layer is responsible for ensuring bit-level integrity of the data being transmitted. In short, its job is to make the layers above believe that the world is an error-free and perfect place. When a packet is handed down to the Data Link layer from the Network layer, it wraps the packet in a *frame*. In fact, the Data Link layer is sometimes called the *frame layer*. The frame built by the Data Link layer comprises several fields, shown graphically in Figure 2-35, that give the network devices the capability to ensure bit-level integrity and proper delivery of the packet, now encased in a frame, *from switch to switch*. Please note that this is different from the Network layer, which concerns itself with routing packets *to the final destination*. Even the addressing is unique. Packets contain the address of the ultimate destination, used by the network to route the packet properly, and frames contain the address of the next link in the network chain (the next switch), used by the network to move the packet along, switch by switch.

As the figure illustrates, the beginning and end fields of the frame are called *flags*. These fields, made up of a unique series of bits (0111110), can only occur at the beginning and end of the frame[13]; they are never allowed to occur within the bitstream inside the frame through a process that we will describe momentarily. These flags are used to signal to a receiving device that a new frame is arriving or that it has reached the end of the current frame, which is why their unique bit pattern can never be allowed

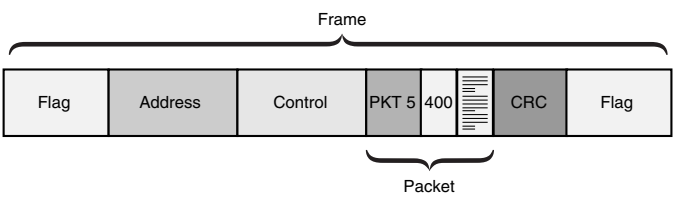


Figure 2-35 Data Link Layer frame.

[13] Indeed, the final flag of one frame is often the beginning flag of the *next* frame.

to occur naturally within the data itself because it could indicate to the receiver (falsely) that this is the end of the current frame. If the flag pattern *does* occur within the bitstream, it is disrupted by the transmitting device through a process called *bit stuffing* or *zero-bit insertion*, in which an extra zero is inserted in the middle of the flag pattern, based on the following rule set.

When a frame of data is created at an originating device, the very last device to touch the frame—indeed, the device that actually adds the flags—is called a *Universal Synchronous/Asynchronous Receiver-Transmitter* (USART). The USART, sometimes called an *Integrated Data Link Controller* (IDLC), is a chipset that has a degree of embedded intelligence. This intelligence is used to detect (among other things) the presence of a false flag pattern in the bitstream around which it builds the frame. Since a flag comprises a zero followed by six ones and a final zero, the IDLC knows that it can never allow that particular pattern to exist between any two real flags. So, as it processes the incoming bitstream, it looks for that pattern and makes the following decision: *If I see a zero followed by five ones, I will automatically and without question insert a zero into the bitstream at that point.* This is illustrated in Figure 2-36.

This, of course, destroys the integrity of the message, but it doesn't matter. At the receive device, the IDLC monitors the incoming bits. As the frame arrives, it sees a *real* flag at the beginning of the frame, an indication that a frame is beginning. As it monitors the bits flowing by, it *will* find the 0 followed by 5 bits, at which point it knows, beyond a shadow of a doubt, that the very next bit is a 0, which it will promptly remove, thus restoring the integrity of the original message.

The receiving device has the ability to detect the extra zero and remove it before the data moves up the protocol stack for interpretation. This bit-stuffing process guarantees that a "false flag" will never be interpreted as a final flag and be acted upon in error.

The next field in the frame is the *address field*. This field identifies the address of the next switch in the chain to which the frame is directed, and changes at every node. The only address that remains constant is the destination address, safely embedded in the packet itself.

Figure 2-36 Bit stuffing or zero bit insertion.

The third field found in many frames is called the *control field*. It contains supervisory information that the network uses to control the integrity of the data link. For example, if a remote device is not responding to a query from a transmitter, the control field can send a "mandatory response required" message that will enable it to determine the nature of the problem at the far end. It is also used in hierarchical multipoint networks to manage communications functions. For example, a multiplexer may have multiple terminal devices attached to it, all of which routinely transmit and receive data. In some systems, only a single device is allowed to "talk" at a time. The control field can be used to force these devices to take turns. This field is optional; some protocols do not use it.

The final field we will cover is the *Cyclic Redundancy Check* (CRC) field. The CRC is a mathematical procedure used to test the integrity of the bits within each frame. It does this by treating the zeroes and ones of data as a binary number (which, of course, it is), instead of as a series of characters. It divides the "number," shown in Figure 2-37, by a carefully crafted polynomial value that is designed to *always* yield a remainder following the division process. The value of this remainder is then placed in the CRC field and transmitted as part of the frame to the next switch. The receiving switch performs the same calculation and then compares the two remainders.

As long as they are the same, the switch knows that the bits arrived unaltered. If they are different, the received frame is discarded and the transmitting switch is ordered to resend the frame, a process that is repeated until the frame is received correctly. This process can result in transmission delay, because the Data Link Layer will not enable a bad frame to be carried through the network. Thus, the Data Link layer converts errors into delays.

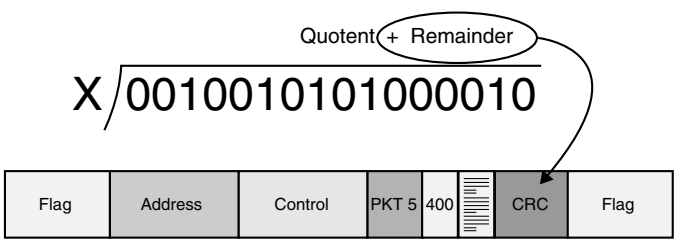


Figure 2-37 CRC-based bit-level error control.

Error Recovery Options

A number of commonly used techniques enable receiving devices to recover from bit errors. The simplest of these is frame discard, the technique used by Frame Relay and ATM networks. In frame discard environments, an errored frame is simply discarded, period. No other form of recovery takes place within the network. Instead, the end devices (the originator and receiver) have the end-to-end responsibility to detect that a frame is missing and take whatever steps are necessary to generate a second copy. The reasons for this strategy will be discussed in the section on fast packet services.

A second common technique is called *forward error correction* (FEC). FEC is used when (1) no backward channel is available over which to request the resend of an errored packet, or (2) the transit delay is so great that a resend would take longer than the application would allow, such as in a satellite hop over which an application is transmitting delay-sensitive traffic. Instead, FEC systems transmit the application data with additional information that enables a receive device to not only determine that an error has occurred, but to fix it. No resend is required.

The third and perhaps most common form of error detection and correction is called *detect and retransmit.* Detect and retransmit systems use the CRC field to detect errors when they occur. The errored frames are then discarded, and the previous switch is ordered to resend the errored frame. This implies a number of things: the frames must be numbered, some positive and negative acknowledgment system must be in place, the transmitter must keep a copy of the frame until its receipt has been acknowledged, and there must be some facility in place to allow the receiver to communicate upstream to the transmitter.

Two recovery techniques are commonly utilized in synchronous systems. To understand them, we must first introduce a couple of transmission protocols used to meter the transmission of frames between switches.

In early communications systems (back in the 1970s), the network was known to be relatively hostile to data transmissions. After all, if noise occurred during a voice conversation, no problem; it was a simple matter to ignore it, provided it wasn't too bad. In data, however, a small amount of noise could be catastrophic, easily capable of destroying a long series of frames in a few milliseconds. As a result, early data systems such as IBM's *Binary Synchronous Communications* (BISYNC) used a protocol called *Stop-and-Wait* that would only permit a single frame at a

time to be outstanding without acknowledgment from the receiver. This was obviously terribly inefficient, but in those early days was as good as it got. Thus, if a major problem occurred, the maximum number of frames that would ever have to be resent was one.

As time passed and network quality improved, designers got brave and began to allow multiple unacknowledged frames to be outstanding, a process called *pipelining*. In pipelined systems, a maximum *window size* is agreed upon that defines the maximum number of frames that can ever be allowed to be outstanding at any point in time. If the number is reached, the window closes, closing down the pipeline and prohibiting other frames from being transmitted. As soon as one or more frames clear the receiver, that many new frames are allowed into the pipeline by the sliding window. Obviously, this protocol is reliant on the capability to number the frames so that the system knows when the maximum window size has been reached.

OK, back to error recovery. We mentioned earlier that two common techniques are used. The first of these is called *selective retransmit*. In selective retransmit environments, if an error occurs, the transmitter is directed to resend *only the errored frame*. This is a complex technique, but is quite efficient.

The second technique is called *Go Back N*. In Go Back N environments, if an error occurs, the transmitter is directed to go back to the errored frame *and retransmit everything from that frame forward*. This technique is less efficient but is far simpler from an implementation point of view.

Let's look at an example. Let's assume that a transmitter generates five frames, numbered one of five, two of five, three of five, and so on. Now let's assume that frame three arrives and is found to be errored. In a selective retransmit environment, the transmitter is directed to resend frame three, and *only* frame three. In a Go Back N environment, however, the transmitter will be directed to resend everything from frame three going forward, which means that it will send frames three, four, and five. The receiver will simply discard frames four and five.

So, let's review the task of the Data Link layer:

- It frames the packet so that it can be checked for bit errors.
- It provides various line control functions so that the network itself can be managed properly.
- It provides addressing information so that the frame can be delivered appropriately.
- It performs error detection and (sometimes) correction.

Practical Implementations

A number of widely known network technologies are found at the Data Link layer of the OSI Model. These include the access protocols used in modern *local area networks* (LANs), such as *Carrier Sense Multiple Access with Collision Detection* (CSMA/CD, used in Ethernet), and Token Ring. CSMA/CD is a protocol that relies on contention for access to the shared backbone over which all stations transmit, while Token Ring is more civilized; stations take turns sharing access to the backbone. This is also the domain of Frame Relay and ATM technologies, which provide high-speed switching.

Frame Relay is a high-speed switching technology that has emerged as a good replacement for private-line circuits. It offers a wide range of bandwidth and, while switched, delivers service quality that is equivalent to that provided by a dedicated facility. It is advantageous for the service provider to sell Frame Relay because it does not require the establishment of a dedicated circuit, thus making more efficient use of network resources. The only downsides of the technology are that it relies on variable size frames, which can lead to variable delivery delays, and it requires careful engineering to ensure that proper QoS is delivered to the customer. Frame Relay offers speeds ranging from 56K to DS3 and is widely deployed internationally.

ATM has become one of the most important technologies in the service provider pantheon today, because it provides the capability to deliver true, dependable, and granular QoS over a switched network architecture, thus giving service providers the ability to aggregate multiple traffic types on a single network fabric. This means that IP, which is a Network-layer protocol, can be transported across an ATM backbone, enabling the smooth and service-driven migration to an all-IP network. Eventually, ATM's overhead-heavy QoS capabilities will be replaced by more elegant solutions, but until that time comes, it still plays a central role in the delivery of service. We will discuss all of these services in later chapters.

The Physical Layer

Once the CRC is calculated and the frame is fully constructed, the Data Link layer passes the frame down to the *Physical layer*, the lowest layer in the networking food chain. This is the layer responsible for the physical

transmission of bits, which it accomplishes in a wide variety of ways. The Physical layer's job is to transmit the bits, which includes the proper representation of zeroes and ones, transmission speeds, and physical connector rules.

For example, if the network is electrical, then what is the proper range of transmitted voltages required to identify whether the received entity is a zero or a one? Is a one in an optical network represented as the presence of light or the absence of light? Is a one represented in a copper-based system as a positive or as a negative voltage, or both? Also, where is information transmitted and received? For example, if pin two is identified as the transmit lead in a cable, which lead is data received over? All of these physical parameters are designed to ensure that the individual bits are able to maintain their integrity and be recognized by the receiving equipment.

Many transmission standards are found at the Physical layer, including T1, E1, the *Synchronous Optical Network* (SONET), the *Synchronous Digital Hierarchy* (SDH), *Dense Wavelength Division Multiplexing* (DWDM), and the many flavors of the *Digital Subscriber Line* (DSL). T1 and E1 are longtime standards that provide 1.544 and 2.048 Mbps of bandwidth respectively. They have been in existence since the early 1960s and occupy a central position in the typical network. SONET and SDH provide standards-based optical transmission at rates above those provided by the traditional carrier hierarchy. DWDM is a frequency division multiplexing technique that enables multiple wavelengths of light to be transmitted across a single fiber, providing massive bandwidth multiplication across the strand. It will be discussed in detail later in the chapter on optical networking. DSL extends the useful life of the standard copper wire pair by expanding the bandwidth it is capable of delivering as well as the distance over which that bandwidth can be delivered.

OSI Summary

We have now discussed the functions carried out at each layer of the OSI Model. Layers six and seven ensure application integrity, layer five ensures security, and layer four guarantees the integrity of the transmitted message. Layer three ensures network integrity; layer two, data integrity; and layer one, the integrity of the bits themselves. Thus, transmission is guaranteed on an end-to-end basis through a series of proto-

cols that are interdependent upon each other and that work closely to ensure integrity at every possible level of the transmission hierarchy.

So, let's now go back to our e-mail example and walk through the entire process. The Eudora e-mail application running on the PC creates a message at the behest of the human user[14] and passes the message to the Application layer. The Application layer converts the message into a format that can be universally understood as an e-mail message, which in this case is X.400. It then adds a header that identifies the X.400 format of the message.

The X.400 message with its new header is then passed down to the Presentation layer, which encodes it as ASCII, encrypts it using Pretty Good Privacy (PGP), and compresses it using a British Telecom Lempel-Ziv compression algorithm. After adding a header that details all this, it passes the message to layer five.

The Session layer assigns a logical session number to the message, glues on a packet header identifying the session ID, and passes the steadily growing message down to the Transport layer. Based on network limitations and rule sets, the Transport layer breaks the message into 11 packets and numbers them appropriately. Each packet is given a header with address and QoS information.

The packets now enter the chained layers, where they will first encounter the network. The Network layer examines each packet in turn and, based on the nature of the underlying network (connection-oriented? connectionless?) and the congestion status, queues the packets for transmission. After creating the header on each packet, they are handed individually down to the Data Link layer.

The Data Link layer proceeds to build a frame around each packet. It calculates a CRC, inserts a Data Link layer address, inserts appropriate control information, and finally adds flags on each end of the frame. Note that all other layers add a header *only;* the Data Link layer is the only layer that also adds a trailer.

Once the Data Link frame has been constructed, it is passed down to the Physical layer, which encodes the incoming bitstream according to the transmission requirements of the underlying network. For example, if the data is to be transmitted across a T- or E-Carrier network, the data will be encoded using Alternate Mark Inversion and will be transmitted

[14] I specifically note "human user" here because some protocols do not recognize the existence of the human in the network loop. In IBM SNA environments, for example, users are devices or processes that "use" network resources. No humans are involved.

across the facility to the next switch at either 1.544 Mbps or 2.048 Mbps, depending on whether the network is T-1 or E-1.

When the bitstream arrives at the next switch (not the destination), the bits flow into the Physical layer, which determines that it can read the bits. The Physical layer hands the bits up to the Data Link layer, which proceeds to find the flags so that it can frame the incoming stream of data and checks it for errors. If we assume that it finds none, it strips off the Data Link frame surrounding the packet and passes the packet up to the Network layer.

The Network layer examines the destination address in the packet, at which point it realizes that it is not the intended recipient. So, it passes it back to the Data Link layer, which builds a new frame around it, calculating a new CRC and adding a new Data Link layer address as it does so. It then passes the frame back to the Physical layer for transmission. The Physical layer spits the bits out the facility to the next switch, which for our purposes we will assume is the intended destination. The Physical layer receives the bits and passes them to the Data Link layer, which checks them for errors. If it finds an errored frame, it requests a resend, but ultimately receives the frame correctly. It then strips off the header and trailer, leaving the original packet.

The packet is then passed up to the Network layer, which, after examining the packet address, determines that it is in fact the intended recipient of the packet. As a result, it passes the packet up to the Transport layer after stripping off the Network layer header.

The Transport layer examines the packet and notices that it has received packet 3 of 11 packets. Because its job is to assemble and pass entire messages up to the Session layer, the Transport layer simply places the packet into a buffer while it waits for the other 10 packets to arrive. It will wait as long as it has to; it knows that it cannot deliver a partial message because the higher layers are not smart enough to figure out the missing pieces.

Once it has received all 11 packets, the Transport layer reassembles the original message and passes it up to the Session layer, which examines the session header created by the transmitter and notes that this is to be handed to whatever process cares about logical channel number seven. It then strips off the header and passes the message up to the Presentation layer.

The Presentation layer reads the Presentation layer header created at the transmit end of the circuit and notes that this is an ASCII message that has been encrypted using PGP and compressed using BTLZ. It decompresses the message using the same protocol, decrypts the

message using the appropriate public key, and, because it is resident in a mainframe, converts the ASCII message to EBCDIC. Stripping off the Presentation layer header, it hands the message up to the Application layer. The Application layer notes that the message is X.400-encoded and is therefore an e-mail message. As a result, it passes the message to the e-mail application that is resident in the mainframe system.

The process just described happens every time you hit the Send button.

Click.

Other Protocol Stacks

Of course, OSI is not the only protocol model. In fact, for all its detail, intricacy, and definition, it is rarely used in practice. Instead, it serves as a true model for comparing disparate protocol stacks. In that regard, it is unequalled in its value to data communications.

The most commonly deployed protocol stack is that used in the Internet, the so-called *TCP/IP stack*. Instead of seven layers, TCP/IP comprises four. The bottom layer, called the *Network Interface layer*, includes the functions performed by OSI's Physical and Data Link layers. It includes a wide variety of protocols, as shown in Figure 2-38.

The *IP layer* is roughly functionally equivalent to the OSI Model's Network layer. It performs routing and congestion control functions, and, as the figure illustrates, includes some of the protocols we mentioned earlier: RIP, OSPF, and a variety of address conversion protocols.

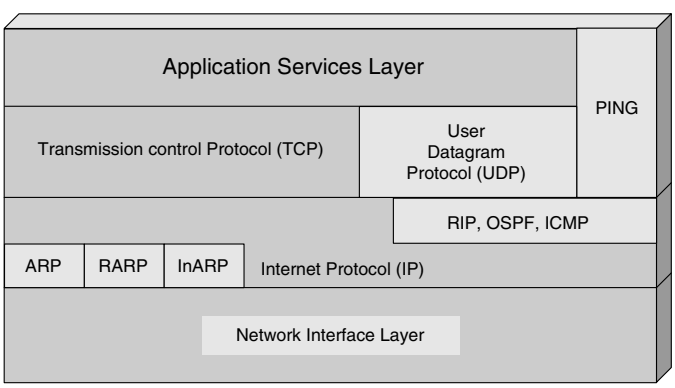


Figure 2-38 The TCP/IP Protocol Suite.

The *Transmission Control Protocol* (TCP) layer is responsible for message integrity, similar to the service provided by OSI's Transport layer. It is extremely capable and has the capability to recover from virtually any network failure imaginable to ensure the integrity of the messages it is designed to protect. For situations where the high degree of protection provided by TCP (and its attendant overhead) is considered to be overkill, a corollary protocol called UDP is also available at this layer. It provides a connectionless network service and is used in situations where the transported traffic is less critical and where the overhead inherent in TCP poses a potential problem due to congestion.

The uppermost layer in the TCP/IP stack is called the *Application Services layer*. This is where the utility of the stack becomes obvious because this is where the actual applications are found such as HTTP, FTP, Telnet, and the other utilities that make the Internet useful to the user.

The point of all these protocols is to give a designer the ability to create a network that will transport the customer's voice, data, video, images, or MP3 files with whatever level of service quality the traffic demands. We now know that data communications protocols make it possible to transport all types of traffic with guaranteed service. Let's turn our attention now to the network itself. In the chapters that follow, we will discuss the history of the most remarkable technological achievement on earth, the telephone network. Later we will discuss the anatomy of a typical data network and the technologies found there.

CHAPTER 3

Telephony

In this chapter we will explore telephony and the telephone network. Described as "the largest machine ever built," the telephone network is an impressive thing. We begin with some history, then explore the network itself, and finally explore telephony service-how it works, how it makes its way across the network, and how it is managed. We will examine the process of voice digitization, followed by the multiplexing and high-speed transport of voice through such technologies as *Pulse Code Modulation* (PCM), *Synchronous Optical Network* (SONET), and *Synchronous Digital Hierarchy* (SDH).

Some people feel that voice is something of an anachronism and has no place in a book about the new, slick world of telecommunications. I disagree; without an understanding of how the voice network operates, it is impossible to understand or appreciate how data networks operate. This chapter is designed to bridge the gap between the two.

We begin our tale in New York City.

Miracle on Second Avenue

February 26th, 1975 was a business-as-usual day at New York Telephone's lower Manhattan switching center. Located at Second Avenue and 13th Street, the massive 11-story building was the telephony nerve center for 12 Manhattan exchanges that provided service to 300 New York City blocks, including 104,000 subscribers and 170,000 telephones. Within the service area were 6 hospitals, 11 firehouses, 3 post offices, 1 police station, 9 schools, and 3 universities. The building was massive, but like most *central offices* (COs), it was completely invisible to the public. It was just a big, windowless structure that belonged to the telephone company. No one really knew what went on in there; nobody cared.

When night fell, most of the building's employees went home, leaving a small crew to handle maintenance tasks and minor service problems. The night was quiet; work in the building was carried out routinely. It was going to be a boring evening.

At 12:30, just after midnight, a relatively inconsequential piece of power equipment in the building's sub-basement cable vault shorted and spit a few errant sparks into the air. It caused no alarms because it didn't actually fail. One of the sparks, however, fell on a piece of insulation and began to smolder. The insulation melted and began to burn, changing from a smoldering spot on the surface of a cable to a full-blown fire. Soon the entire cable vault was aflame.

The cables in a central office were routed from the cable vault to upper-floor switching equipment through six-inch diameter holes cored in the concrete floors of the office. The fire burned its way up the cables, exited the cored holes, and spread from floor to floor. Soon all of the lower floors of the building were engulfed, and New York Telephone was on its way to hosting the single worst disaster that any American telephone company had ever experienced.

Emergency service vehicles converged on the building. They evacuated everyone inside and began flooding the lower floors with hundreds of thousands of gallons of water. Smoke and steam billowed up and out of the structure (see Figure 3-1), severely damaging equipment on the upper floors that had not as yet been affected by the fire.

Two days later the fire was finally out and telco engineers were able to reenter the building to assess the damage. On the first floor, the 240-foot main distribution frame was reduced to a melted puddle of iron. Water had ruined the power equipment in the basement. Four panel-

Figure 3-1 Smoke and steam billow from the 2nd Avenue central office.

switching offices on the lower floors were completely destroyed. Cable distribution ducts between floors were deformed and useless. Carrier equipment on the second floor was destroyed. Switching hardware on the fourth, fifth, and sixth floors was smoke and water-damaged and would require massive restoration and cleaning before they could be used. *And 170,000 telephones were out of service.*

Within an hour of discovering the fire, the Bell System mobilized its forces in a massive effort to restore service to the affected area. New York Telephone, AT&T Long Lines, Western Electric (now Lucent), and Bell Laboratories converged on the building and commandeered a vacant storefront across the street to serve as their base of operations. Lee Oberst, New York City Area Vice-President, coordinated the nascent effort that would last just under a month and cost more than $90 million.

The Bell System, and it really was a system, immediately commissioned a host of parallel efforts to restore the central office. Calling upon the organization's widespread resources, Chairman of the Board John deButts put out an urgent demand for personnel, and within hours 4,000 employees from across the globe descended upon New York City and began to work 12-hour shifts, with 2,000 employees in the building on each shift.

Meanwhile, other efforts were underway. Central office engineers reviewed the original drawings of the building's complex network to determine what they would need in the way of new equipment to restore service. All other *Bell Operating Companies* (BOCs) were placed on indefinite equipment holds pending the restoration of the New York office. Nassau Recycle Corporation, a Western Electric subsidiary, moved in to begin the removal and recycling process of the 6,000 tons of debris that came out of the building, much of it toxic. Mobile telephone subsidiaries from across the country sent mobile radio units to the city to provide emergency telephony services. The units were installed all over the affected area and announcements were posted throughout the city to tell residents where they were located.

Simultaneously, Bell Laboratories scientists studied the impact of the fire and crafted the best technique for cleaning the equipment that could be salvaged. 1,350 quarts of specially formulated cleaning fluid were mixed and shipped to the building along with thousands of toothbrushes and hundreds of thousands of Q-Tips. A high-capacity facility between New York and New Jersey, still in the planning stages, was accelerated, installed, and put into service to carry the traffic that would normally have flowed through the Second Avenue office.

Within 24 hours, miracles were underway. Service had been restored to all affected medical, police, and fire facilities. The day after the fire, a new main distribution frame had been located at Western Electric's Hawthorne manufacturing facility and was shipped by cargo plane to New York. Luckily, the third floor of the building had been vacant and was therefore available as a staging area to assemble and install the 240-foot-long iron frame. Under normal circumstances, from the time a frame is ordered, shipped, and installed in an office, six months elapse. *This frame was ordered, shipped, installed, and wired in four days*.

It is almost impossible to understand the magnitude of the restoration effort, but the following numbers may help. Six thousand tons of debris were removed from the building and 3,000 tons were installed, including 1.2 billion feet of underground wire, 8.6 million feet of frame wire, 525,000 linear feet of exchange cable, and 380 million conductor feet of switchboard cable. Five million underground splices hooked it all together, and 30 trucking companies, 11 airlines, and 4,000 people were pressed into service. Just after midnight on March 21st, 22 days following the fire, service from the building was restored to 104,000 subscribers. Normally, the job would have taken more than a year. But because of the Bell System's remarkable ability to marshal resources during times of crisis, the building was restored in less than a month (see Figure 3-2). AT&T Chairman John DeButts:

> "In the last couple of weeks I have had the opportunity to observe at first hand the strength of the organization structure that the Justice Department's antitrust suit seeks to destroy. This service restoration has been called a dramatic accomplishment—rightly. But only in its urgency does the teamwork demonstrated on this occasion differ from the teamwork that characterizes the Bell System's everyday job."

Of course, the antitrust suit, now known universally as divestiture, went forward as planned, beginning in 1984. The Bell System became a memory, with just as many people hailing its death as mourning it. And although much can be said for the innovation, competitive behavior, and reduced prices for telecommunications services that came from the breakup of the Bell System, it is hard to read an account such as this one without a small lump in the throat. In fact, most technology historians conclude that we could not build the Bell System network today.

To understand the creation of a system that could accomplish something as remarkable as the fire recovery described previously, let's take a few pages to describe the history of this marvelous industry. I think you'll find it rather interesting.

Figure 3-2
Twenty-two days later, the building is restored and ready for service.

The History of Telephony

As early as 1677, inventor Robert Hooke, who formulated the theory of planetary movement, demonstrated that sound vibrations could be transmitted over a piece of drawn iron wire, received at the other end, and interpreted correctly. His work proved to be something of a bellwether and in 1820, 143 years later, Charles Wheatstone transmitted interpretable sound vibrations through a variety of media, including thin glass and metal rods. In 1831, Michael Faraday demonstrated that vibrations such as those made by the human voice could be converted to electrical pulses. Needless to say, this was fundamental to the eventual development of the telephone.

Bernard Finn is the curator of the Smithsonian's National Museum of American History. His knowledge of the world of science and its van-

guard during the heady times of telephony's arrival is unparalleled. He observes that America was a bit of a backwater as far as science went. "The inventive climate of that early part of the century was largely [focused on] mechanical inventions," he notes. "Even the early electrical stuff was basically mechanical and the machine shop was the center of inventive activity."

With the invention of the telegraph, which occurred simultaneously in the United States, England, and Germany in the 1830s, it became possible to communicate immediately across significant distances. By the second half of the 19th Century, three individuals were working on practical applications of Faraday's observations. Alexander Graham Bell, a speech teacher for the hearing impaired, and a part-time inventor; Elisha Gray, the inventor of the telegraph, and an employee of Western Electric; and Thomas Edison, an inventor and former employee of Western Union, were all working on the same problem: how to send multiple simultaneous messages across a single pair of wires. All three invented devices that they called harmonic telegraphs; they were nothing more than frequency division multiplexers, but for the time were remarkably advanced conceptually.

The original devices that they created performed the multiplexing task mechanically by vibrating metallic reeds at different frequencies. The frequencies would pass down the line and be received correctly at the other end. The only problem with this technique was channel separation; because the frequency bands were relatively close to each other, they would eventually interfere with one another, causing problems at the receiving end of the circuit. For a telegraph, harmonic multiplexing was deemed to not be practical.

All three inventors—Gray, Edison, and Bell—were in a dead heat to create the first device that would transport voice across a long-distance network. None of them had really tested their inventions extensively; they had been used in the laboratory only. Nevertheless, on February 14, 1876, Alexander Graham Bell filed a notice of invention on his own untested device. Simultaneously, Elisha Gray filed a notice of invention on his device. Some argument exists as to who filed first; many believe that Gray actually filed first. Whatever the case, three days later Bell became the first person to transmit voice electronically across a network. And in 1877, following numerous experiments and tweaks to his original device, Bell founded the Bell Telephone Company.

Meanwhile, Thomas Edison continued to work on his own device, patented in 1875 and in 1876 was hired by Western Union. The arrival of the telephone was seen as a major problem by the company, but they

had no intention of sitting idly by while Gray and Bell destroyed their business with their new-fangled invention. In 1877, Edison crafted a very good transmitter based on compressed carbon powder (still in widespread use today, by the way; see Figure 3-3) that would eventually replace the far less capable transmitter invented by Bell.

For the experimenters among the readers out there, it's a fun exercise to build a compressed carbon microphone, as shown in Figure 3-4. In a mortar and pestle (OK, a plastic bag and a hammer), grind two charcoal briquettes to a fine powder. Pour the powder into a jar lid until the powder is even with the lip of the lid. Stretch a piece of plastic wrap tightly over the lid and secure it with a rubber band. Next, drill a hole in each side of the lid and insert an insulated wire that has been stripped back about a half-inch to expose the copper wire. Next, connect the wires to a speaker and battery, as shown in the illustration. When you speak into

Figure 3-3 Bell's carbon microphone, still in use today.

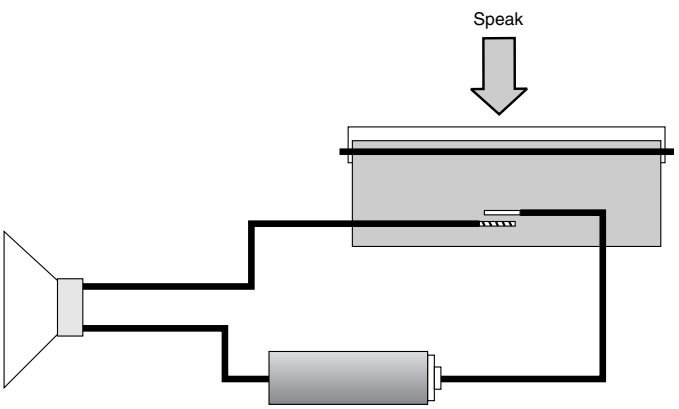


Figure 3-4 Building a simple carbon microphone and telephone.

the "microphone," the sound waves impinging upon the stretched plastic wrap cause the carbon powder to be compressed and expanded, which in turn changes the resistance between the two conductors inserted into the powder.

Naturally, tensions ran high between the Bell Telephone Company and Western Union during this period. In 1877, Bell offered to sell his patent to Western Union for $100,000. They turned down Bell's offer, deciding instead to buy Gray and Edison's patents and form the American Speaking Telephone Company.

Bell sued Western Union for patent infringement in 1878, and the case was settled in 1879 to everyone's satisfaction. Bell won the rights to Western Union's telephone patents, provided he pay royalties for the duration of the 17-year patent life of each device. Meanwhile, Bell Telephone Company agreed to stay out of the telegraph business and Western Union agreed to stay away from telephony.

Once the legal wrangling had ended, telephone service moved along rather quickly. By the spring of 1880, the United States had 138 exchanges and 30,000 subscribers. By 1887, 146,000 miles of wire had been strung to connect 150,000 subscribers to nearly 750 main offices and 44 branch offices.

As we described in Chapter 2, "Protocols," no switches initially existed, so telephones were sold in pairs, one for each end of the connection. Wires were strung in a haphazard fashion attached to the outside of buildings, strung across neighbors' rooftops. Obviously, this one-to-one relationship was somewhat limiting. A technique was needed that would enable one phone to connect to many.

The answer came in the form of the central office. Connections were installed from all the phones in a local area to the central exchange where operators could monitor the lines for service requests. The customer would then tell the operator whom they wanted to speak with, and the operator would set up the call using patch cords. When the parties had finished speaking, they would pull down the patch cord, freeing up the equipment for another call. This entire function was the first form of switching. The design soon became problematic, however, because an operator could typically only monitor about 100 customer positions effectively.

The answer, of course, came with the development of the switch, first with Strowger's invention and later from a series of switching innovations that led to the technology we have today. The first semi-automatic switch was installed in Newark, New Jersey in 1914, and the first truly automatic switch went live in Omaha, Nebraska in 1921. For all this

innovation, however, direct long-distance dialing did not become a reality until 1951.

Soon the network had evolved to a point where it could handle thousands of simultaneous calls. As the technology evolved, so too did the business. In 1892, Alexander Graham Bell inaugurated a 950-mile circuit between New York and Chicago, ushering in the facile ability to carry out long-distance telephony. Meanwhile, the company continued to change; after acquiring Western Electric, it changed its name to *American Telephone and Telegraph* (AT&T), and in an ongoing attempt to protect its fiefdom, began buying up small competitors as they emerged. In 1909, the company purchased a controlling interest in Western Union, thus garnering the attention of the Interstate Commerce Commission, the federal agency responsible (as of 1909) for the oversight of American wire and radio-based communications. That responsibility would later be passed on to the newly created *Federal Communications Commission* (FCC).

In 1913, in the first of a series of anti-trust decisions, the Kingsbury Commitment forced AT&T to divest its holdings in Western Union, stop buying its competition, and provide free interconnections with other network providers. AT&T did not realize it then, but the Kingsbury Commitment was the harbinger of drastic things to come.

In the years that followed, a number of significant technological events took place in telephony. Load coils were created and installed on telephone lines, extending signal strength dramatically and reducing bandwidth requirements for each customer. In 1915, the first amplifiers were installed on long-distance telephone circuits, making it possible to install circuits of essentially an unlimited length. In fact, later that same year, a circuit was successfully installed between New York and San Francisco.

In 1934, President Roosevelt created the FCC with the Communications Act of 1934 being signed into law. This act moved industry oversight from the Interstate Commerce Commission to the FCC, and recognized the importance of telephone service, mandating that it would be both affordable and universal.

By now, AT&T provided local and long-distance services and offered central office equipment and telephones to more than 90 percent of the market. Not surprisingly, that smacked of monopoly to the Federal Government, and from that point on, they were squarely in the FCC's gun sights.

In 1948, AT&T sued the Hush-a-Phone Corporation for manufacturing a device that physically connected to the telephone network. The device, shown in Figure 3-5, was nothing more than a metal box that fit

over the mouthpiece of the telephone, blocking out extraneous noise and providing a degree of privacy to the person using the phone. It had no electrical component to it; it was merely a box. Hush-a-Phone won the case, and the District of Columbia Court of Appeals ruled that AT&T could not prohibit people from making money from devices that did not electrically connect to AT&T's network.

In 1949, the Justice Department filed an anti-trust suit against AT&T and Western Electric. The result was the consent decree of 1956, which enabled AT&T to keep Western Electric, but restricted them to the delivery of common carrier services.

In the early 1960s, inventor Tom Carter created a device called the Carterphone, shown in Figure 3-6. The Carterphone enabled mobile car radios to connect to the telephone network and *did* require electrical connectivity to AT&T. Initially, AT&T prohibited Carter from connecting his device under any circumstances, but when he appealed to the FCC, he was given permission, opening the *Customer-Provided Equipment* (CPE) market for the first time. AT&T's concerns about possible damage to the network were well founded, but by the time AT&T vs. Carter came to trial, the device had been in use for several years and clearly hadn't done any damage whatsoever.

Figure 3-5
Hush-a-Phone.

Figure 3-6
Carterphone.

In 1969, the very next year, the FCC gave MCI permission to offer private line services between St. Louis and Chicago over its privately owned microwave system. Then in 1971, the court extended its 1956 Consent Decree mandate, ordering AT&T to allow non-Bell companies such as MCI to connect directly to their network, ending AT&T's stranglehold on the private line market. The decision was based on a far-reaching FCC policy designed to create nationwide, full-blown competition in the private-line marketplace.

It didn't end there, however. In 1972, the FCC mandated that satellites could be used to transport voice and compete with AT&T, and that value-added carriers could resell AT&T services. In 1977, in the now famous Execunet decision, MCI won a legal battle that allowed them to compete directly with AT&T in the switched long-distance services market, AT&T's bastion of revenue. In 1974, they extended their attack, filing an anti-trust suit against AT&T and charging them with unfairly restricting competition and dominating the marketplace. That same year the Justice Department filed an anti-trust suit of their own, signaling the beginning of the end for the Bell System.

In 1980, another crack appeared in AT&T's armor when the FCC consciously recognized the difference between basic and enhanced services. *Computer Enquiry II* stipulated that basic services would be regulated and therefore tightly controlled. Enhanced services, including CPE, would be deregulated and made completely competitive. AT&T was told

that it could sell enhanced services, but only through fully separate subsidiaries to ensure no mixing of revenues between the two sides of the business.

In 1981, the United States vs. AT&T came to trial in Judge Harold Greene's court. In the months that followed, it became painfully clear to AT&T that it would not win this game. On January 8, 1982, the two sides announced that they had reached a mutually acceptable agreement. The agreement, known as the Modified Final Judgment, stipulated that AT&T would divest itself of its 22 local telephone companies, the Bell Operating Companies. The company would retain ownership of Western Electric, Bell Laboratories, and AT&T Long Lines and would be allowed to enter non-carrier lines of business such as computers and the like. Meanwhile, the BOCs were gathered into seven *Regional BOCs* (RBOCs), tasked with providing local service to the regions they served. The RBOCs were further subdivided into *Local Access and Transport Areas* (LATAs) that defined the areas they were enabled to provide transport within. A state like California, for example, is very large, and the transport of traffic between San Francisco and San Diego, even though the traffic never leaves Pacific Bell territory, clearly travels over a long distance and must therefore be handed off to a long-distance carrier for transport between LATAs.

Although the best-known impact of divestiture was the breakup of AT&T, one result of which was the liberalization of the telecommunications marketplace in the United States, a second decision that was tightly intertwined with the Bell System's breakup was largely invisible to the public, yet it was *at least* as important to AT&T competitors MCI and Sprint as the breakup itself. This decision, known as Equal Access, had one seminal goal: to make it possible for end customers to take advantage of one of the products of divestiture, the ability to select one's long-distance provider from a pool of available service providers, in this case, AT&T, MCI, or Sprint. This, of course, was the realization of a truly competitive marketplace in the long-distance market segment.

To understand this evolution, it is helpful to have a high-level understanding of the overall architecture of the network. In the pre-divestiture world, AT&T was *the* provider for local service, long-distance service, and communications equipment. An AT&T central office therefore was awash in AT&T hardware: switches, cross-connect devices, multiplexers, amplifiers, repeaters, and a myriad of other devices.

Figure 3-7 shows a typical network layout in the pre-divestiture world. A customer's telephone is connected to the service provider's network by a local loop connection (so-called twisted-pair wire). The local

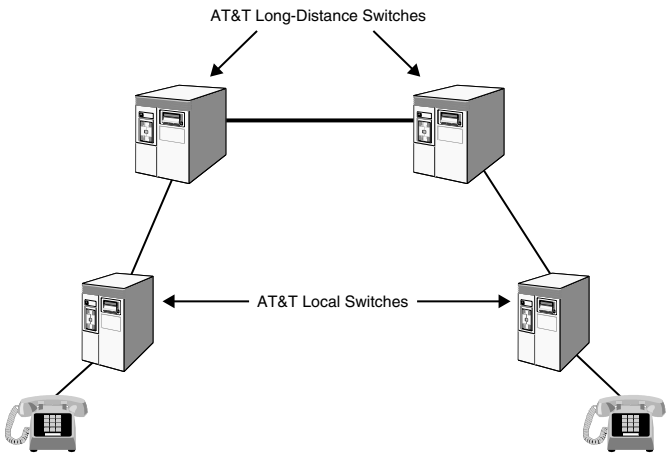


Figure 3-7
Pre-Divestiture connectivity.

loop, in turn, connects to the local switch in the central office. This switch is the point at which customers first touch the telephone network, and it has the responsibility to perform the initial call setup, maintain the call while it is in progress, and tear it down when the call is complete. This switch is called a local switch because its primary responsibility is to set up local calls that originate and terminate within the same switch. It has one other responsibility, though, and that is to provide the necessary interface between the local switch and the long distance switch, so that calls between adjacent local switches (or between far-flung local switches) can be established.

The process, then, goes something like this. When a customer lifts the handset and goes off-hook, a switch in the telephone closes, completing a circuit that enables a current flow, which in turn brings dial tone to the customer's ear. Upon hearing the dial tone, the customer enters the destination address of the call (otherwise known as a telephone number). The switch receives the telephone number and analyzes it, determining from the area code and prefix information whether the call can be completed within the local switch or if it must leave the local switch for another one.

If the call is indeed local, it merely burrows through the crust of the switch and then reemerges at the receiving local loop. If the call is a toll or long-distance call, it must burrow through the hard crunchy coating of the switch, pass through the soft, chewy center, and emerge again on the other crunchy side on its way to a long-distance switch. Keep in mind that the local switch has no awareness of the existence of customers or

telephony capability beyond its own cabinets. Thus, when it receives a telephone number that it is incapable of processing, it hands it off to a higher-order switch, with the implied message, "Here, I have no idea what to do with this, but I assume that you do."

The long-distance switch receives the number from the local switch, processes the call, establishes the necessary connection, and passes the call on to the remote long-distance switch over a long-distance circuit. The remote long-distance switch passes the call to the remote local switch, which rings the destination telephone, and ultimately the call is established.

Please note that in this pre-divestiture example, the originating local loop, local switch, long-distance switch, remote local loop, and all of the interconnect hardware and wiring belong to AT&T. They are all manufactured by Western Electric, based on a set of internal manufacturing standards that, were there other manufacturers in the industry, would be considered proprietary. Because AT&T was the only game in town prior to divestiture, AT&T created the standard for transmission interfaces.

Fast-forward now to January 1, 1984, and put yourself into the mind of Bill McGowan, whose company's very survival depended upon the successful implementation of Equal Access. Unfortunately, Equal Access had one very serious flaw. Keep in mind that because the post-1984 network was emerging from the darkness of monopoly control, all of the equipment that comprised the network infrastructure was bought at the proverbial company store and was, by the way, proprietary.

Consider the newly recreated post-divestiture network model shown in Figure 3-8. At the local-switch level, precious little has changed; at this point in time, still only a single local services provider is available. At the long-distance level, however, a significant change takes place. Instead of a single long-distance service provider called AT&T, there are now three: AT&T, MCI, and Sprint. The competitive mandate of Equal Access was designed to guarantee that a customer could freely select their long-distance provider of choice. If they wanted to use MCI's service instead of AT&T's, a simple call to the local telephone company's service representative would result in the generation of a service order that would cause the customer's local service to be logically disconnected from AT&T and reconnected to MCI so that long-distance calls placed by the subscriber would automatically be handed off to MCI. The problem of "equal access" to customers for the three long-distance providers was solved.

Since 1984, the telecommunications marketplace has continued to evolve, sometimes in strange and unpredictable ways. Harold Greene

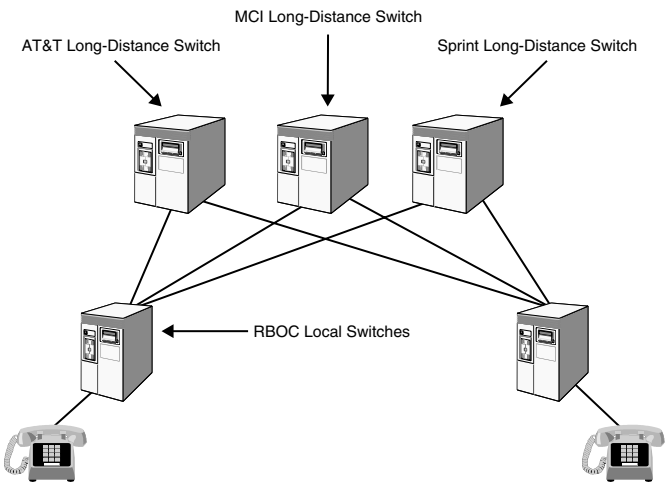


Figure 3-8
Post-Divestiture connectivity.

oversaw the remarkable transformation of the industry until his death in January of 2000. Over time, the seven RBOCs slowly accreted to a smaller number as SBC, Pacific Bell, and Ameritech joined forces, sucking SNET into their midst in the process; NYNEX and Bell Atlantic danced around each other until they became Verizon, pulling GTE into the fray; and Qwest acquired USWest. Only Bellsouth remains as a stand-alone suitor from earlier days, and none of them are called RBOCs anymore; they're *Incumbent Local Exchange Carriers* (ILECs).

A host of new players emerged from the proverbial woodwork including bypassers, which became *Competitive Access Providers* (CAPs), which in turn became *Competitive Local Exchange Carriers* (CLECs). Service, now the favored watchword, has given rise to *Data Local Exchange Carriers* (DLECs), *Building Local Exchange Carriers* (BLECs), *Internet Service Providers* (ISPs), *Application Service Provider* (ASPs), and LSPs. Old-timers remember when the world was fine with just BSPs. (Sorry, inside joke.)

In 1996, the FCC released the Communications Act of 1996, designed to revamp the Communications Act of 1934 and make it more friendly to the services carried by network providers today. It also was designed to address the requests by *Incumbent Local Exchange Carriers* (ILECs) to become long-distance providers within their service areas through a 14-point checklist that they must complete before being considered for entry into the long-distance market. At the time of this writing (July 2001), none of them have complied totally with the

demands, but movement is underway and some of them have been granted limited entry to long distance.

Overall, the market continues to liberalize. Western Electric has ceased to exist, and Lucent has taken its place. The Internet has become the next great technology and service frontier, and both existing and new service providers are leaping at its promises of wealth and riches. Outside the United States, telecom companies once considered to be primitive rival the level of services offered in the United States, and in spite of the telecom meltdown that has plagued the industry of late, innovation continues and new players spring up like early morning mushrooms.

Let's turn our attention now to the network itself.

The Telephone Network

"Sure, I know how it works. You pick up the phone, dial the numbers, and wait. A little man grabs the words, runs down the line, and delivers them to whomever I'm calling. It seems just about that simple. I mean, come on. How complicated can it be? It's just a telephone call."

Thus was described to me the overall process of placing a telephone call by a fellow on the street whom I once interviewed for a video I was creating about telephony. His perception of the telephone network, how it works, and what it requires to work is similar to most people's. Yet the telephone network is without question the single greatest and most complex agglomeration of technology on the planet. It extends its web seamlessly to every country on earth, providing instantaneous communication for not only voice, but for video, data, television, medical images, sports scores, music, high-quality graphics, secure military intelligence, banking information, and teleconferences. Yet it does so with almost complete transparency and with 100-percent availability. The only time its presence is noticed is when it isn't there, as happened on Second Avenue in New York, in Hinsdale, Illinois following a major central office fire, and in Chicago following a flood that isolated the Mercantile Exchange and placed hundreds of customers out of service.

How the network works is something of a mystery to most people, so we're going to dissect the typical telephone network and examine its parts, complete with pictures. This section is not for the squeamish.

The best way to gain an understanding of how the telephone network operates is by studying a modern railroad system. Consider Figure 3-9, which is a route map for the mythical Midland, Amarillo, and Roswell

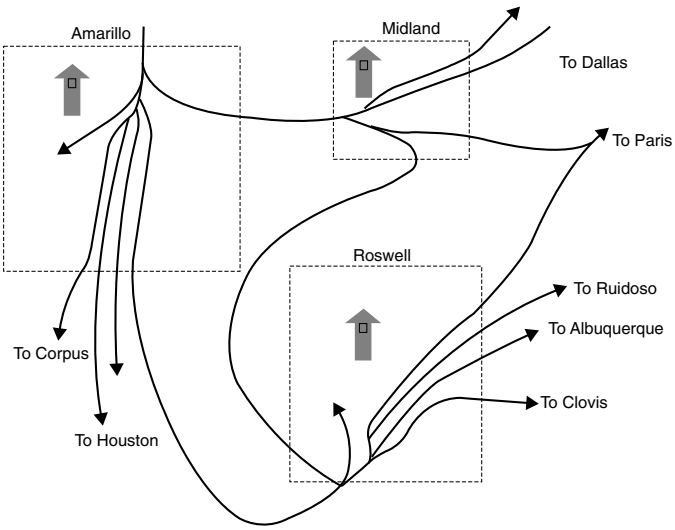


Figure 3-9 *Midland, Amarillo, and Roswell Railroad.*

Railroad. Rail yards in each of the three cities are interconnected by high-volume trunk lines. The train yards, also known as switch yards, are used as aggregation, storage, and switching facilities for the cargo that arrives on trains entering each yard.

A 90-car train from El Paso, for example, may arrive in Midland as planned. Half the cars are destined for Midland, while the other half are destined for Amarillo. At the Midland yard the train is stored, disassembled, reassembled for transport, and switched as required to move the Amarillo traffic on to Amarillo. Switches in the yards (see Figure 3-10) create temporary paths from one side of the yard to the other. Meanwhile, route bosses in the yard towers analyze traffic patterns and route trains across a variety of alternative paths to ensure the most efficient delivery. For example, traffic from Amarillo to Roswell could be routed through Midland, but it would obviously be more efficient to send it on the direct line that runs between Amarillo and Roswell. Assuming that the direct route is available and is not congested, the route boss might very well choose that alternative.

Notice also that short local lines, called feeder lines, pump local traffic into the switchyards. These lines typically run shorter trains destined most likely for local delivery. Some of them, however, carry cargo destined for distant cities. In those cases, the cargo would be combined with that of other trains to create a large, efficient train with all cargo bound for the same destination.

Figure 3-10
A typical railroad switch.

Trunks, lines, feeders, local access spurs, switches, routers-all these terms are used commonly in the telecommunications industry. Trunks are high-bandwidth, long-distance transport facilities. Lines, feeders, and local access spurs are local loops. Switches and routers are, well, switches and routers. And the overall function of the two is exactly the same, as is their goal of delivering their transported payload in the most efficient fashion possible.

When Bell's contraption first arrived on the scene, it wasn't a lot more complicated than a railroad, frankly. As we noted earlier, there was no initial concept of switching. Instead, the plan was to gradually evolve the network to a full mesh architecture as customers demanded more and more connections. Eventually, operators were added to provide a manual switching function of sorts, and over time they were replaced with, then electromechanical, then all-electronic switches. Ultimately, intelligence was overlaid in the form of signaling, giving the network the capability to make increasingly informed decisions about traffic handling and provide value-added services.

Now that you understand the overall development strategy that Bell and his cohorts had in mind, as well as the basics of switching, we turn our attention to the inner workings of the typical network, shown in Figure 3-11. I must take a moment here to thank my good friend Dick Pecor, who created this drawing, from his head, I might add. Thanks, Dick.

Scalpel, please.

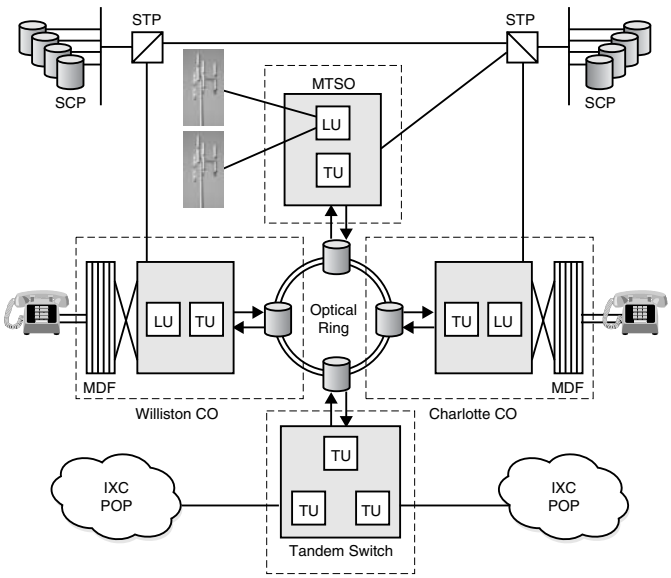


Figure 3-11 Typical network.

In the Belly of the Beast

When a customer makes a telephone call, a complex series of events takes place that ultimately leads to the creation of a temporary end-to-end, service-rich path. Let's follow a typical phone call through the network. Cristina in Williston is going to call Adam in Charlotte. This is a high-level explanation; we'll add more detail later.

When Cristina picks up the telephone in her home, the act of lifting the handset[1] closes a circuit that enables a current to flow from the switch in the local central office that serves her neighborhood to her telephone. The switch electronically attaches an oscillator to the circuit called a *dial tone generator*, which creates the customary sound that we all listen for when we want to place a call. The dial tone serves to notify the caller that the switch is ready to receive the dialed digits.

Cristina now dials Adam's telephone number by pressing the appropriate buttons on the phone. Each button generates a *pair of tones* (listen

[1] It doesn't matter whether the phone is corded or cordless. If cordless, pushing the TALK button creates a radio link between the handset and the base station, which in turn closes the circuit.

carefully—you can hear them) that are slightly dissonant. This is done to prevent the possibility of a human voice randomly generating a frequency that could cause a misdial. The tone pairs, shown in Figure 3-12, are carefully selected such that they could not be generated by the human voice. This technique is called *Dual Tone Multi-Frequency* (DTMF). It is not, however, the only way.

You may have noticed a switch on many phones with two positions labeled TONE and PULSE (see Figure 3-13). When the switch is set to the TONE position, the phone generates DTMF. When it is set on PULSE, it generates the series of clicks that old dial telephones made when they were used to place a call[2]. When the dial was rotated, let's say to the number three, it caused a switch contact to open and close rapidly three times, sending a series of three electrical pulses (or more correctly, interruptions) to the switch. DTMF has been around since the 1970s, but switches are still capable of being triggered by pulse dialing.

Want to impress your friends? Try pulse dialing on a DTMF telephone. Simply find a phone that has a real button or buttons that you can push down to hang up the phone. Pick up the handset, and then dial the number you want to call by rapidly pushing and releasing the buttons the

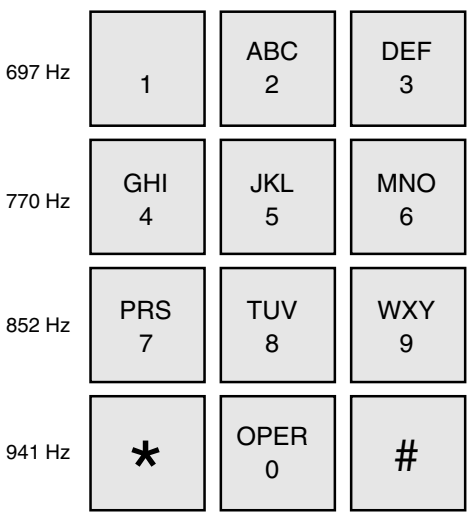


Figure 3-12 DTMF tone pairings.

[2] About eight years ago, I took a trip to Seattle to teach a class, and my family accompanied me. One evening while strolling along Pike Street we came upon a bank of modern pay phones, all of which had dials instead of DTMF buttons. My kids, still little back then, begged me for quarters so that they could call their friends on those cool new phones.

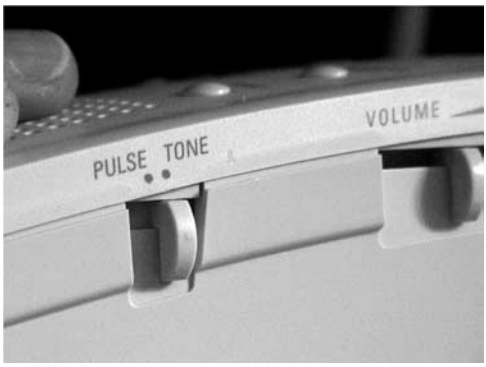


Figure 3-13 *Pulse/Tone switch on telephone.*

appropriate number of times, leaving a second or two of delay between each dialed digit. It takes a little practice, but it really does work. Try something simple like Information (411) first.

Back to our example. Cristina finishes dialing Adam's number and a digits collector in the switch receives the digits. The switch then performs a rudimentary analysis of the number to determine whether it is served out of the same switch. It does this by looking at the area code (*Numbering Plan Area* [NPA]) and prefix (NXX) of the dialed number.

A telephone number is comprised of three sections:

505 - 555 - 7837

The first three digits are the NPA, which identifies the called region. For example, I live in Vermont where the entire state is served by a single NPA, 802. Other states, such as California, have a dozen or more NPAs to serve its much denser population base.

The second three digits are the NXX, which identifies the exchange that the number is served from, and by extension the switch to which the number is connected. Each NXX can serve 10,000 numbers (555-0000 through 555-9999). Remember the New York fire? Twelve exchanges were lost, under which 104,000 subscribers were operating (out of a possible 120,000). A modern central office switch can typically handle as many as 15 to 20 exchanges of 10,000 lines each.

In our example, Adam is served out of a different switch than Cristina, so the call must be routed to a different central office. Before that routing can take place, however, Cristina's local switch routes a query to the signaling network, known as *Signaling System 7* (SS7). SS7 provides the network with intelligence. It is responsible for setting up, maintaining, and tearing down a call while at the same time providing access to enhanced services such as *Custom Local Area Signaling Services* (CLASS),

800 Number Portability, *Local Number Portability* (LNP), *Line Information Database* (LIDB) lookups for credit-card verification, and other enhanced features. In a sense, it makes the local switch's job easier by centralizing many of the functions that formerly had to be performed locally.

The original concept behind SS7 was to separate the actual calls on the public telephone network from the process of setting up and tearing down those calls as a way to make the network more efficient. This had the effect of moving the intelligence out of the *Public Switched Telephone Network* (PSTN) and into a separate network where it could be somewhat centralized and therefore made available to a much broader population. The SS7 network, shown in Figure 3-14, consists of packet switches (*Signal Transfer Points* [STPs]) and intelligent database engines (*Service Control Points* [SCPs]) interconnected to each other, and to the actual telephone company switches (*Service Switching Points* [SSPs]) via high-speed digital links, typically operating at 56 to 64 Kbps.

When a customer in an SS7 environment places a call, the following process takes place. The local switching infrastructure issues a software interrupt via the SSP so that the called and calling party information can be handed off to the SS7 network, specifically an STP. The STP in turn routes the information to an associated SCP, which performs a database lookup to determine whether any special call-handling instructions apply. For example, if the calling party has chosen to block the delivery of caller-ID information, the SCP database will ensure that this occurs.

Once the SCP has performed its task, the call information is returned to the STP packet switch, which consults routing tables and then establishes a route for the call. Upon receipt of the call, the destination switch determines whether the called party's phone is available, and if it is, it will ring the phone. If the customer's number is not available due to a

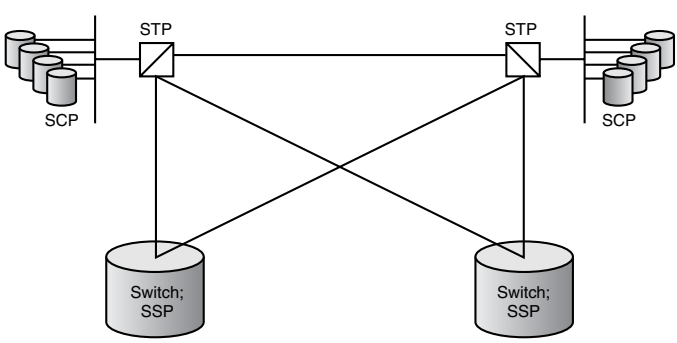


Figure 3-14 The SS7 network.

busy condition or some other event, a packet will be returned to the source indicating the fact and SS7 will instruct the originating switch to put a busy tone or reorder in the caller's ear.

At this point, the calling party has several options, one of which is to invoke one of the many CLASSservices such as *Automatic Ringback*. With Automatic Ringback, the network monitors the called number for a period of time, waiting for the line to become available. As soon as it is, the call will be cut through, and the calling party will be notified of the incoming call via some kind of distinctive ringing.

Thus, when a call is placed to a distant switch, the calling information is passed to SS7, which uses the caller's number, the called number, and SCP database information to choose a route for the call. It then determines whether any special call-handling requirements should be invoked, such as CLASS services, and instructs the various switches along the way to process the call as appropriate.

These features comprise a set of services known as the *Advanced Intelligent Network* (AIN), a term coined by Telcordia (formerly Bellcore). The SSPs (switches) are responsible for basic calling, while the SCPs manage the enhanced services that ride atop the calls. The SS7 network, then, is responsible for the signaling required to establish and tear down calls and to invoke supplementary or enhanced services.

Network Topology

Before we enter the central office, we should pause to explain the topology of the typical network (see Figure 3-15). The customer's telephone and most likely his or her PC and modem are connected via *house wiring* (sometimes called inside wire) to a device on the outside of the house or office building called a *protector block* (see Figure 3-16). It is nothing more than a high-voltage protection device (a fuse, if you will) designed to open the circuit in the event of a lightning strike or the presence of some other high-voltage source. It protects both the subscriber and the switching equipment from electrical damage.

The protector connects to the network via twisted-pair wire. Twisted pair is literally that, a pair of wires that have been twisted around each other to reduce the amount of crosstalk and interference that occurs between wire pairs packaged within the same cable. The number of twists per foot is carefully chosen. An example of twisted pair is shown in Figure 3-17.

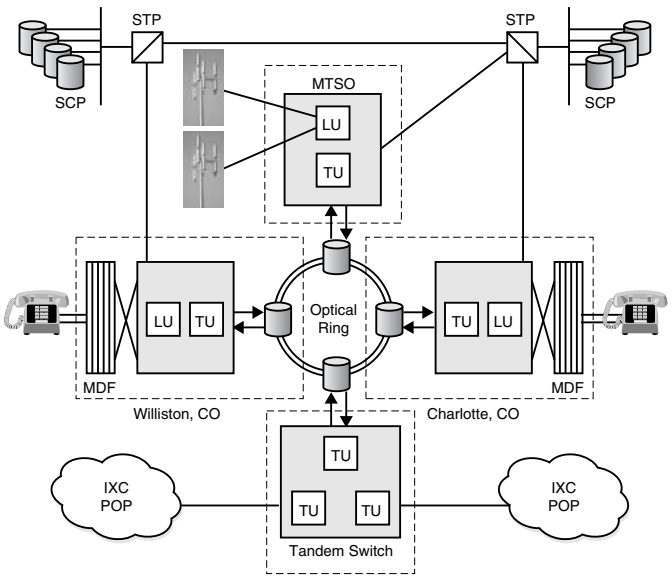


Figure 3-15
Typical network.

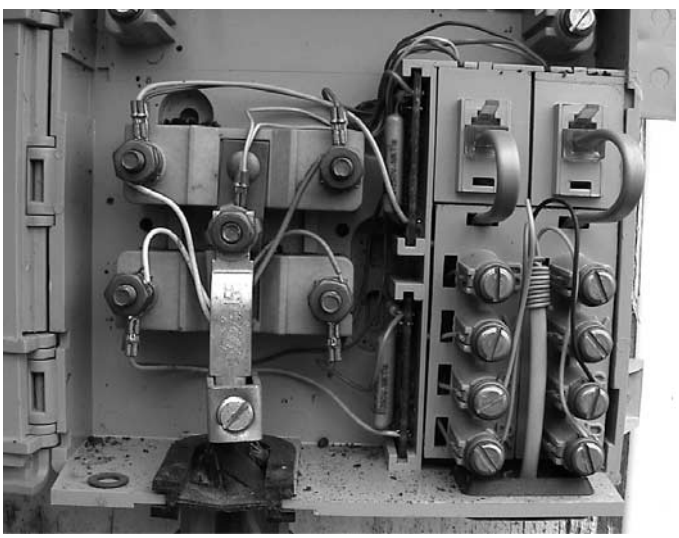


Figure 3-16
Protector block, shown at left.

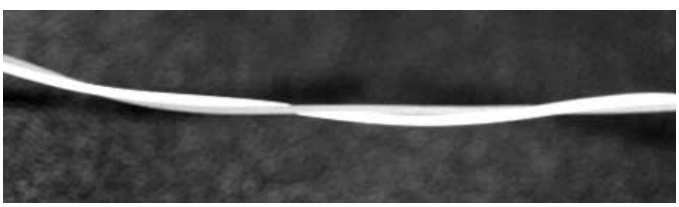


Figure 3-17
Twisted pair.

The twisted pair(s) that provides service to the customer arrives at the house on what is called the drop wire. It is either aerial, as shown in Figure 3-18, or buried underground. We note that multiple drop wires may be used because today most homes are wired with multiple pairs, since the average household typically orders a second line for a home office, computer, fax machine, or teenager.

Once it reaches the edge of the subscriber's property, the drop wire typically terminates on a terminal box, such as that shown in Figure 3-19. There all of the pairs from the neighborhood are cross-connected to the main cable that runs up the center of the street. This architecture is used primarily to simplify network management.

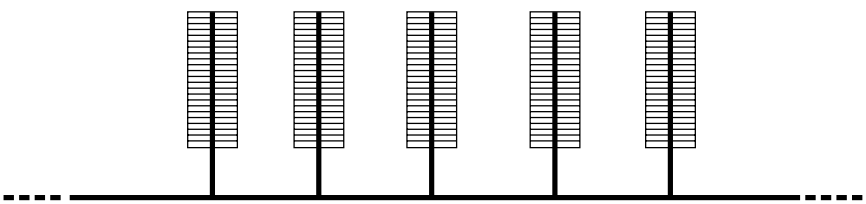
When a new neighborhood is built today, network engineers estimate the number of pairs of wire that will be required by the homes in that neighborhood. They then build the houses, install the network and cross-connect boxes along the street, and cross connect each house's drop wire to a single- wire pair. Every pair in the cable has an appearance at every terminal box along the street, as shown in Figure 3-20. This enables a cable pair to be reassigned to another house elsewhere on the street, should the customer move. It also enables cable pairs to be easily replaced should a pair go bad.

This design dramatically simplifies the installation and maintenance process, particularly given the high demand for additional cable pairs today. This design also results in a challenge for network designers. These multiple appearances of the same cable pair in each junction box

Figure 3-18
Drop wire.

Figure 3-19
Terminal box, sometimes known as a "B-Box."

Figure 3-20
Along the street, terminal boxes (Sometimes called B-Boxes) are installed. Each B-Box hosts an appearance of every pair of wires in the cable, which may contain as many as 500 pairs. With this design every pair in the cable is potentially available to every home or business along the street, making installation extremely flexible.



are called *bridged taps*. They create problems for digital services because electrical signal echoes can occur at the point where the wire terminates at a pair of terminal lugs.

Suppose, for example, that cable pair number 117 is assigned to the house at #2 Blanket Flower Circle. It is no longer necessary therefore for that cable pair to have an appearance at other terminal boxes because it is now assigned. Once the pair has been cross-connected to the customer's local loop drop wire, the technician *should* remove the appearances at other locations along the street by terminating the open wire appearances at each box. This eliminates the possibility of a

signal echo occurring and creating errors on the line, particularly if the line is digital.

When outside plant engineers first started designing their networks, they set them up so that each customer was given a cable pair from their house all the way to the central office. The problem with this model was cost. It was very expensive to provision a cable pair for each customer.

With the arrival of TDM, however, the "one-dog, one-bone" solution was no longer the only option. Instead, engineers were able to design a system under which customers could share access to the network, as shown in Figure 3-21. This technique, known as a *subscriber loop carrier,* uses a collection of T-1 carriers to combine the traffic from a cluster of subscribers and thus reduce the amount of wire required to interconnect them to the central office.

The best known carrier system is called the SLC-96 (pronounced *SLICK)*, originally manufactured by Western Electric/Lucent, which transports traffic from 96 subscribers over four four-wire T-Carriers (plus a spare). A remote SLC terminal is shown in Figure 3-22. Thus, 96 subscribers require only 20 wires between their neighborhood and the central office, instead of the 192 wires that would otherwise be required.

The only problem with this model is that customers are by and large restricted to the 64 Kbps of bandwidth that loop carrier systems assign to each subscriber. That means that subscribers wanting to buy *more* than 64 Kbps, such as those that want *Digital Subscriber Lines* (DSLs), are out of luck. And since it is estimated that as many as 70 percent of all subscribers in the United States are served from loop carriers, this poses a service problem that service providers are scrambling to overcome. New versions of loop carrier standards and technologies such as GR-303 and optical remotes that use fiber instead of copper for the

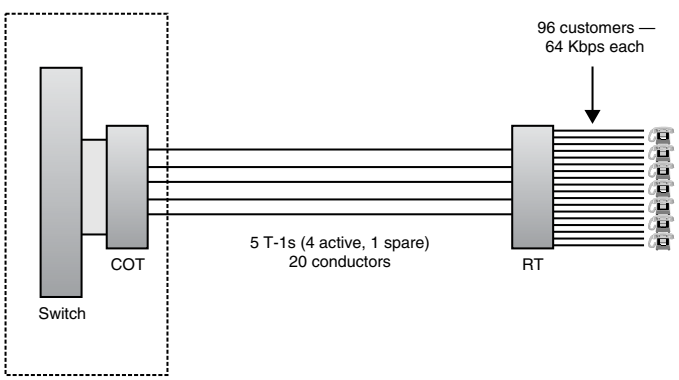


Figure 3-21
Subscriber loop carrier system. Customer share access to the network via a collection of multiplexed facilities to reduce outside plant cost.

Figure 3-22
A remote loop carrier terminal.

trunk line between the remote terminal and the central office terminal go a long way toward solving this problem. There is still quite a ways to go, however.

Typically, as long as a customer is within 12,000 feet from a central office, they will be given a dedicated connection to the network, as shown in Figure 3-23. If they are farther than 12,000 feet from the CO, however, they will normally be connected to a subscriber loop carrier system of one type or another.

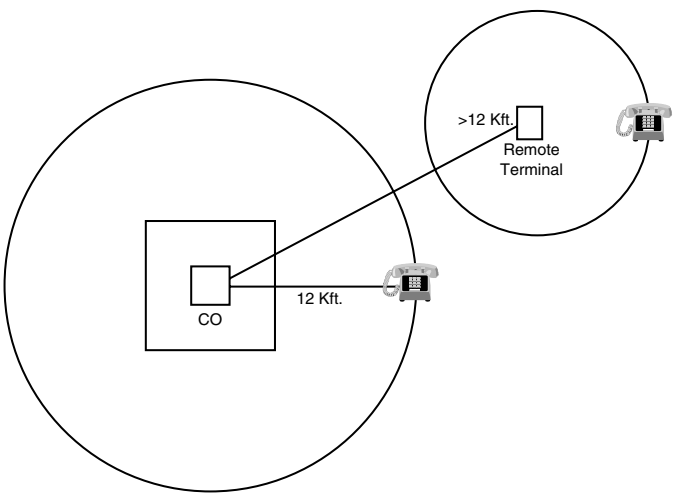


Figure 3-23
Carrier Serving Area (CSA) architecture.

Either way, the customer's local loop, whether as a standalone pair of wires or as a timeslot on a carrier system, makes its way over the physical infrastructure on its way to the network. It may be aerial, as shown in Figure 3-24, or underground, as shown in Figure 3-25. If it has to

Figure 3-24 Aerial plant. Telephony is the lowest set of facilities on the pole.

Figure 3-25 Installation of underground plant.

travel a significant distance, it may encounter a load coil along the way, which is a device that "tunes" the local loop to the range of frequencies required for voice transport and extends the distance over which the signals can travel.

A *load pot*, shown in Figure 3-26, comprises multiple load coils and performs loading for all the cable pairs in a cable that require it. It may also encounter a repeater if it is a digital loop carrier; the repeater receives the incoming signal, now weakened and noisy from the distance it has traveled, and reconstructs it, regenerating it before sending it on its way. A repeater, sometimes called a regenerator (and sometimes *wrongly* called an amplifier), is shown in Figure 3-27. In this photograph,

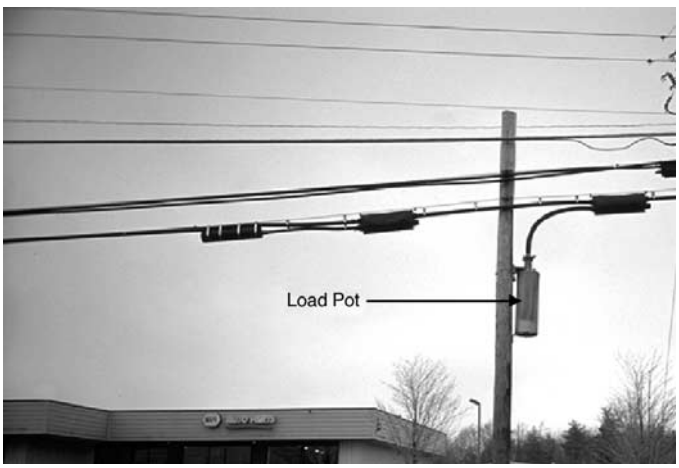


Figure 3-26
A load pot containing load coils.

Figure 3-27
Dick Pecor with regenerator housing.

Dick Pecor models the latest in regenerative repeater environmental cases.

One last item of interest: in spite of the fact that we call them telephone poles, the wooden poles that support telephone cables are in fact shared among telephone, power, and cable providers, as shown in Figure 3-28. Telephony plant is the lowest, followed by cable. Power is the highest, high enough that a technician working on a phone or cable problem could not accidentally touch the open power conductors. Normally, the telephone company owns the pole and leases space on it to other utilities.

As a cable approaches the central office, its pairs are often combined with those of other approaching cables in a splice case (see Figure 3-29) to create a larger cable. For example, four 250-pair cables may be combined to create a 1,200-pair cable, which in turn may be combined with others to create a 3,600-pair cable that enters the central office. Once inside the office, the cables are broken out for distribution. This is done in the cable

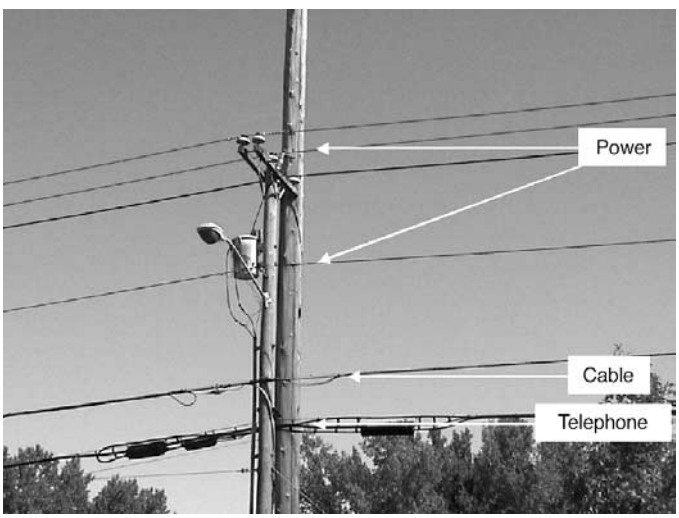


Figure 3-28
Shared pole for aerial plant.

Figure 3-29
Splice cases (two on left, one on right).

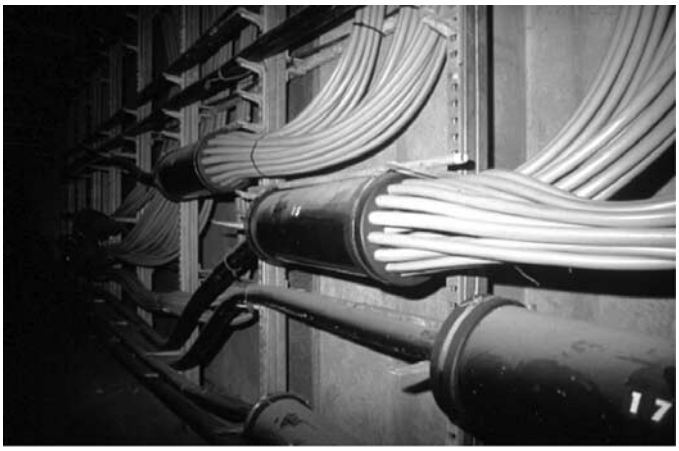


Figure 3-30
In the cable vault, the large cables shown on the left are broken down into the smaller cables on the right for distribution throughout the office.

vault; an example is shown in Figure 3-30. The large cable on the left side of the splice case is broken down into the collection of smaller cables exiting on the right.

Into the Central Office

We could say a great deal more about the access segment of the network and will later. For now, though, let's begin our tour of the central office.

By now, our cable has traveled over aerial and underground traverses and has arrived at the central office. It enters the building via a buried conduit that feeds into the *cable vault*, the lowest sub-basement in the office (remember, this is where the New York City fire began). Because the cable vault is exposed to the underground conduit system, the danger exists that noxious and potentially explosive gases (methane, mostly) could flow into the cable vault and be set afire by a piece of electrical equipment that sparks momentarily. These rooms are therefore closely monitored by the electronic equivalent of the canary in a coal mine and will cause alarms to sound if gas levels reach dangerous levels. A cable vault is shown in Figure 3-31.

The cables that enter the cable vault are large and encompass hundreds if not thousands of wire pairs. Their security is obviously critical, because the loss of a single cable could mean the loss of service for hundreds or thousands of customers. To help maintain the integrity of the outside cable plant, underground cables are pressurized with dry air and are fed from a pressurization pump and manifold system in the cable

Figure 3-31
Inside the cable vault.

vault (see Figures 3-32a and 3-32b). The pressure serves two purposes: it keeps moisture from leaking into a minor breach in the cable, and it serves as an alarming system in the event of a major cable failure. Cable plant technicians can analyze the data being fed to them from pressure transducers along the cable route and determine the location of the break.

As soon as the large cables have been broken down into smaller, easier-to-manupulate-fire-retardant cables, they leave the cable vault on their way up to the *Main Distribution Frame* (MDF).

Before we leave the basement of the CO, we should discuss power, a major consideration in an office that provides telecommunications services to hundreds of subscribers.

When you plug in a laptop computer, the transformer does not power the laptop. The transformer's job is to charge the battery (assuming the battery is installed in the laptop); the battery powers the computer. That way, if commercial power goes away, the computer is unaffected because it was running on the battery to begin with.

Central offices work the same way. They are powered by massive, wet-cell battery arrays, shown in Figure 3-33, that are stored in the basement. The batteries are quite large, about two feet tall, and are connected together by massive copper bus bars. Meanwhile, commercial power, shown in Figure 3-34 (Okay, not really), is fed to the building from several redundant sources on the power grid to avoid dependency on a single source of power. The AC power is fed into a rectifier bank that converts it to 48 volts DC; the power is then trickled to the batteries. The voltage maintains a constant charge on them.

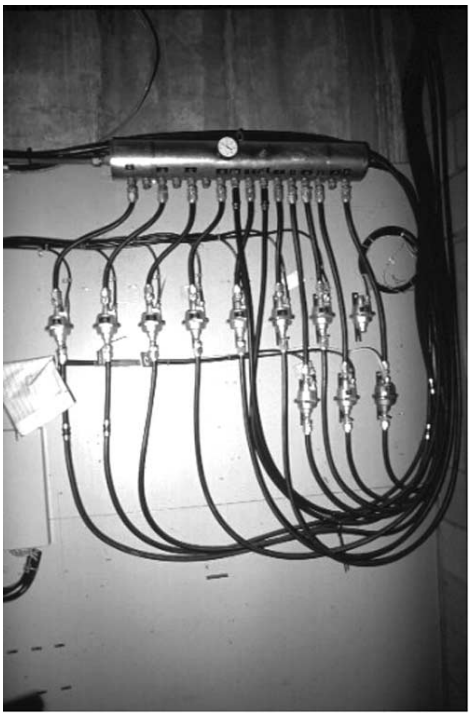


Figure 3-32a
Pressure transducers.

Figure 3-32b
Pressure maintenance equipment.

Figure 3-33
CO battery array.

Figure 3-34
Technicians working on CO commercial power.

In the event that a failure of commercial power should occur, the building's *uninterruptible power supply* (UPS) equipment, shown in Figure 3-35, kicks in and begins a complex series of events designed to protect service in the office. First, it recognizes that the building is now isolated and is on battery power exclusively. The batteries have enough current to power a typical CO for about 8 hours before things start to fail. Second, technicians begin overseeing the process of restoral and of shutting down nonessential systems to conserve battery power.

Figure 3-35 Uninterruptible Power Supply, or UPS.

Third, the UPS system initiates the automatic startup of the building's turbine, a massive jet engine that can be spun up in about a half-hour. The turbine is either in a soundproof room in the basement (see Figure 3-36) or in an enclosure on the roof of the building (see Figure 3-37). Once the turbine has spun up to speed, the building's power load can slowly be shed onto it. It will power the building until it runs out of kerosene, but most buildings have several day's supply of fuel in their underground tanks. As Al Bergman, a data center design engineer and friend told me several years ago, "If we're down so long that we run out of fuel, our problems are far worse than an office that's out of service."

Returning now to our copper facilities, the cables leave the cable vault via ducts and travel upstairs to whichever floor houses the *Main Distribution Frame* (MDF). The MDF, shown in Figure 3-38, is a large iron jungle gym sort of frame that provides physical support for the thousands of

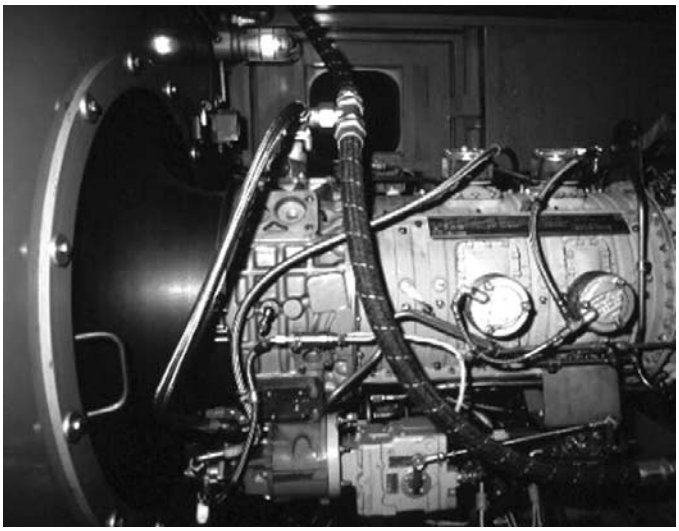


Figure 3-36
CO Turbine.

Figure 3-37
Turbine in rooftop enclosure.

pairs of wire that interconnect customer telephones to the switch. The cables from the cable vault ascend and are hardwired to the *vertical side* of the MDF, shown in Figure 3-39. The ends of the cables are called the *cable heads*. The vertical side of the MDF has additional overvoltage protection, shown in the figure.

The arrays of plug-ins are called carbons; they are simply carbon fuses that open in the event of an overvoltage situation and protect the equipment and people in the office. A close-up of carbons is shown in Figure 3-40.

Figure 3-38 Main Distribution Frame, or MDF.

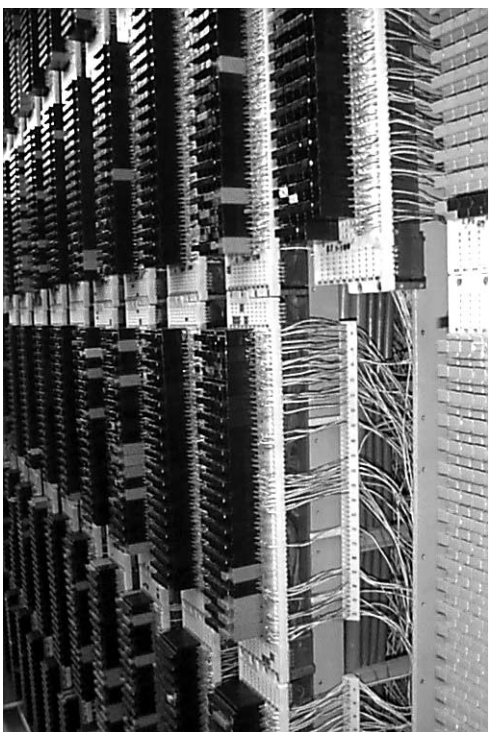


Figure 3-39 Vertical side of MDF, showing protectors.

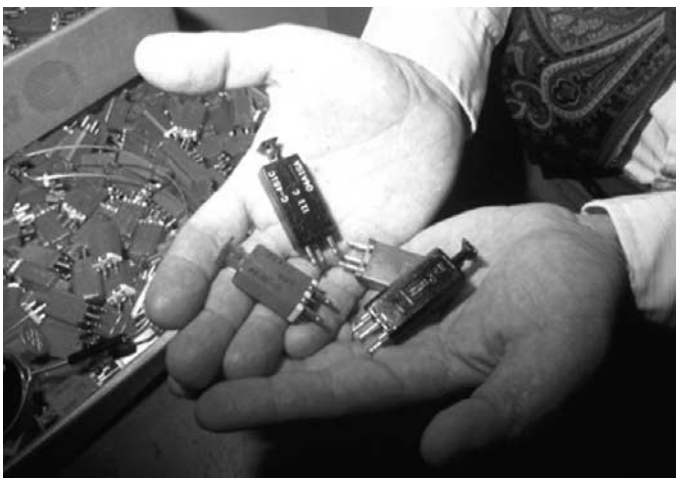


Figure 3-40
Close-up of carbons.

The vertical side of the MDF is manually wired to the *horizontal side.* The horizontal side, shown in Figure 3-41, is wired to the central office switch line units. Notice the mass of wire lying on each shelf of the frame; these are the cable pairs from the customers served by the office. Imagine the complexity of troubleshooting a problem in that hairball. I have spent many hours up to my shoulders in wire, tugging on a wire pair while a technician 50 feet down the frame, also up to his elbows in wire, feels for the wire that is moving so it can be traced.

The horizontal side also provides craft/technician access for repair purposes. In Figure 3-42, Dick Pecor has connected a test set to the appearance of a line unit and is listening for a dial tone.

From the mainframe, the cable pairs are connected to the local switch in the office. Remember that the job of the local switch is to establish temporary connections between two customers that want to talk, or between two computers that want to spit bits at each other. The *line units* (LUs) on the switch provide a connection point for every cable pair served by that particular switch in the office. Conceptually, then, it is a relatively simple task for the switch to connect one subscriber in the switch with another subscriber in the same switch. After all, the switch maintains translations—a directory, if you will—so it knows the subscribers to which it is directly connected.

Far more complicated is the task of connecting a subscriber in one switch to a subscriber in another. This is where network intelligence becomes critically important. As mentioned earlier, when the switch receives the dialed digits, it performs a rudimentary analysis on them to

Figure 3-41
Horizontal side of MDF.

Figure 3-42
Dick Pecor testing cable pair on horizontal side of MDF.

determine whether the called party is locally hosted. If the number is in the same switch, the call is established. If it resides in another switch, the task is a bit more complex.

First, the local switch must pass the call on to the local tandem switch, which provides access to the *points of presence* (POPs) of the various long-distance carriers that serve the area. The tandem switch typically does not connect directly to subscribers; it connects to other switches only.

The tandem switch then hands the call off to the long-distance carrier, which transports it over the long-distance network to the carrier's switch in the remote (receiving) office.

SS7's influence once again becomes obvious here. One of the problems that occurred in earlier telephone system designs was the following. When a subscriber placed a call, the local switch handed the call off to the tandem, which in turn handed the call off to the long-distance provider. The long-distance provider seized a trunk, over which it transported the dialed digits to the receiving central office. The signaling information therefore traveled over the path designed to produce revenue for the telephone company, a process known as *in-band signaling*. As long as the called party was home, and wasn't on the phone, the call would go through as planned and revenue would flow. If they weren't home, however, or if they were on the phone, then no revenue was generated. Furthermore, the network resources that another caller might have used to place a call were not available to them, because they were tied up transporting call setup data, which produces no revenue.

SS7 changes all that. With SS7, the signaling data travels across a dedicated packet network from the calling party to the called party. SS7 verifies the availability of the called party's line, reserves it, and then, *and only then,* seizes a talk path. Once the talk path has been created, it rings the called party's phone and places a ringing tone in the caller's ear. As soon as the called party answers, SS7 silently bails out until one end or the other hangs up. At that point, it returns the path to the pool of available network resources.

Interoffice Trunking

We have not discussed the manner in which offices are connected to one another. As Figure 3-43 illustrates, an optical fiber ring with add-drop multiplexers interconnects the central offices so that interoffice traffic can be safely and efficiently transported. The switches have *trunk units* (TUs) that connect the back side, called the trunk side, of the switch to the *wide area network* (WAN), in this case the optical ring.

Trunks that interconnect offices have historically been four-wire copper, coax or microwave facilities (a pair in each direction). Today they are largely optical, but are still referred to as four-wire because of their two-way nature.

An interesting point should be made about trunks. In the 1960s and early 1970s, most interoffice trunks were analog rather than digital. To signal, they used single frequency tones. Because these trunks did not

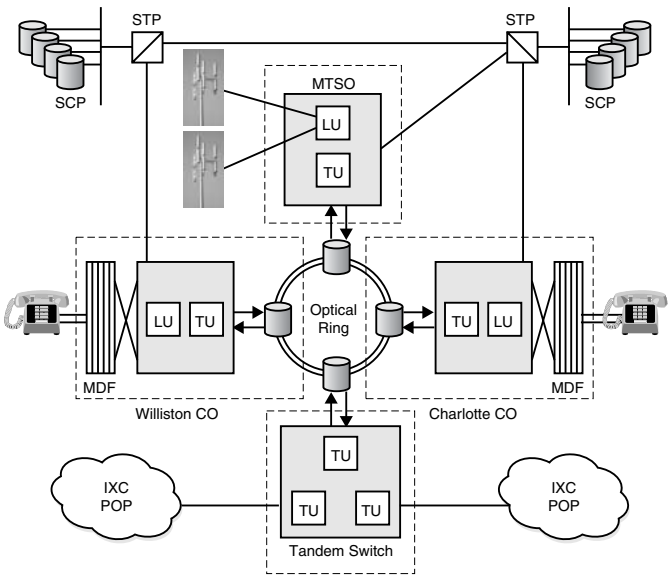


Figure 3-43 *Typical network showing fiber ring interconnecting offices.*

"talk" directly to customers, there was no reason to worry about a human voice inadvertently emitting a sound that could be misconstrued as a dialing tone. There was therefore no reason to use DTMF dialing. Instead, trunk signaling was performed using single frequency tones. Specifically, if a switch wanted to seize a long-distance trunk, it issued a single-frequency 2600-Hz tone, which would signal the seizure to take place. Once the trunk seizure had occurred, the dialed digits could be outpulsed and the call would proceed as planned.

In 1972, John Draper, better known by his hacker name "Captain Crunch," determined that the toy plastic bosun's whistle that came packed in boxes of Cap'n Crunch cereal emitted, you guessed it, 2600 Hz. Anyone who knew this could steal long-distance service from AT&T by blowing the whistle at the appropriate time during call setup. Before long, word of this capability became common knowledge and Cap'n Crunch cereal became the breakfast food of choice for hackers all over the country.

Soon hackers everywhere were constructing "blue boxes," small oscillators built from cheap parts that would emit 2600 Hz and make possible the kind of access that Draper and his cohorts were engaged in. In fact, Steve Wozniak and Steve Jobs, both founders of Apple, were early blue box users and according to legend used the money they made building blue boxes to fund the company that became Apple.

Draper, a highly skilled hacker, was eventually caught and prosecuted for his activities, but he was given work furlough and was able to continue his software design studies. He is now a successful intrusion detection software designer.

Returning to our example again, let's retrace our steps. Cristina dials Adam's number. The call travels over the local loop, across aerial and/or underground facilities, and enters the central office via the cable vault. From the cable vault, the call travels up to the main distribution frame and then on to the switch. The number is received by the switch in Cristina's serving central office, which performs an SS7 database lookup to determine the proper disposition of the call and any special service information about Cristina that it should invoke. The local switch routes the call over inter-office facilities to a tandem switch, which in turn connects the call to the POP of whichever long-distance provider to which Cristina subscribes. The long-distance carrier invokes the capabilities of SS7 to determine whether Adam's phone is available, and if it is, it hands the call off to the remote local service provider. When Adam answers, the call is cut through and it progresses normally.

Of course, calls can be routed in other ways. The local loop could be wireless, and if it is, the call from the cell phone is received by a cell tower (see Figure 3-44) and is transported to a special dedicated cellular switch in a central office called a *Mobile Telephone Switching Office* (MTSO). The MTSO processes the call and hands it off to the wireline network via interoffice facilities. From that point on, the call is handled like any other. It is either terminated locally on the local switch or handed to a tandem switch for long-distance processing. The fact of the matter is that the only part of a cellular network that is truly wireless is the local loop;

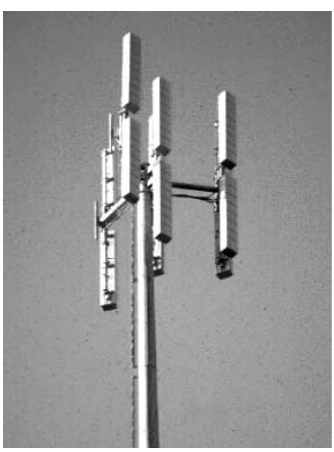


Figure 3-44
Cell tower.

everything else is wired. We will discuss cellular telephony in greater detail in the chapter on access.

Before we wrap up this chapter, we should take a few minutes to discuss carrier systems, voice digitization, and multiplexed transport, all of which take place (for the most part) in the central office. In spite of all the hype out there about the Internet and IP magic, the *plain old telephone service* (POTS) remains the cash cow in the industry. In this final section, we'll explain T- and E-Carriers, the Synchronous Optical Network (SONET), the Synchronous Digital Hierarchy (SDH), and voice digitization techniques.

Conserving Bandwidth: Voice Transport

The original voice network, including access, transmission facilities, and switching components, was exclusively analog until 1962 when T-Carrier emerged as an interoffice trunking scheme. The technology was originally introduced as a short-haul, four-wire facility to serve metropolitan areas and was a technology that customers would *never* have a reason to know about. After all, what customer could ever need a meg-and-a-half of bandwidth? Over the years, however, it evolved to include coaxial cable facilities, digital microwave systems, fiber, and satellite, and, of course, became a premier access technology that customers knew a great deal about.

Consider the following scenario. A corporation builds a new headquarters facility in a new area just outside the city limits. The building will provide office space for approximately 2,000 employees, a considerable number. Those people will need telephones, computer data facilities, fax lines, videoconferencing circuits, and a variety of other forms of connectivity.

The telephone company has two options that it can exercise to provide access to the building. It can make an assessment of the number of pairs of wire that the building will require and install them, or it can do the same assessment but provision the necessary bandwidth through carrier systems that transport multiple circuits over a shared facility. Obviously, this second option is the most cost-effective and is in fact the option that is most commonly used for these kinds of installations. This model should sound familiar. Earlier we discussed loop carrier systems and the

fact that they reduce the cost of provisioning network access to far-flung neighborhoods. This is the same concept; instead of a residential neighborhood, we're provisioning a "corporate neighborhood."

The most common form of multiplexed access and transport is T-Carrier, or E-Carrier outside the United States. Let's take a few minutes to describe them.

Framing and Formatting in T-1

The standard T-Carrier multiplexer, shown in Figure 3-45, accepts inputs from 24 sources, converts the inputs to PCM bytes, and then time division multiplexes the samples over a shared four-wire facility, as shown in Figure 3-46. Each of the 24 input channels yields an 8-bit sample, in round-robin fashion, once every 125 microseconds (8,000 times per second). This yields an overall bit rate of 64 Kbps for each channel (8 bits per sample × 8,000 samples per second). The multiplexer gathers one 8-bit sample from each of the 24 channels and aggregates them into a 192-bit frame. To the frame it adds a frame bit, which expands the frame to a 193-bit entity. The frame bit is used for a variety of purposes that will be discussed in a moment.

The 193-bit frames of data are transmitted across the four-wire facility at the standard rate of 8,000 frames per second, for an overall T-1 bit rate of 1.544 Mbps. Keep in mind that 8 Kbps of the bandwidth consists

Figure 3-45 *T-Carrier multiplexer channel banks, showing DS-0 cards.*

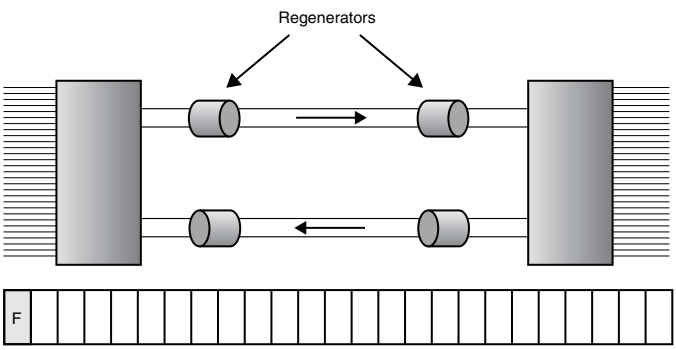


Figure 3-46
A Time Division Multiplexer in action.

of frame bits (one frame bit per frame, 8,000 frames per second); only 1.536 Mbps belong to the user.

Beginnings: D1 Framing

The earliest T-Carrier equipment was referred to as D1 and was considerably more rudimentary in function than modern systems (see Figure 3-47). In D1, every 8-bit sample carried 7 bits of user information (bits 1 through 7) and 1 bit for signaling (bit 8). The signaling bits were used for exactly that: indications of the status of the line (on-hook, off-hook, busy, high and dry, and so on), while the 7 user bits carried encoded voice information. Because only 7 of the 8 bits were available to the user, the result was considered to be less than toll quality (128 possible values, rather than 256). The frame bits, which in modern systems indicate the beginning of the next 192-bit frame of data, toggled back and forth between 0 and 1.

Evolution: D4

As time went on and the stability of network components improved, an improvement on D1 was sought after and found. Several options were developed, but the winner emerged in the form of the D4 or superframe format. Rather than treat a single 193-bit frame as the transmission entity, superframe "gangs together" 12 193-bit frames into a 2,316-bit entity, shown in Figure 3-48, that obviously includes 12 frame bits.

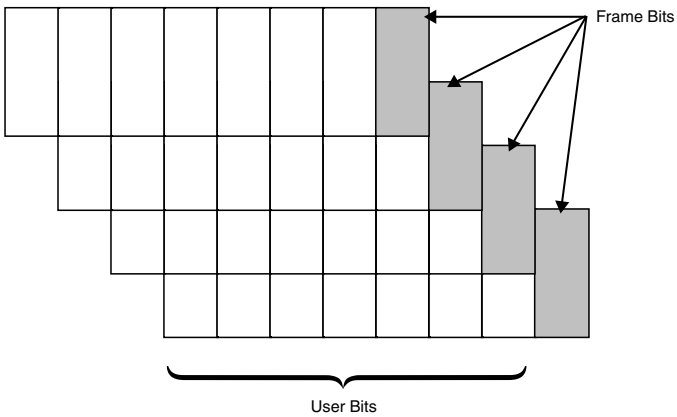


Figure 3-47
D1 framing.

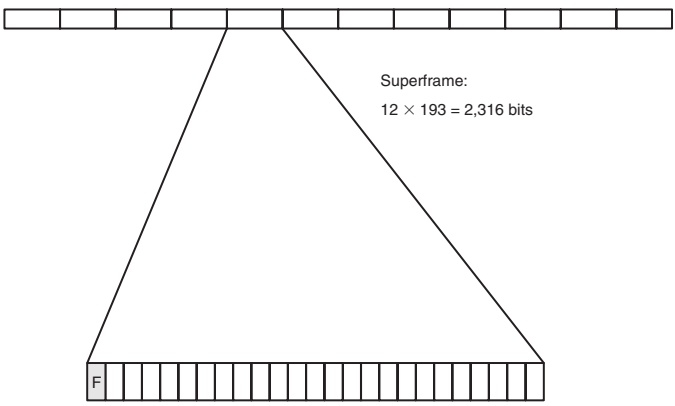


Figure 3-48
Superframe (D4) framing.

Please note that the bit rate has not changed; we have simply changed our view of what constitutes a frame.

Since we now have a single (albeit large) frame, we clearly don't need 12 frame bits to frame it; consequently, some of them can be redeployed for other functions. In superframe, the 6 odd-numbered frame bits are referred to as terminal framing bits and are used to synchronize the channel bank equipment. The odd framing bits, on the other hand, are called signal framing bits and indicate to the receiving device *where* robbed-bit signaling occurs.

In D1, the system reserved 1 bit from every sample for its own signaling purposes, which succeeded in reducing the user's overall throughput. In D4, that is no longer necessary; instead, we signal less frequently, and

only occasionally rob a bit from the user. In fact, because the system operates at a high transmission speed, network designers determined that signaling can occur relatively infrequently and still convey adequate information to the network. Consequently, bits are robbed from the sixth and eighth iteration of each channel's samples, and then only the least significant bit from each sample. The resulting change in voice quality is negligible.

Back to the signal framing bits: within a transmitted superframe, the second and fourth signal framing bits would be the same, but the sixth would toggle to the opposite value, indicating to the receiving equipment that the samples in that subframe of the superframe should be checked for signaling state changes. The eighth and tenth signal framing bits would stay the same as the sixth, but would toggle back to the opposite value once again in the twelfth, indicating once again that the samples in that subframe should be checked for signaling state changes.

Today: Extended Superframe (ESF)

Although superframe continues to be widely utilized, an improvement came about in the 1980s in the form of *extended superframe* (ESF), shown in Figure 3-49. ESF groups 24 frames into an entity instead of 12 and, like superframe, reuses some of the frame bits for other purposes. Bits 4, 8, 12, 16, 20, and 24 are used for framing and form a constantly repeating pattern (001011 . . .). Bits 2, 6, 10, 14, 18, and 22 are used as a 6-bit *cyclic redundancy check* (CRC) to check for bit errors on the facility. Finally, the remaining bits, all of the odd frame bits in the frame, are

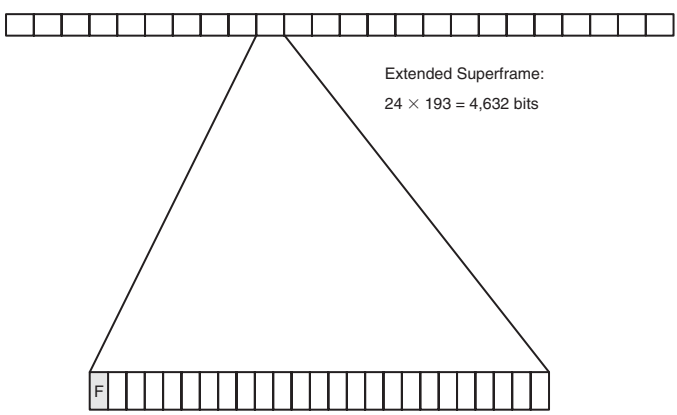


Figure 3-49 Extended Superframe (ESF) framing.

used as a 4-Kbps facility data link for end-to-end diagnostics and network management tasks.

ESF provides one major benefit over its predecessors: the capability to do nonintrusive testing of the facility. In earlier systems, if the user reported trouble on the span, the span would have to be taken out of service for testing. With ESF, that is no longer necessary because of the added functionality provided by the CRC and the facility data link.

The Rest of the World: E-1

E-1, used for the most part outside of the United States and Canada, differs from T-1 on several key points. First, it boasts a 2.048-Mbps facility, rather than the 1.544-Mbps facility found in T-1. Second, it utilizes a 32-channel frame rather than 24. Channel one contains framing information and a *four-bit cyclic redundancy check* (CRC-4), channel 16 contains all signaling information for the frame, and channels 1 through 15 and 17 through 31 transport user traffic. The frame structure is shown in Figure 3-50.

A number of similarities exist between T-1 and E-1 as well. Channels are all 64 Kbps, frames are transmitted 8,000 times per second, and whereas T-1 gangs together 24 frames to create an extended superframe, E-1 gangs together 16 frames to create what is known as an ETSI multiframe. The multiframe is subdivided into two sub-multiframes; the CRC-4 in each one is used to check the integrity of the sub-multiframe that preceded it.

A final word about T-1 and E-1: because T-1 is a departure from the international E-1 standard, it is incumbent upon the T-1 provider to perform all interconnection conversions between T-1 and E-1 systems. For example, if a call arrives in the United States from a European country, the receiving American carrier must convert the incoming E-1 signal to T-1. If a call originates from Canada and is terminated in Australia, the

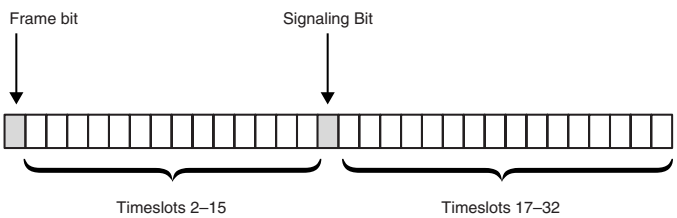


Figure 3-50
E-1 framing.

Canadian originating carrier must convert the call to E-1 before transmitting it to Australia.

Up the Food Chain: From T-1 to DS3 . . . and beyond

When T-1 and E-1 first emerged on the telecommunications scene, they represented a dramatic step forward in terms of the bandwidth that service providers now had access to. In fact, T-1 and E-1 were *so* bandwidth-rich that a customer would never need to exploit their full capabilities. What customer, after all, could ever have a use for 1 million-and-a-half bits per second of bandwidth?

Of course, that question was rendered moot in short order as increasing requirements for bandwidth drove demand that went well beyond the limited capabilities of low-speed transmission systems. As T-1 became mainstream, its usage went up, and soon requirements emerged for digital transmission systems with capacities greater than 1.544 Mbps. The result was the creation of what came to be known as the North American Digital Hierarchy, shown in Figure 3-51. The table also shows the European and Japanese hierarchy levels.

From DS-1 to DS-3

We have already seen the process for creating the DS-1 signal from 24 incoming DS-0 channels and an added frame bit. Now we turn our attention to higher bit-rate services. As we wander our way through this

Figure 3-51 North American Digital Hierarchy.

Hierarchy Level	Europe	United States	Japan
DS-0	64 Kbps	64 Kbps	64 Kbps
DS-1		1.544 Mbps	1.544 Mbps
E-1	2.048 Mbps		
DS-1c		3.152 Mbps	3.152 Mbps
DS-2		6.312 Mbps	6.312 Mbps
E-2	8.448 Mbps		32.064 Mbps
DS-3	34.368 Mbps	44.736 Mbps	
DS-3c		91.053 Mbps	
E-3	139.264 Mbps		
DS-4		274.176 Mbps	
			397.2 Mbps

explanation, pay particular attention to the complexity involved in creating higher rate payloads.

The next level in the North American Digital Hierarchy is called DS-2. Although it is rarely seen outside of the safety of the multiplexer in which it resides, it plays an important role in the creation of higher bit-rate services. It is created when a multiplexer *bit-interleaves* four DS-1 signals and inserts a control bit, known as a C-bit, into every 48 bits in the payload stream. Bit interleaving is an important construct here, because it contributes to the complexity of the overall payload.

In a bit-interleaved system, multiple bit streams are combined on a bit-by-bit basis, as shown in Figure 3-52. When payload components are bit-interleaved to create a higher-rate multiplexed signal, the system first selects bit 1 from channel 1, bit 1 from channel 2, bit 1 from channel 3, and so on. Once it has selected and transmitted all of the first bits, it goes on to the second bits from each channel, then the third, until it has created the super-rate frame. Along the way it intersperses C-bits, which are used to perform certain control and management functions within the frame.

Once the 6.312-Mbps DS-2 signal has been created, the system shifts into high gear to create the next level in the transmission hierarchy. Seven DS-2 signals are then bit-interleaved along with C-bits after every 84 payload bits to create a composite 44.736-Mbps DS-3 signal. The first part of this process, the creation of the DS-2 payload, is called *M12 multiplexing*. The second step, which combines DS-2s to form a DS-3, is called *M23 multiplexing*. The overall process is called *M13* and is illustrated in Figure 3-53.

The problem with this process is the bit-interleaved nature of the multiplexing scheme. Because the DS-1 signal components arrive from different sources, they may be (and usually are) slightly off from one another in terms of the overall phase of the signal; in effect, their speeds

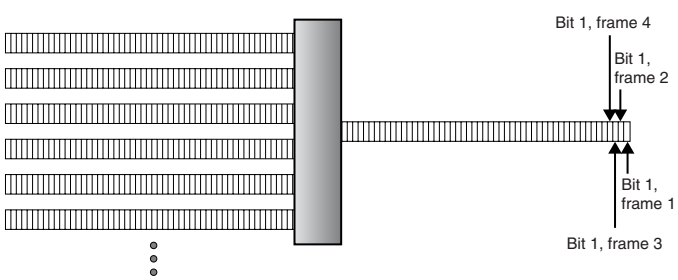


Figure 3-52
Bit-interleaved system.

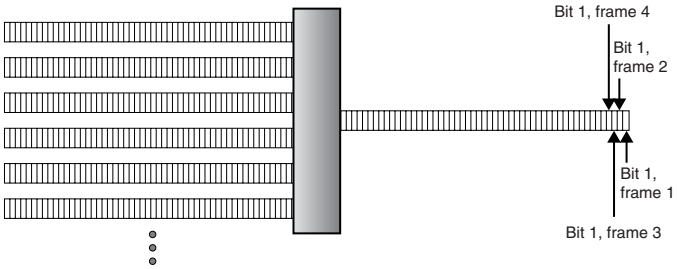


Figure 3-53 M13 multiplexing process.

differ slightly. This is unacceptable to a multiplexer that must rate-align them if it is to properly multiplex them, beginning with the head of each signal. In order to do this, the multiplexer inserts additional bits, known as stuff bits, into the signal pattern at strategic places that serve to rate-align the components. The structure of a bit-stuffed DS-2 frame is shown in Figure 3-54, whereas a DS-3 frame is shown in Figure 3-55.

The complexity of this process should now be fairly obvious to the reader. If we follow the left-to-right path shown in Figure 3-56, we see the rich complexity that suffuses the M13 signal-building process. Twenty-four 64-Kbps DS0s are aggregated at the ingress side of the T-1[3] multiplexer, grouped into a T-1 frame, and combined with a single frame bit to form an outbound 1.544-Mbps signal (I call this the M01 stage; that's my nomenclature, used for the sake of naming continuity). That signal then enters the intermediate M12 stage of the multiplexer, where it is combined (bit-interleaved) with three others and a good dollop of alignment overhead to form a 6.312-Mbps DS-2 signal. That DS-2 then enters the M23 stage of the mux, where it is bit-interleaved with six others and

M 0		C 1		F 0		C 1		C 1		F 1	
M 1		C 2		F 0		C 2		C 2		F 1	
M 1		C 3		F 0		C 3		C 3		F 1	
M 1		C 4		F 0		C 4		C 4		F 1	

Figure 3-54 M12 frame comprised of four sub-frames and 48-bit payload fields: 1,176 bits.

[3] The process is similar for the E-1 hierarchy.

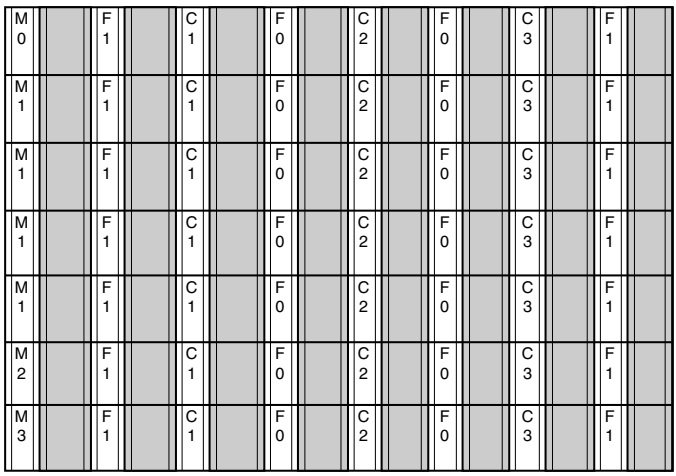


Figure 3-55
M13 frame comprised of seven sub-frames and 84-bit payload fields: 4,760 bits.

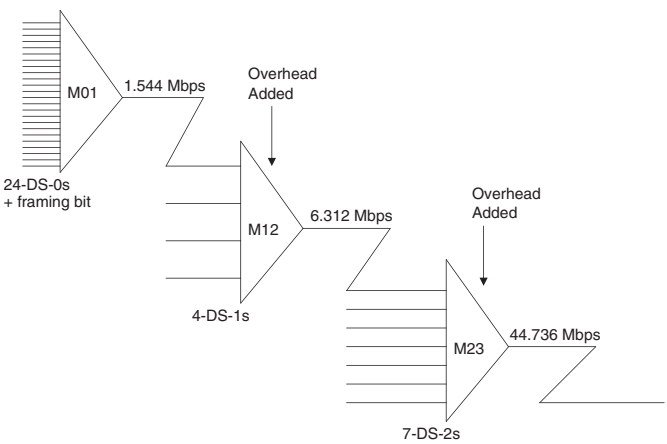


Figure 3-56
The M13 multiplexing process and its complexity.

another scoop of overhead to create a DS-3 signal. At this point, we have a relatively high-bandwidth circuit that is ready to be moved across the WAN.

Of course, as our friends in the United Kingdom are wont to say, the inevitable spanner always gets tossed into the works (those of us on the left side of the Atlantic call it a wrench). Keep in mind that the 28 (do the math) bit-interleaved DS-1s may well come from 28 different sources, which means that they may well have 28 different destinations. This translates into the pre-SONET digital hierarchy's greatest weakness, and one of SONET's greatest advantages. We'll discuss technology shortly.

In order to drop a DS-1 at its intermediate destination, we have to bring the composite DS-3 into a set of back-to-back DS-3 multiplexers (sometimes called M13 multiplexers). There the ingress mux removes the second set of overhead, finds the DS-2 that the DS-1 we have to drop out is carried in, removes its overhead, finds the right DS-1, drops it out, and then rebuilds the DS-3 frame, including reconstruction of the overhead, before transmitting it on to its next destination. This process is complex, time-consuming, and expensive. So what if we could come up with a method for adding and dropping signal components that eliminated the M13 process entirely? What if we could do it as simply as the process shown in Figure 3-57?

We have. It's called SONET in North America, SDH in the rest of the world, and it dramatically simplifies the world of high-speed transport.

SONET brings with it a subset of advantages that makes it stand above competitive technologies. These include mid-span meet, improved *operations, administration, maintenance, and provisioning* (OAM&P), support for multipoint circuit configurations, nonintrusive facility monitoring, and the capability to deploy a variety of new services. We will examine each of these in turn.

SONET Advantages: Mid-Span Meet

Because of the monopoly nature of early networks, interoperability was a laughable dream. Following the divestiture of AT&T, however, and the realization of Equal Access, the need for interoperability standards became a matter of some priority. Driven largely by MCI, the newly competitive telecommunications industry fought hard for standards that

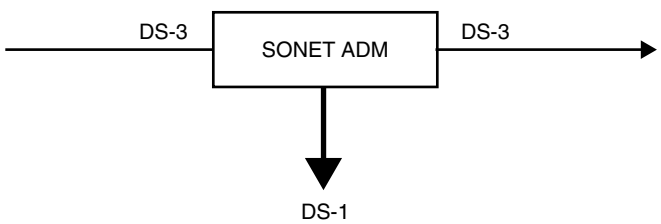


Figure 3-57 A much simplified add-drop process!

would enable different vendors' optical multiplexing equipment to interoperate. This interoperability came to be known as mid-span meet, SONET's greatest contribution to the evolving industry.

Improved OAM&P

Improved OAM&P is without question one of the most important contributions that SONET brings to the networking table. Element and network monitoring, management, and maintenance have always been catch-as-catch-can efforts because of the complexity and diversity of elements in a typical service provider's network. SONET overhead includes error-checking capabilities, bytes for network survivability, and a diverse set of clearly defined management messages.

Multipoint Circuit Support

When SONET was first deployed in the network, the bulk of the traffic it carried derived from point-to-point circuits such as T-1 and DS-3 facilities. With SONET came the capability to hub the traffic, a process that combines the best of cross-connection and multiplexing to perform a capability known as *groom and fill*. This means that aggregated traffic from multiple sources can be transported to a hub, managed as individual components, and redirected out any of several outbound paths without having to completely disassemble the aggregate payload. Prior to SONET, this process required a pair of back-to-back multiplexers, sometimes called an M13 (which stands for "multiplexer that interfaces between DS-1 and DS-3"). This capability, combined with SONET's discreet and highly capable management features, results in a wonderfully manageable system of network bandwidth control.

Nonintrusive Monitoring

SONET overhead bytes are embedded in the frame structure, meaning that they are universally transported alongside the customer's payload. Thus, tight and granular control over the entire network can be realized, leading to more efficient network management and the capability to deploy services on an as-needed basis.

New Services

SONET bandwidth is imminently scalable, meaning that the capability to provision additional bandwidth for customers who require it on an as-needed basis becomes real. As applications evolve to incorporate more and more multimedia content and to therefore require greater volumes of bandwidth, SONET offers it by the bucket load. Already interfaces between SONET and Gigabit Ethernet are being written; interfaces to ATM and other high-speed switching architectures have been in existence for some time already.

SONET Evolution

SONET was initially designed to provide multiplexed point-to-point transport. However, as its capabilities became better understood and networks became "mission-critical," its deployment became more innovative, and soon it was deployed in ring architectures, as shown in Figure 3-58. These rings represent one of the most commonly deployed network topologies. For the moment, however, let's examine a point-to-point deployment. As it turns out, rings don't differ all that much.

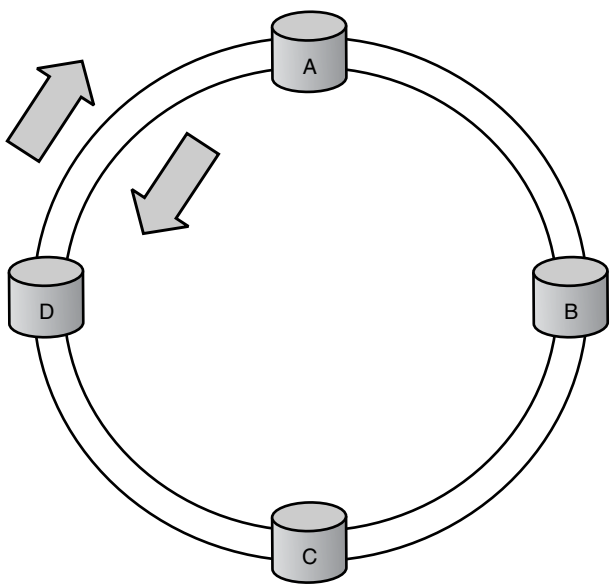


Figure 3-58 Ring architectures used in SONET.

If we consider the structure and function of the typical point-to-point circuit, we find a variety of devices and "functional regions," as shown in Figure 3-59. The components include end devices, multiplexers in this case. These end devices provide the point of entry for traffic originating in the customer's equipment and seeking transport across the network; a full-duplex circuit, which provides simultaneous two-way transmission between the network components; a series of repeaters or regenerators responsible for periodically reframing and regenerating the digital signal; and one or more intermediate multiplexers that serve as nothing more than pass-through devices.

When nonSONET traffic is transmitted into a SONET network, it is packaged for transport through a step-by-step, quasi-hierarchical process that attempts to make reasonably good use of the available network bandwidth and ensures that receiving devices can interpret the data when it arrives. The intermediate devices, including multiplexers and repeaters, also play a role in guaranteeing traffic integrity, and to that end the SONET standards divide the network into three regions: path, line, and section. To understand the differences between the three, let's follow a typical transmission of a DS-3, probably carrying 28 T-1s, from its origination point to the destination.

When the DS-3 first enters the network, the ingress SONET multiplexer packages it by wrapping it in a collection of additional information, called *path overhead*, which is unique to the transported data. For example, it attaches information that identifies the original source of the DS-3 so that it can be traced in the event of network transmission problems, a bit-error control byte, information about how the DS-3 is actually mapped into the payload transport area (and unique to the payload type), an area for network performance and management information,

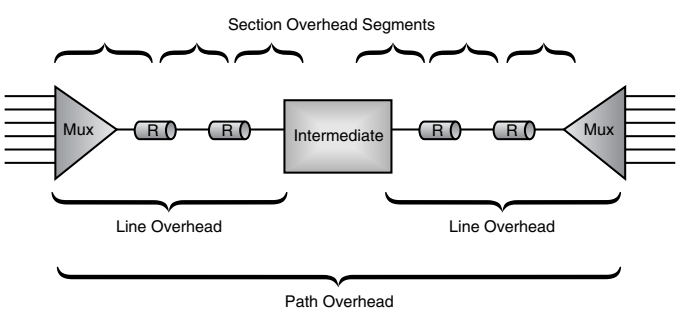


Figure 3-59 SONET network regions and functional devices.

and a number of other informational components that have to do with the end-to-end transmission of the unit of data.

The packaged information, now known as a *payload,* is inserted into a SONET frame, and at that point another layer of control and management information is added, called *line overhead.* Line overhead is responsible for managing the movement of the payload from multiplexer to multiplexer. To do this, it adds a set of bytes that enable receiving devices to find the payload inside the SONET frame. As you will learn a bit later, the payload can occasionally wander around inside the frame due to the vagaries of the network. These bytes enable the system to track that movement.

In addition to these tracking bytes, the line overhead includes bytes that monitor the integrity of the network and can add a switch to a backup transmission span if a failure in the primary span occurs. Line overhead also includes another bit-error-checking byte, a robust channel for transporting network management information, and a voice communications channel that enables technicians at either end of the line to plug in with a handset (sometimes called a butt-in or buttinski) and communicate while troubleshooting.

The final step in the process is to add a layer of overhead that enables the intermediate repeaters to find the beginning of and synchronize a received frame. This overhead, called the *section overhead,* contains a unique initial framing pattern at the beginning of the frame, an identifier for the payload signal being carried, another bit-error check, a voice communications channel, and another dedicated channel for network management information, similar to but smaller than the one identified in the line overhead.

The result of all this overhead, much of which seems like overkill (and in many peoples' minds *is*), is that the transmission of a SONET frame containing user data can be identified and managed with tremendous granularity from the source all the way to the destination.

So, to summarize, the hard little kernel of DS-3 traffic is gradually surrounded by three layers of overhead information, as shown in Figure 3-60, that help it achieve its goal of successfully transiting the network. The section overhead is used at every device the signal passes through, including multiplexers and repeaters, the line overhead is only used between multiplexers, and the information contained in the path overhead is only used by the source and destination multiplexers. The intermediate multiplexers don't care about the specific nature of the payload, because they don't have to terminate or interpret it.

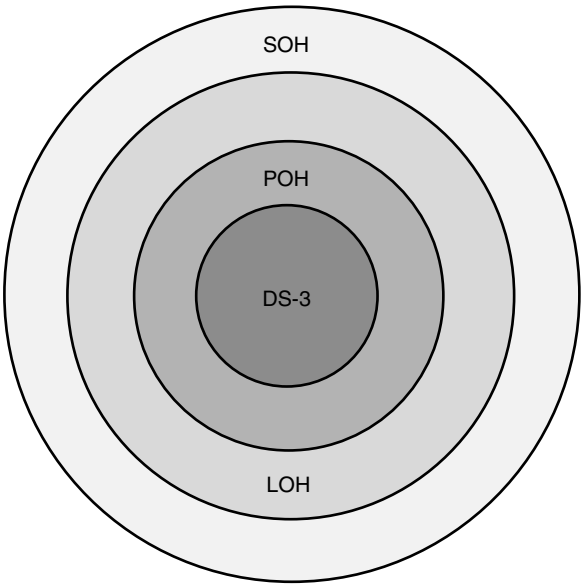


Figure 3-60 Layers of SONET overhead surround the payload prior to transmission.

The SONET Frame

Keep in mind once again that we are doing nothing more complicated than building a T-1 frame with an attitude. Recall that the T-1 frame is comprised of 24 8-bit channels (samples from each of 24 incoming data streams) plus a single bit of overhead. In SONET, we have a similar construct: a lot more channel capacity, and a lot more overhead, but the same functional concept.

The fundamental SONET frame is shown in Figure 3-61 and is known as a *Synchronous Transport Signal, Level One* (STS-1). It is 9 bytes tall and 90 bytes wide, for a total of 810 bytes of transported data, including both user payload and overhead. The first three columns of the frame are the section and line overhead, known collectively as the *transport overhead*. The bulk of the frame itself, to the left, is the *synchronous payload envelope* (SPE), which is the container area for the user data that is being transported. The data, previously identified as the payload, begins somewhere in the payload envelope. The actual starting point will vary, as we will see later. The path overhead begins when the payload begins; because it is unique to the payload itself, it travels closely with the payload. The first byte of the payload is in fact the first byte of the path overhead.

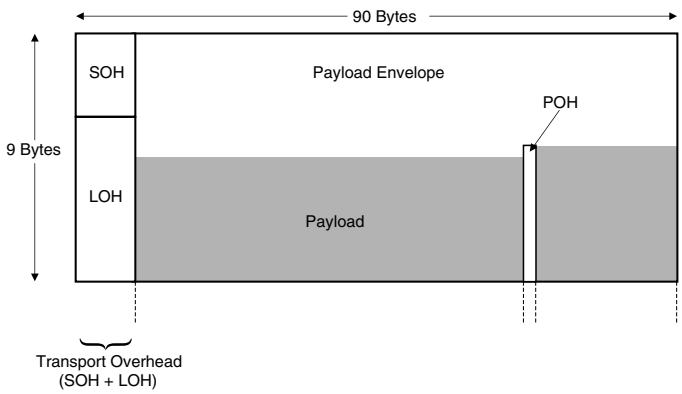


Figure 3-61
Fundamental SONET frame.

A word about nomenclature—two distinct terms are used, often (incorrectly) interchangeably. The terms are *Synchronous Transport Signal* (STS) and *Optical Carrier Level* (OC). They are used interchangeably because although an STS-1 and an OC-1 are both 51.84-Mbps signals, one is an electrically framed signal (STS), while the other describes an optical signal (OC). Keep in mind that the signals that SONET transports usually originate at an electrical source such as a T-1. These data must be collected and multiplexed at an electrical level before being handed over to the optical transport system. The optical networking part of the SONET system speaks in terms of OC.

The SONET frame is transmitted serially on a row-by-row basis. The SONET multiplexer transmits (and therefore receives) the first byte of row one, all the way to the ninetieth byte of row one, and then wraps to transmit the first byte of row two all the way to the ninetieth byte of row two, and so on, until all 810 bytes have been transmitted.

Because the rows are transmitted serially, the many overhead bytes do not all appear at the beginning of the transmission of the frame. Instead, they are peppered along the bitstream like highway markers. For example, the first two bytes of overhead in the section overhead are the framing bytes, followed by the single-byte signal identifier. The next 87 bytes are user payload, followed by the next byte of section overhead. In other words, 87 bytes of user data exist between the first three section overhead bytes and the next one. The designers of SONET were clearly thinking the day they came up with this, because each byte of data appears just when it is needed. Truly a remarkable thing!

Because of the unique way that the user's data is mapped into the SONET frame, the data can actually start pretty much anywhere in the

payload envelope. The payload is always the same number of bytes, which means that if it starts late in the payload envelope, it may well run into the payload envelope of the next frame. In fact, this happens more often than not, but it's OK. SONET is equipped to handle this odd behavior. We'll discuss it shortly.

SONET Bandwidth

The SONET frame consists of 810, 8-bit bytes and, like the T-1 frame, it is transmitted once every 125 seconds (8,000 frames per second). Doing the math, this works out to an overall bit rate of

$$810 \text{ bytes/frame} \times 8 \text{ bits/byte} \times 8{,}000 \text{ frames/second} = 51.84 \text{ Mbps}$$

This is the fundamental transmission rate of the SONET STS-1 frame. That's a lot of bandwidth. 51.84 Mbps is slightly more than a 44.736 Mbps DS-3, a respectable carrier level by anyone's standard. What if more bandwidth is required, however? What if the user wants to transmit multiple DS-3s, or perhaps a single signal that requires more than 51.84 Mbps, such as a 100-Mbps Fast Ethernet signal? Or for that matter, a payload that requires *less* than 51.84 Mbps. In those cases, we have to invoke more of SONET's magic.

The STS-N Frame

In situations where multiple STS-1s are required to transport multiple payloads, all of which fit in an STS-1's payload capacity, SONET enables the creation of what are called STS-N frames, where N represents the number of STS-1 frames that are multiplexed together to create the frame. If three STS-1s are combined, the result is an STS-3. In this case, the three STS-1s are brought into the multiplexer and *byte interleaved* to create the STS-3, as shown in Figure 3-62. In other words, the multiplexer selects the *first* byte of frame one, followed by the *first* byte of frame two, followed by the *first* byte of frame three. Then it selects the *second* byte of frame one, followed by the *second* byte of frame two, followed by the *second* byte of frame three, and so on, until it has built an interleaved frame that is now three times the size of an STS-1: 9×270 bytes instead of 9×90. Interestingly (and impressively), the STS-3 is still generated 8,000 times per second.

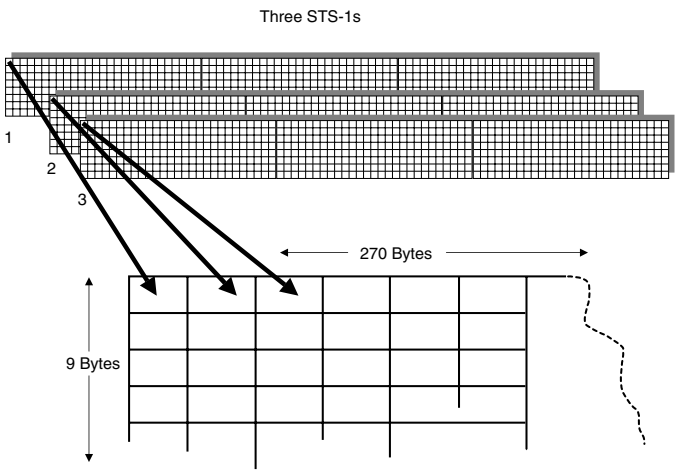


Figure 3-62 Byte inter-leaving in SONET.

The technique described previously is called a *single-stage multiplexing process,* because the incoming payload components are combined in a single step. Also, a two-stage technique is commonly used. For example, an STS-12 can be created in one of two ways. Twelve STS-1s can be combined in a single-stage process to create the byte-interleaved STS-12; alternatively, four groups of three STS-1s can be combined to form four STS-3s, which can then be further combined in a second stage to create a single STS-12. Obviously, two-stage multiplexing is more complex than its single-stage cousin, but both are used.

NOTE: The overall bit rate of the STS-N system is N × STS-1. However, the maximum bandwidth that can be transported is STS-1, but N of them can be transported. This is analogous to a channelized T-1.

The STS-Nc Frame

Let's go back to our Fast Ethernet example mentioned earlier. In this case, 51.84 Mbps is inadequate for our purposes, because we have to transport the 100-Mbps Ethernet signal. For this, we need what is known as a *concatenated signal.* One thing you can say about SONET is that it doesn't hurt your polysyllabic vocabulary.

On the long, lonesome stretches of outback highway in Australia, unsuspecting car drivers often encounter a devilish vehicle known as a road train. Imagine an 18-wheel tractor-trailer (see the top drawing in Figure 3-63 for a remarkable illustration) barreling down the highway at 80 miles per hour, but now imagine that it has six trailers-in effect, a 98-wheeler. These things give passing a whole new meaning. If a road train is rolling down the highway pulling three 50-foot trailers (see the middle drawing in Figure 3-63), then it has the capability to transport 150 feet of cargo, but only if the cargo is segmented into 50-foot chunks.

But what if the trucker wants to transport a 150-foot-long item? In that case, a special trailer must be installed that provides room for the 150-foot payload (see the bottom drawing in Figure 3-63).

If you understand the difference between the second and third drawings, then you understand the difference between an STS-N and an STS-Nc. The word concatenate means "to string together," which is exactly what we do when we need to create what is known as a *super-rate frame* -in other words, a frame capable of transporting a payload that requires more bandwidth than an STS-1 can provide, such as our 100-Mbps Fast Ethernet frame. In the same way that an STS-N is analogous to a channelized T-1, an STS-Nc is analogous to an *unchannelized* T-1. In both cases, the customer is given the full bandwidth that the pipe provides; the difference lies in how the bandwidth is parceled out to the user.

Overhead Modifications in STS-Nc Frames

When we transport multiple STS-1s in an STS-N frame, we assume that they may arrive from different sources. As a result, each frame is inserted into the STS-N frame with its own unique set of overhead.

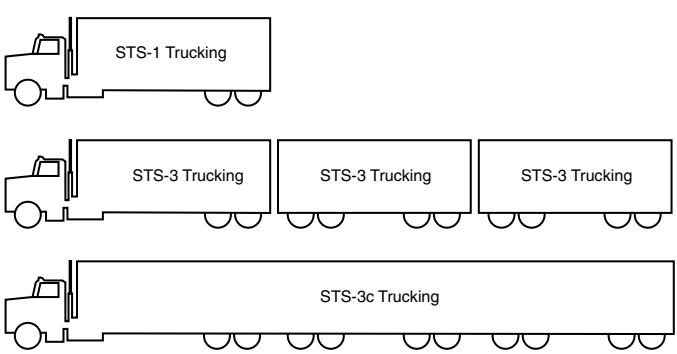


Figure 3-63 Australian road trains and SONET transport.

When we create a concatenated frame, though, the data that will occupy the combined bandwidth of the frame derives from the same source. If we pack a 100-Mbps Fast Ethernet signal into a 155.53-Mbps STS-3c frame, there's only one signal to pack. It's pretty obvious that we don't need three sets of overhead to guide a single frame through the maze of the network.

For example, each frame has a set of bytes that keeps track of the payload within the synchronous payload envelope. Because we only have one payload, therefore we can eliminate two of them. The path overhead that is unique to the payload can also similarly be reduced, since a column of it exists for each of the three formerly individual frames.

In the case of the pointer that tracks the floating payload, the first pointer continues to perform that function; the others are changed to a fixed binary value that is known to receiving devices as a *concatenation indication.* The details of these bytes will be covered later in the overhead section.

Transporting Subrate Payloads: Virtual Tributaries

Let's now go back to our Australian road train example. This time the driver is carrying individual cans of Fosters Beer. From what I remember about the last time I was dragged into an Aussie pub (and it isn't much), the driver could probably only transport about six cans of Fosters per a 50-foot trailer. So, now we have a technique for carrying payloads smaller than the fundamental 50-foot payload size. This analogy works well for understanding SONET's capability to transport payloads that require less bandwidth than 51.84 Mbps, such as T-1 or traditional 10-Mbps Ethernet.

When a SONET frame is modified for the transport of subrate payloads, it is said to carry *virtual tributaries.* Simply put, the payload envelope is chopped into smaller pieces that can then be individually used for the transport of multiple lower-bandwidth signals.

Creating Virtual Tributaries

To create a virtual tributary-ready STS, the synchronous payload envelope is subdivided. An STS-1 comprises 90 columns of bytes, four of which

are reserved for overhead functions (section, line, and path). That leaves 86 for the actual user payload. To create *virtual tributaries* (VTs), the payload capacity of the SPE is divided into seven 12-column pieces called *virtual tributary groups*. Math majors will be quick to point out that $7 \times 12 = 84$, leaving two unassigned columns. These columns, shown in Figure 3-64, are indeed unassigned, and are given the rather silly name of *fixed stuff*.

Now comes the fun part. Each of the VT groups can be further subdivided into one of four different VTs to carry a variety of payload types, as shown in Figure 3-65. A VT1.5, for example, can easily transport a 1.544-Mbps signal within its 1.728-Mbps capacity, with a little room left over. A VT2, meanwhile, has enough capacity in its 2.304-Mbps structure to

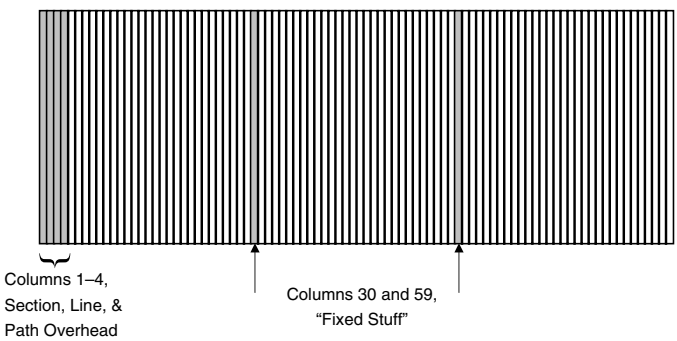


Figure 3-64
SONET "fixed stuff."

VT Type	Columns/VT	Bytes/VT	VTs/Group	VTs/SPE	VT Bandwidth
VT1.5	3	27	4	28	1.728
VT2	4	36	3	21	2.304
VT3	6	54	2	14	3.456
VT6	12	106	1	7	6.912

Figure 3-65
SONET virtual tributary payload transport.

carry a 2.048-Mbps European E-1 signal, with a little room left over. A VT3 can transport a DS-1C signal, while a VT6 can easily accommodate a DS-2, again, each with a little room left over.

One aspect of VTs that must be mentioned is the mix-and-match nature of the payload. Within a single SPE, the seven VT groups can carry a variety of different VTs. However, each VT group can carry only one VT type.

That "little room left over" comment is, by the way, one of the key points that SONET and SDH detractors point to when criticizing them as legacy technologies. Such criticism claims that in these times of growing competition and the universal drive for efficiency, they are inordinately wasteful of bandwidth, given that they were designed when the companies that delivered them were monopolies and less concerned about such things than they are now. We will discuss this issue in a later section of the book. For now, though, suffice it to say that one of the elegant aspects of SONET is its capability to accept essentially any form of data signal, map it into standardized positions within the SPE frame, and transport it efficiently and at a very high speed to a receiving device on the other side of town or the other side of the world.

Creating the Virtual Tributary Superframe

You will recall that when DS-1 frames are transmitted through modern networks today, they are typically formatted into extended superframes in order to eke additional capability out of the comparatively large percentage of overhead space that is available. When DS-1 or other signals are transported via an STS-1 formatted into VT groups, four consecutive STS-1s are grouped together to create a single VT Superframe, as shown in Figure 3-66. To identify the fact that the frames are behaving as a VT Superframe, certain overhead bytes are modified to indicate the change.

NOTE: *For those readers interested in more detail about the SONET overhead, please refer to the bibliography in the Appendix. Several good books on SONET and SDH are listed there.*

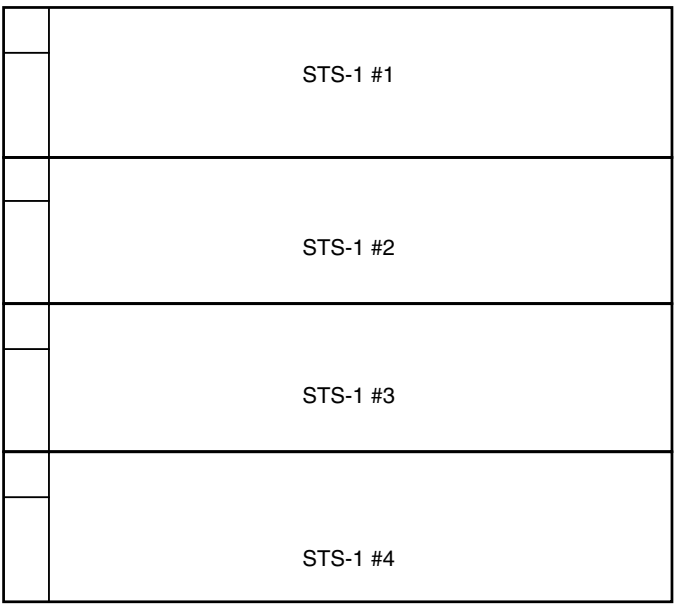


Figure 3-66
VT Superframe.

SONET Synchronization

SONET relies on a timing scheme called *plesiochronous timing*. As implied earlier, the word sounds like one of the geological periods that we all learned in geology classes (Jurassic, Triassic, Plesiochronous, Plasticene). Plesiochronous derives from Greek and means "almost timed." Other words that are commonly tossed about in this industry are *asynchronous* (not timed), *isochronous* (constant delay in the timing), and *synchronous* (timed). SONET is plesiochronous in spite of its name (SYNCHRONOUS Optical Network) because the communicating devices in the network rely on multiple timing sources and are therefore enabled to drift slightly relative to each other. This is fine, because SONET has the capability to handle this with its pointer adjustment capabilities.

The devices in a SONET network have the luxury of choosing from any of five timing schemes to ensure accuracy of the network. As long as the schemes have Stratum 4 accuracy or better, they are perfectly acceptable timing sources. The five are discussed here:

- **Line timing** Devices in the network derive their timing signal from the arriving input signal from another SONET device. For example, an add-drop multiplexer that sits out on a customer's

premises derives its synchronization pulse from the incoming bit stream and might provide further timing to a piece of CPE that is out beyond the ADM.

- **Loop timing** Loop timing is somewhat similar to line timing; in loop timing, the device at the end of the loop is most likely a terminal multiplexer.
- **External timing** The device has the luxury of deriving its timing signal directly from a Stratum 1 clock source.
- **Through timing** Similar to line timing, a device that is through timed receives its synchronization signal from the incoming bit stream, but then forwards that timing signal on to other devices in the network. The timing signal then passes "through" the intermediate device.
- **Free running** In free running timing systems, the SONET equipment in question does not have access to an external timing signal and must derive its timing from internal sources only.

One final point about SONET should be made. When the standard is deployed over ring topologies, two timing techniques are used. Either external timing sources are depended upon to time network elements, or one device on the ring is internally timed (free running) while all the others are through-timed.

SONET Summary

Clearly, SONET is a complex and highly capable standard designed to provide high-bandwidth transport for legacy and new protocol types alike. The overhead that it provisions has the capability to deliver a remarkable collection of network management, monitoring, and transport granularity.

The European *Synchronous Digital Hierarchy* (SDH) shares many of SONET's characteristics, as we will now see. SONET, you will recall, is a limited North American standard, for the most part. SDH, on the other hand, provides high-bandwidth transport for the rest of the world.

Most books on SONET and SDH cite a common list of reasons for their proliferation, including a recognition of the importance of the global marketplace and a desire on the parts of manufacturers to provide devices that will operate in both SONET and SDH environments, the global expansion of ring architectures, a greater focus on network

management and the value that it brings to the table, and massive, unstoppable demand for more bandwidth. To those, add an increasing demand for high-speed routing capability to work hand-in-glove with transport; the deployment of DS-1, DS-3, and E-1 interfaces directly to the enterprise customer as access solutions; and a growth in demand for broadband access technologies such as cable modems, the many flavors of DSL, and two-way satellite connectivity. Reasons for the widespread use of SONET and SDH also include the ongoing replacement of traditional circuit-switched network fabrics with packet-based transport and mesh architectures, a renewed focus on the SONET and SDH overhead with an eye toward using it more effectively, and convergence of multiple applications on a single, capable, high-speed network fabric. Most visible among these is the hunger for bandwidth; according to consultancy RHK, global volume demand will grow from approximately 350,000 terabytes of transported data per month in April 2000 to more than 16 million terabytes of traffic per month in 2003. And who can argue?

SDH Nomenclature

Before launching into a functional description of SDH, it would be good to first cover the differences in naming conventions between the two. This will help to dispel confusion (hopefully!).

The fundamental SONET unit of transport uses a 9-row by 90-column frame that comprises 3 columns of section and line overhead, 1 column of path overhead, and 87 columns of payload. The payload, which is primarily user data, is carried in a payload envelope that can be formatted in various ways to make it carry a variety of payload types. For example, multiple SONET STS-1 frames can be combined to create higher-rate systems for transporting multiple STS-1 streams, or a single higher-rate stream created from the combined bandwidth of the various multiplexed components. Conversely, SONET can transport subrate payloads, known as virtual tributaries, which operate at rates slower than the fundamental STS-1 SONET rate. When this is done, the payload envelope is divided into virtual tributary groups, which can in turn transport a variety of virtual tributary types.

In the SDH world, similar words apply, but they are different enough that they should be discussed. As you will see, SDH uses a fundamental transport "container" that is three times the size of its SONET counterpart. It is a 9-row by 270-column frame that can be configured into one of five container types, typically written C-n(where C means container).

N can be 11, 12, 2, 3, or 4; they are designed to transport a variety of payload types.

When an STM-1 is formatted for the transport of virtual tributaries (known as virtual containers in the SDH world), the payload pointers must be modified. In the case of a payload that is carrying virtual containers, the pointer is known as an *Administrative Unit type 3* (AU-3). If the payload is *not* structured to carry virtual containers but is instead intended for the transport of higher rate payloads, then the pointer is known as an *Administrative Unit type 4* (AU-4). Generally speaking, an AU-3 is typically used for the transport of North American Digital Hierarchy payloads; AU-4 is used for European signal types.

The SDH Frame

To understand the SDH frame structure, it is first helpful to understand the relationship between SDH and SONET. Functionally, they are identical. In both cases, the intent of the technology is to provide a globally standardized transmission system for high-speed data. SONET is indeed optimized for the T-1-heavy North American market, whereas SDH is more applicable to Europe. Beyond that, however, the overhead and design considerations of the two are virtually identical. However, some key differences can be seen.

Perhaps the greatest difference between the two lies in the physical nature of the frame. A SONET STS-1 frame comprises 810 total bytes for an overall aggregate bit rate of 51.84 Mbps, perfectly adequate for the North American 44.736-Mbps DS-3. An SDH STM-1 frame, however, designed to transport a 139.264-Mbps European E-4 or a CEPT-4 signal, must be larger if it is to accommodate that much bandwidth. It clearly won't fit in the limited space available in an STS-1. An STM-1, then, operates at a fundamental rate of 155.52 Mbps, enough for the bandwidth requirements of the E-4. This should be where the déjà vu starts to kick in. Perceptive readers will remember that 155.52 Mbps number from our discussions of the SONET STS-3, which offers *exactly* the same bandwidth. An STM-1 frame is shown in Figure 3-67. It is a byte-interleaved, 9-row by 270-column frame, with the first 9 columns devoted to overhead and the remaining 261 devoted to payload transport.

A comparison of the bandwidth between SONET and SDH systems is also interesting. The fundamental SDH signal is exactly *three times* the bandwidth of the fundamental SONET signal, and this relationship continues all the way up the hierarchy.

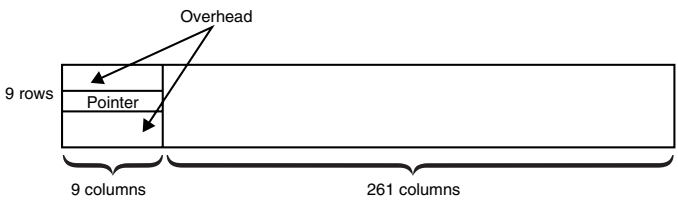


Figure 3-67
An SDH STM-1 frame.

STM Frame Overhead

The overhead in an STM frame is very similar to that of an STS-1 frame, although the nomenclature varies somewhat. Instead of section, line, and path overhead to designate the different regions of the network that the overhead components address, SDH uses the *regenerator section overhead* (RSOH), the *multiplex section overhead* (MSOH), and path overhead, as shown in Figure 3-68. The RSOH occupies the first three rows of nine bytes, and the *multiplex section* the final five. Row four is reserved for the pointer. As in SONET, the path overhead floats gently on the payload tides, rising and falling in response to phase shifts. Functionally, these overhead components are identical to their SONET counterparts.

Overhead Details

Because an STM-1 is three times as large as an STS-1, it has three times the overhead capacity, and nine columns instead of three (plus path overhead). The first row of the RSOH is its SONET counterpart, with the exception of the last two bytes, which are labeled as being reserved for

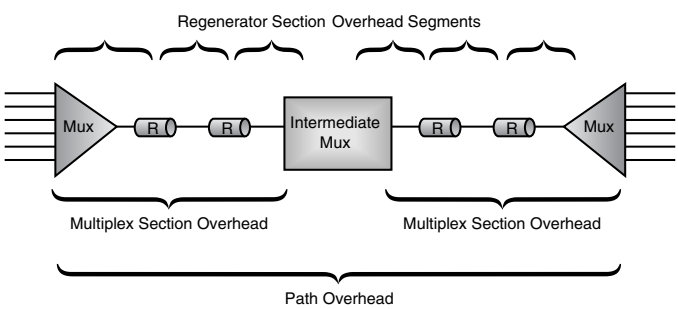


Figure 3-68
SDH Overhead.

national use and are specific to the *Post, Telephone, and Telegraph* (PTT) administration that implements the network. In SONET, they are not yet assigned. The second row is different from SONET in that it has three bytes reserved for media-dependent implementations (differences in the actual transmission medium, whether copper, coaxial, or fiber) and the final two are reserved for national use. As before, they are not yet definitively assigned in the SONET realm.

The final row of the RSOH also sports two bytes reserved for media-dependent information while they are reserved in SONET. All other regenerator section/section overhead functions are identical between the two.

The MSOH in the SDH frame is almost exactly the same as that of the SONET line overhead, with one exception. Row nine of the SDH frame has two bytes reserved for national administration use. They are reserved in the SONET world.

The pointer in an SDH frame is conceptually identical to that of a SONET pointer, although it has some minor differences in nomenclature. In SDH, the pointer is referred to as an *Administrative Unit* (AU) pointer, referring to the standard naming convention described earlier.

SONET and SDH were originally rolled out to replace the T1 and E1 hierarchies, which were suffering from demands for bandwidth beyond what they were capable of delivering. Their principal deliverable was voice, and lots of it. Let's take a moment now to describe the process of voice digitization, still a key component of network transport.

Voice Digitization

The goal of digitizing the human voice for transport across an all-digital network grew out of work performed at Bell Laboratories shortly after the turn of the century. That work led to a discrete understanding of not only the biological nature and spectral makeup of the human voice, but also to a better understanding of language, sound patterns, and the sounded emphases that comprise spoken language.

The Nature of Voice

A typical voice signal comprises frequencies that range from approximately 30 Hz to 10 KHz. Most of the speech energy, however, lies between 300 Hz and 3,300 Hz, the so-called voice band. Experiments

have shown that the frequencies below 1 KHz provide the bulk of recognizability and intelligibility, whereas the higher frequencies provide richness, articulation, and natural sound to the transmitted signal.

The human voice comprises a remarkably rich mix of frequencies, and this richness comes at a considerable price. In order for telephone networks to transmit voice's entire spectrum of frequencies, significant network bandwidth must be made available to every ongoing conversation. A substantial price tag is attached to bandwidth, however; it is a finite commodity within the network, and the more of it that is consumed, the more it costs.

The Network

Thankfully, work performed at Bell Laboratories at the beginning of the twentieth century helped network designers confront this challenge head-on. To understand it, let's take a tour of the telephone network.

The typical network, as shown in Figure 3-69, is divided into several regions: the access plant; the switching, multiplexing, and circuit connectivity equipment (the central office); and the long-distance transport plant. The access and transport domains are often referred to as the *out-*

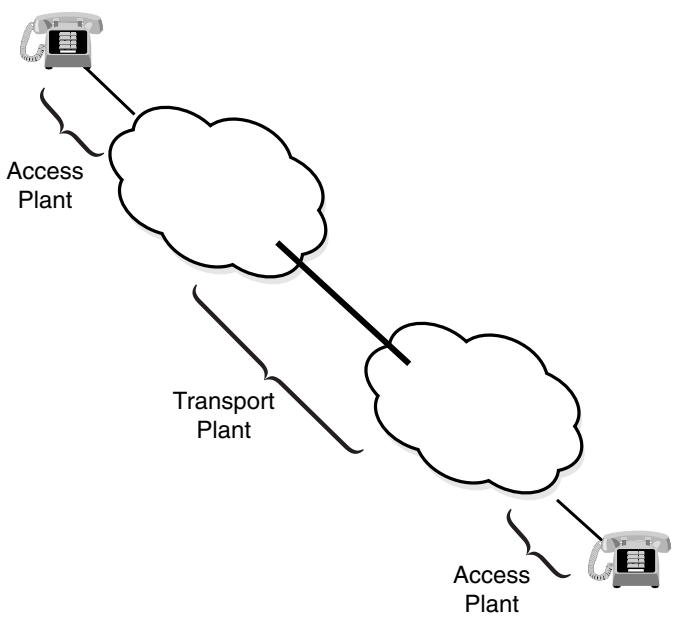


Figure 3-69 Network regions.

side plant, whereas the central office is, conversely, the *inside plant*. The outside plant has the responsibility of aggregating inbound traffic for switching and transport across the long haul as well as terminating traffic at a particular destination. The inside plant, on the other hand, has the responsibility of multiplexing incoming traffic streams, switching the streams, and selecting an outbound path for ultimate delivery to the next central office in the chain or the final destination. Switching therefore is centrally important to the development of the modern network.

Multiplexing

Equally important as the development of the central office switch is the concept of multiplexing, which enables multiple conversations to be carried simultaneously across a single shared physical circuit. The first such systems used *frequency division multiplexing* (FDM), a technique made possible by the development of the vacuum tube, in which the range of available frequencies is divided into chunks that are then parceled out to subscribers.

For example, Figure 3-70 illustrates that subscriber 1 might be assigned the range of frequencies between 0 and 4,000 Hz, whereas subscriber 2 is assigned 4,000 to 8,000 Hz, 3 is given 8,000 to 12,000 Hz, and

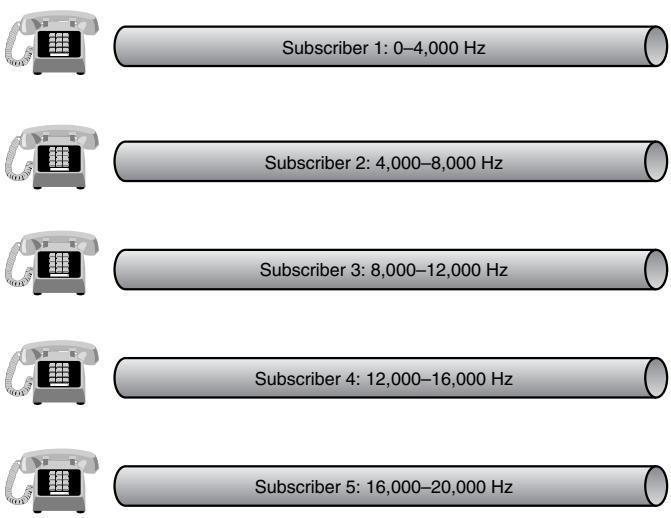


Figure 3-70 Frequency division multiplexing.

so on, up to the maximum range of frequencies available in the channelized system. In FDM, we often observe that users are given "some of the frequency all of the time," meaning that they are free to use their assigned frequency allocation at any time, but may *not* step outside the bounds given to them.

Early FDM systems were capable of transporting 24 4-KHz channels for an overall system bandwidth of 96 KHz. FDM, while largely replaced today by more efficient systems that will be discussed later, is still used in analog cellular telephone and microwave systems, among others.

This model worked well in early telephone systems. Because the lower regions of the 300 to 3,300 Hz voiceband carried the frequency components that enable recognizability and intelligibility, telephony engineers concluded that although the higher frequencies enrich the transmitted voice, they are not necessary for calling parties to recognize and understand each other. This understanding of the makeup of the human voice helped them create a network that was capable of faithfully reproducing the sounds of a conversation while keeping the cost of consumed bandwidth to a minimum. Instead of assigning the full complement of 10 KHz to each end of a conversation, they employed filters to bandwidth-limit each user to approximately 4,000 Hz, a resource savings of some 60 percent. Within the network, subscribers were FDMed across shared physical facilities, thus enabling the telephone company to efficiently conserve network bandwidth.

Time, of course, changes everything. As with any technology, FDM has its downsides. It is an analog technology and therefore suffers from the shortcomings that have historically plagued all transmission systems. The wire over which information is transmitted behaves like a longwire antenna, picking up noise along the length of the transmission path and very effectively homogenizing it with the voice signal. Additionally, the power of the transmitted signal diminishes over distance, and if the distance is far enough, the signal will have to be amplified to make it intelligible at the receiving end. Unfortunately, the amplifiers used in the network are not particularly discriminating; they have no way of separating the voice noise. The result is that they convert a weak, noisy signal into a loud noisy signalbetter, but far from ideal. A better solution was needed.

The better solution came about with the development of *time division multiplexing* (TDM), which became possible because of the transistor and integrated circuit electronics that arrived in the late 1950s and early 1960s. TDM is a digital transmission scheme, which implies a small number of discrete signal states, rather than the essentially infinite

range of values employed in analog systems. Although digital systems are as susceptible to noise impairment as their analog counterparts, the discrete nature of their binary signaling makes it relatively easy to separate the noise from the transmitted signal. In digital carrier systems, only three valid signal values are used: one positive, one negative, and zero. Anything else is construed to be noise. It is therefore a trivial exercise for digital repeaters to discern what is desirable and what is not, thus eliminating the problem of cumulative noise. The role of the regenerator, as shown is Figure 3-71, is to receive a weak, noisy digital signal, remove the noise, reconstruct the original signal, and amplify it before transmitting the signal onto the next segment of the transmission facility. For this reason, repeaters are also called *regenerators*, because that is precisely the function they perform.

One observation: it is estimated that as much as 60 percent of the cost of building a transmission facility lies in the regenerator sections of the span. For this reason, optical networking, discussed a bit later, has various benefits, not the least of which is the capability to reduce the number of regenerators required on long transmission spans. In a typical network, these regenerators must be placed approximately every 6,000 feet along a span, which means that a considerable expense is involved when providing regeneration along a long-haul network.

Digital signals, often called square waves, comprise a rich mixture of signal frequencies. Not to bring too much physics into the discussion, we must at least mention the Fourier series, which describes the makeup of a digital signal. The Fourier series is a mathematical representation of the behavior of waveforms. Among other things, it notes the following fact. If we start with a fundamental signal, such as that shown in Figure 3-72, and mathematically add to it its odd harmonics (a harmonic is defined as a wave with a frequency that is a whole-number multiple of another wave), we see a rather remarkable thing happening. The waveform gets steeper on the sides and flatter on top. As we add more and more of the odd harmonics (which, after all, are infinite), the wave begins to look like the typical square wave. Now, of course, there is no such thing as a true square wave. For our purposes, though, we'll accept the fact.

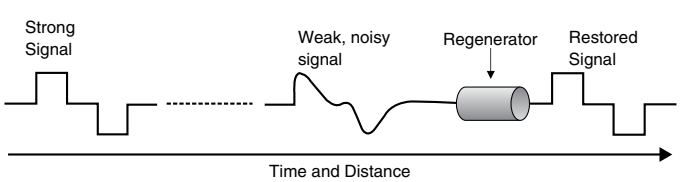


Figure 3-71
Role of the regenerator.

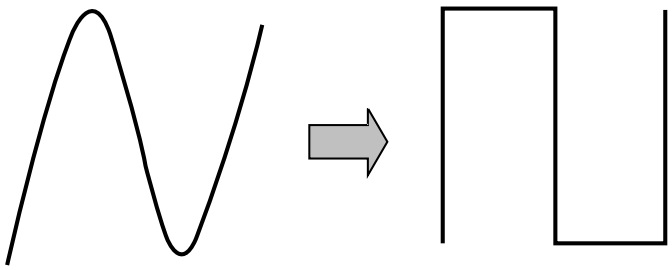


Figure 3-72 Fourier transform of analog wave to digital wave.

It should now be intuitive to the reader that digital signals comprise a mixture of low-, medium-, and high-frequency components, which means that they cannot be transmitted across the bandwidth-limited 4-KHz channels of the traditional telephone network. In digital carrier facilities, the equipment that restricts the individual transmission channels to 4-kHz chunks is eliminated, thus giving each user access to the full breadth of available spectrum across the shared physical medium. In frequency division systems, we observed that we give users some of the frequency all of the time." In time division systems, we turn that around and give users *all* of the frequency *some* of the time. As a result, high-frequency digital signals can be transmitted without restriction.

Digitization brings with it a cadre of advantages, including improved voice and data transmission quality, better maintenance and troubleshooting capabilities (and therefore reliability), and dramatic improvements in configuration flexibility. In digital carrier systems, the TDM is known as a channel bank. Under normal circumstances, it enables either 24 or 30 circuits to share a single, four-wire facility. The 24-channel system is called a T-Carrier, whereas the 30-channel system, used in most of the world, is called an E-Carrier. Originally designed in 1962 as a way to transport multiple channels of voice over expensive transmission facilities, they soon became useful as data transmission networks as well. That, however, came later. For now, we'll focus on voice.

Voice Digitization

The process of converting analog voice to a digital representation in the modern network is a logical and straightforward process. It comprises four distinct steps: *Pulse Amplitude Modulation* (PAM) sampling, in which the amplitude of the incoming analog wave is sampled every

125 microseconds; companding, during which the values are weighted toward those most receptive to the human ear; quantization, in which the weighted samples are given values on a nonlinear scale; and finally encoding, during which each value is assigned a distinct binary value. Each of the stages of *Pulse Code Modulation* (PCM) will now be discussed in detail.

Pulse Code Modulation (PCM)

Thanks to the work performed by Harry Nyquist at Bell Laboratories in the 1920s, we know that to optimally represent an analog signal as a digitally encoded bitstream, the analog signal must be sampled at a rate that is equal to twice the bandwidth of the channel over which the signal is to be transmitted. Since each analog voice channel is allocated 4 KHz of bandwidth, it follows that each voice signal must be sampled at twice that rate, or 8,000 samples per second. In fact, that is precisely what happens in T-Carrier systems, which we now use to illustrate our example.

The standard T-Carrier multiplexer accepts inputs from 24 analog channels, as shown in Figure 3-73. Each channel is sampled in turn every one-eight thousandth of a second in a round-robin fashion, resulting in the generation of 8,000 pulse amplitude samples from each channel every second. The sampling rate is important. If the sampling rate is too high, too much information is transmitted, and bandwidth is wasted; if the sampling rate is too low, then we run the risk of aliasing. Aliasing is the interpretation of the sample points as a false waveform, due to the paucity of samples.

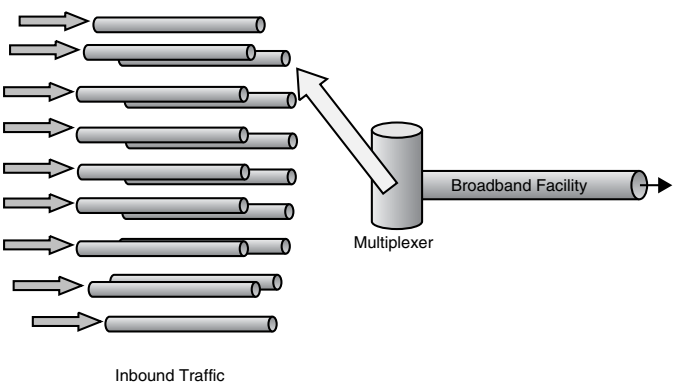


Figure 3-73
Time division multiplexing.

This PAM process represents the first stage of PCM, the process by which an analog baseband signal is converted to a digital signal for transmission across the T-Carrier network. This first step is shown in Figure 3-74.

The second stage of PCM, shown in Figure 3-75, is called quantization. In quantization, we assign values to each sample within a constrained range. For illustration purposes, imagine what we now have before us. We have "replaced" the continuous analog waveform of the signal with a series of amplitude samples that are close enough together that we can discern the shape of the original wave from their collective amplitudes. Imagine also that we have graphed these samples in such a way that the "wave" of sample points meanders above and below an established zero point on the x-axis, so that some of the samples have positive values and others are negative, as shown.

The amplitude levels enable us to assign values to each of the PAM samples, although a glaring problem with this technique should be obvious to the careful reader. Very few of the samples actually line up *exactly* with the amplitudes delineated by the graphing process. In fact, most of them fall *between* the values, as shown Figure 3-75. It doesn't take much of an intuitive leap to see that several of the samples will be assigned the same digital value by the *coder-decoder* (CODEC) that performs this function, yet they are clearly *not* the same amplitude. This inaccuracy in the measurement method results in a problem known as *quantizing*

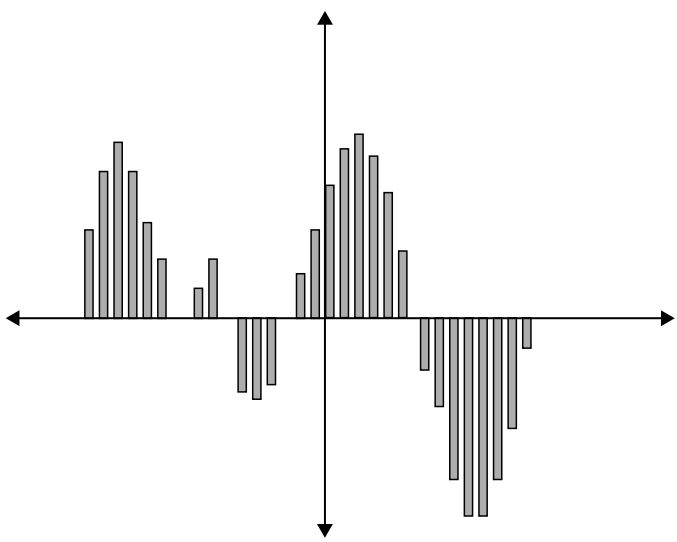


Figure 3-74
PAM samples.

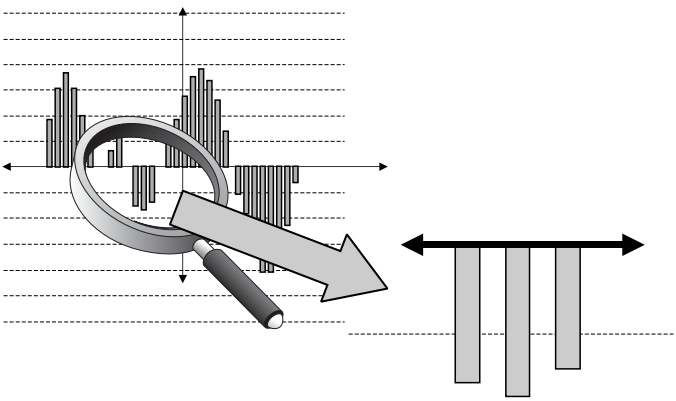


Figure 3-75
Quantizing the samples.

noise and is inevitable when linear measurement systems, such as the one suggested by Figure 3-75, are employed in CODECs.

Needless to say, design engineers recognized this problem rather quickly, and equally quickly came up with an adequate solution. It is a fairly well-known fact among psycholinguists and speech therapists that the human ear is far more sensitive to discrete changes in amplitude at low volume levels than it is at high volume levels, a fact not missed by the network designers tasked with optimizing the performance of digital carrier systems intended for voice transport. Instead of using a linear scale for digitally encoding the PAM samples, they designed and employed a nonlinear scale that is weighted with much more granularity at low volume levels—that is, close to the zero line—than at the higher amplitude levels. In other words, the values are extremely close together near the x-axis, and get farther and farther apart as they travel up and down the y-axis. This nonlinear approach keeps the quantizing noise to a minimum at the low amplitude levels where hearing sensitivity is the highest and enables it to creep up at the higher amplitudes, where the human ear is less sensitive to its presence. It turns out that this is not a problem, because the inherent shortcomings of the mechanical equipment (microphones, speakers, the circuit itself) introduce slight distortions at high amplitude levels that hide the effect of the nonlinear quantizing scale.

This technique of compressing the values of the PAM samples to make them fit the nonlinear quantizing scale results in a bandwidth savings of more than 30 percent. In fact, the actual process is called *companding,* because the sample is first compressed for transmission, and then expanded for reception at the far end, hence the term.

The actual graph scale is divided into 255 distinct values above and below the zero line. In North America and Japan, the encoding scheme is known as μ-Law (Mu-Law). The rest of the world relies on a slightly different standard known as A-Law.

Eight segments can be found above the line and eight below (one of which is the shared zero point). Each segment, in turn, is subdivided into 16 steps. A bit of binary mathematics now enables us to convert the quantized amplitude samples into an 8-bit value for transmission. For the sake of demonstration, let's consider a negative sample that falls into the thirteenth step in segment five. The conversion would take on the following representation:

1 101 1101

where the initial 0 indicates a negative sample, 101 indicates the fifth segment, and 1101 indicates the thirteenth step in the segment. We now have an 8-bit representation of an analog amplitude sample that can be transmitted across a digital network and then be reconstructed with its many counterparts as an accurate representation of the original analog waveform at the receiving end. This entire process is known as PCM, and the result of its efforts is often referred to as toll-quality voice.

Alternative Digitization Techniques

Although PCM is perhaps the best-known, high-quality voice digitization process, it is by no means the only one. Advances in coding schemes and improvements in the overall quality of the telephone network have made it possible for encoding schemes to be developed that use far less bandwidth that traditional PCM. In this next section, we will consider some of these techniques.

Adaptive Differential Pulse Code Modulation (ADPCM)

Adaptive Differential Pulse Code Modulation (ADPCM) is a technique that enables toll-quality voice signals to be encoded at a half rate (32 Kbps) for transmission. ADPCM relies on the predictability that is

inherent in human speech to reduce the amount of information required. The technique still relies on PCM encoding, but adds an additional step to carry out its task.

The 64-Kbps PCM-encoded signal is fed into an ADPCM transcoder, which considers the *prior* behavior of the incoming stream to predict the behavior of the *next* sample. Here's where the magic happens: instead of transmitting the actual value of the predicted sample, it encodes in 4 bits and transmits the *difference* between the actual and predicted samples. Since the difference from sample to sample is typically quite small, the results are generally considered to be very close to toll-quality. This 4-bit transcoding process, which is based on the known behavior characteristics of human voice, enables the system to transmit 8,000 4-bit samples per second, thus reducing the overall bandwidth requirement from 64 to 32 Kbps.

It should be noted that ADPCM works well for voice, because the encoding and predictive algorithms are based upon its behavior characteristics. It does not, however, work as well for higher bit rate data (above 4800 bps), which has an entirely different set of behavior characteristics.

Continuously Variable Slope Delta (CVSD)

Continuously Variable Slope Delta (CVSD) is a unique form of voice encoding that relies on the values of individual bits to predict the behavior of the incoming signal. Instead of transmitting the volume (height or y-value) of PAM samples, CVSD transmits information that measures the changing slope of the waveform. So, instead of transmitting the actual change itself, it transmits the *rate* of change.

To perform its task, CVSD uses a reference voltage to which it compares all incoming values. If the incoming signal value is less than the reference voltage, the CVSD encoder reduces the slope of the curve to make its approximation better mirror the slope of the actual signal. If the incoming value is *more* than the reference value, then the encoder will increase the slope of the output signal, again causing it to approach and therefore mirror the slope of the actual signal. With each recurring sample and comparison, the step function can be increased or decreased as required.

For example, if the signal is increasing rapidly, then the steps are increased one after the other in a form of step function by the encoding algorithm. Obviously, the reproduced signal is not a particularly exact representation of the input signal. In practice, it is pretty jagged. Filters therefore are used to smooth the transitions.

CVSD is typically implemented at 32 Kbps, although it can be implemented at rates as low as 9600 bps. At 16 to 24 Kbps, recognizability is still possible. Down to 9600, recognizability is seriously affected, although intelligibility is not.

Linear Predictive Coding (LPC)

We mention *Linear Predictive Coding* (LPC) here only because it has carved out a niche for itself in certain voice-related applications such as voice mail systems, automobiles, aviation, and electronic games that speak to children. LPC is a complex process, implemented completely in silicon, which enables voice to be encoded at rates as low as 2400 bps. The resulting quality is far from toll-quality, but it is certainly intelligible and its low bit rate capability gives it a distinct advantage over other systems.

LPC relies on the fact that each sound created by the human voice has unique attributes, such as frequency range, resonance, and loudness, among others. When voice samples are created in LPC, these attributes are used to generate prediction coefficients. These predictive coefficients represent linear combinations of previous samples, hence the name, *Linear* Predictive Coding.

Prediction coefficients are created by taking advantage of the known *formants* of speech, which are the resonant characteristics of the mouth and throat, which give speech its characteristic timbre and sound. This sound, referred to by speech pathologists as the "buzz," can be described by both its pitch and its intensity. LPC therefore models the behavior of the vocal cords and the vocal tract itself.

To create the digitized voice samples, the buzz is passed through an inverse filter that is selected based upon the value of the coefficients. The remaining signal, after the buzz has been removed, is called the residue.

In the most common form of LPC, the residue is encoded as either a *voiced* or *unvoiced* sound. Voiced sounds are those that require vocal cord vibration, such as the *g* in *glare,* the *b* in *boy,* or the *d* and *g* in *dog.* Unvoiced sounds require no vocal cord vibration, such as the *h* in *how,* the *sh* in *shoe,* or the *f* in *frog.* The transmitter creates and sends the prediction coefficients, which include measures of pitch, intensity, and whatever voiced and unvoiced coefficients are required. The receiver undoes the process. It converts the voice residue, pitch, and intensity coefficients into a representation of the source signal, using a filter similar to the one used by the transmitter to synthesize the original signal.

Digital Speech Interpolation (DSI)

Human speech has many measurable (and therefore predictable) characteristics, one of which is a tendency to have embedded pauses. As a rule, people do not spew out a series of uninterrupted sounds. They tend to pause for emphasis, to collect their thoughts, or to reword a phrase while the other person listens quietly on the other end of the line. When speech technicians monitor these pauses, they discover that during considerably more than half of the total connect time the line is silent.

Digital Speech Interpolation (DSI) takes advantage of this characteristic silence to drastically reduce the bandwidth required for a single channel. Whereas 24 channels can be transported over a typical T-1 facility, DSI enables as many as 120 conversations to be carried over the same circuit. The format is proprietary and requires the setting aside of a certain amount of bandwidth for overhead.

A form of statistical multiplexing lies at the heart of DSI's functionality. Standard T-Carrier is a TDM scheme in which channel ownership is assured. A user assigned to channel three will *always* own channel three, regardless of whether they are actually using the line. In DSI, channels are not owned. Instead, large numbers of users share a pool of available channels. When a user starts to talk, the DSI system assigns an available timeslot to that user and notifies the receiving end of the assignment. This system works well when the number of users is large, because statistical probabilities are more accurate and indicative of behavior in larger populations than in smaller ones.

DSI has a downside, of course, and it comes in several forms. *Competitive clipping* occurs when more people start to talk than there are available channels, resulting in someone being unable to talk. *Connection clipping* occurs when the receiving end fails to learn which channel a conversation has been assigned within a reasonable amount of time, resulting in signal loss.

Two approaches have been created to address these problems, both of which are widely utilized in DSI systems. In the case of competitive clipping, the system intentionally clips off the front end of the initial word of the second person who speaks. This technique is not optimal, but does prevent the loss of the conversation and also obviates the problem of clipping out the middle of a conversation, which would be more difficult for the speakers to recover from. The loss of an initial syllable or two can be mentally reconstructed far more easily than sounds in the middle of a sentence.

A second technique for recovering from clipping problems is to temporarily reduce the encoding rate. The typical encoding rate for DSI is 32 Kbps. In certain situations, the encoding rate may be reduced to 24 Kbps, thus freeing up significant bandwidth for additional channels.

Summary

A few years ago, while filming a video about telephony on location in Texas, I interviewed a small town sheriff about his use of telecommunications technology in his job. I wanted to know how it has changed the way he does his job.

"Well, sir," he began, puffing out his chest and sticking his thumbs into his waistband, "we use telecommunications all the time. We use our radios and cell phones in the cars, and our telephones there to talk here in town and for long distance. And now," he said, patting a fax machine on his desk, "we've got backup." I wasn't sure what he meant by that, so I asked. "We've always had trouble with the phones goin' out around here, and that was a bad thing. Can't very well do our job if we can't talk. But now we've got this here fax machine." I was puzzled. I was missing his point, so I probed a little deeper. "Don't you get it, son? Before, if we lost the phones, we were like fish outta water. Now, I know that if the phones go down, I can always send a fax."

Unfortunately, many peoples' understanding of the inner workings of the telephone network is at about the same level as the understanding of the sheriff (who was a wonderful guy, by the way. I set him straight on his understanding of the telephone network and he treated me to the best chicken fried steak I have ever eaten). Hopefully, this chapter and those that follow are helping to lift the haze a bit.

We will return to the central office several times as we examine the data transport side of telecommunications, but for now, on to access.

CHAPTER 4

Premises Technologies

This chapter addresses the network devices found in a typical premises environment, including computers, wired and wireless *local area networks* (LANs), and a number of other options. We begin with an examination of a typical computer. In one way or another, the computer is the ultimate premises technology device. In one form or another, the computer appears in every device used by a customer to access the network.

The Computer

For all its complexity, the typical computer only has a small number of components, as shown in Figure 4-1. These are the *central processing unit* (CPU), main memory, secondary memory, *input/output* (I/O) devices, and a parallel bus that ties all the components together. It also has two types of software that make the computer useful to a human. The first is application software such as word processors, spreadsheet applications, presentation software, and MP3 encoders. The second is the operating system that manages the goings-on within the computer, including hardware component inventory and file locations. In a sense, it is the executive assistant to the computer itself; some mainframe manufacturers refer to their operating system as the EXEC.

The concept of building modular computers came about in the 1940s when Hungarian-born mathematician John Von Neumann applied the work he had done in logic and game theory to the challenge of building large electronic computers (see Figure 4-2). As one of the primary contributors to the design of the *Electronic Numerical Integrator and Calculator* (ENIAC), Von Neumann introduced the concept of stored program control and modular computing, the design under which all modern computers are built today. A personal computer's internals are shown in Figure 4-3.

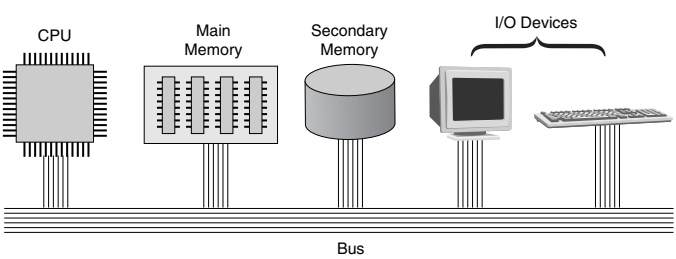


Figure 4-1 Computer components.

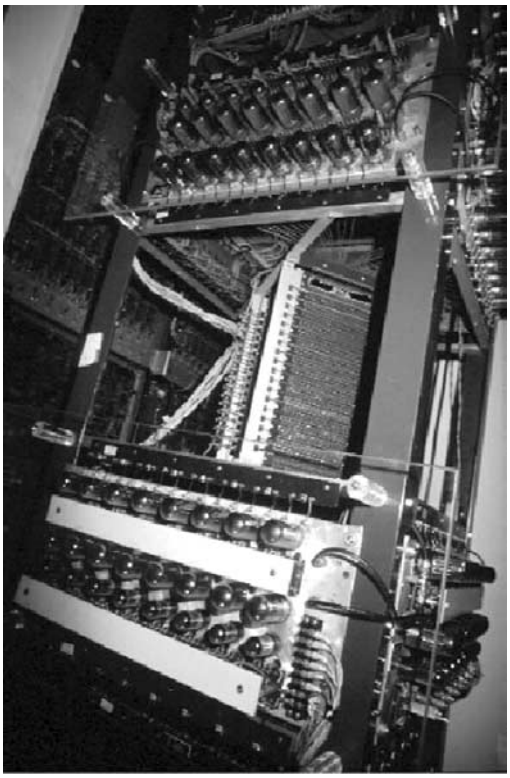


Figure 4-2
A section of the original ENIAC machine.

The CPU

The CPU is the brain of the computer. Its job is to receive data input from the I/O devices (keyboard, mouse, modem, and so on), manipulate the data in some way based on a set of commands from a resident application, and package the newly gerrymandered data for presentation to a human user at another I/O device (monitor). The CPU has its own set of sub-components. These include a clock, an *arithmetic-logic unit* (ALU), and registers. The clock is the device that provides synchronization and timing to all devices in the computer, and it is characterized by the number of clock cycles per second it is capable of generating. These cycles are called Hertz. Modern systems today operate at 850 to 1,000 Megahertz, or MHz. The faster the clock, the faster the machine can perform computing operations.

The ALU is the specialized silicon intelligence in the CPU that performs the mathematical permutations that make the CPU useful. All

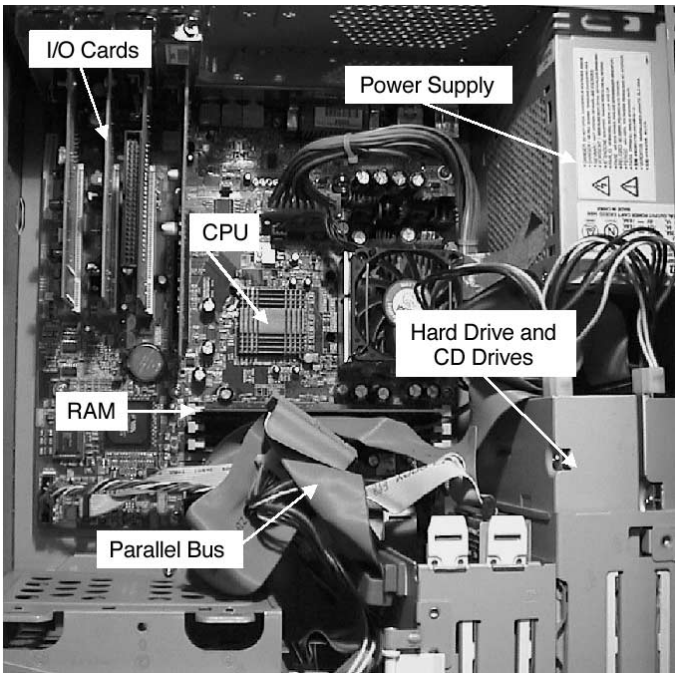


Figure 4-3
PC internals showing major components.

functions performed by a computer—word processing, spreadsheets, multimedia, videoconferencing—are viewed by the computer as mathematical functions and are therefore executed as such. It is the job of the ALU to carry out these mathematical permutations.

Registers are nothing more than very fast memory located close to the ALU for rapid I/O functions during execution cycles.

Main Memory

Main memory, sometimes called *Random Access Memory* (RAM), is another measure of the "goodness" of a computer today. RAM is the segment of memory in a computer used for execution space and as a place to store operating system, data, and application files that are in current use. RAM is silicon-based, solid-state memory and is extremely fast in terms of access speed. It is, however, volatile. When the PC is turned off, or power is lost, whatever information is stored in RAM disappears. When basic computer skills courses tell students to "save often," this is the reason. When a computer user is writing a document in a word

processor, or populating a spreadsheet, or manipulating a digital photograph, the file lives in RAM until the person saves, at which time it is written to Main memory, which is nonvolatile, as we'll see in a moment. Modern systems typically have a minimum of 128 *Megabytes* (MB) of RAM.

Secondary Memory

Secondary memory has become a very popular line of business in the evolving PC market. It provides a mechanism for the long-term storage of data files and is nonvolatile; when the power goes away, the information it stores does not. Secondary memory tends to be a much slower medium in terms of access time than Main memory because it is usually mechanical in nature, whereas Main memory is solid-state.

Consider, for example, the hard drive shown in Figure 4-4, which chose a hot July day to fail, right in the middle of writing this book (and yes, I had backed up—saved—often). That's why the disk platters are exposed. Notice that the drive comprises three platters and an armature upon which are mounted read/write heads similar to those used in cassette decks of yore.

Figure 4-5 is a schematic diagram that more clearly illustrates how hard drives actually work. The platters, typically made of aluminum and cast to extremely exacting standards, are coated with iron oxide identical to that found on recording tape. Adjacent to the platters, which are

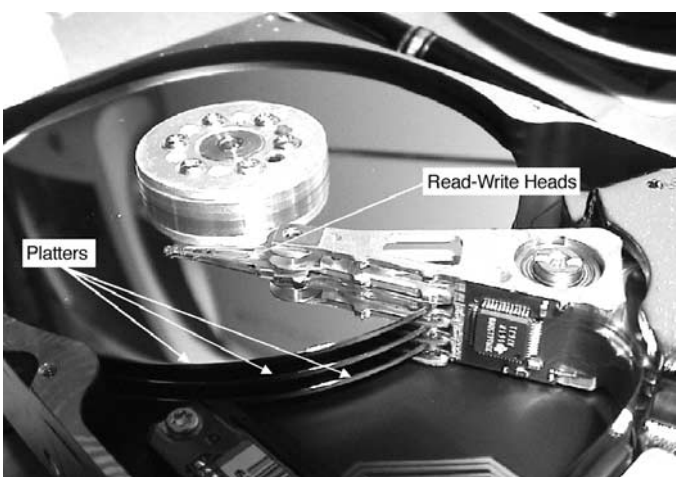


Figure 4-4 Close-up of a hard drive, showing platters and read-write head armature.

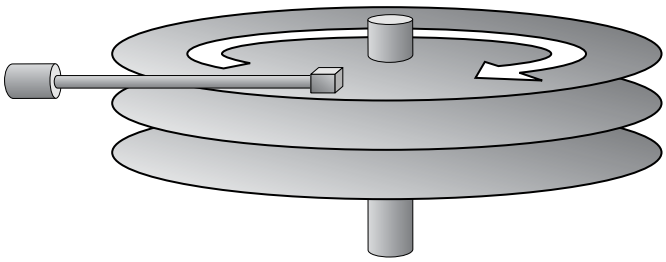


Figure 4-5 Schematic diagram of a hard drive. As the platters spin, the read-write heads access the magnetized surfaces of each platter, reading and writing information

mounted on a spindle attached to a high-speed motor, is an armature upon which is mounted a stack of read-write heads that write information to the disk surfaces and read information from the disk surfaces.

Remember when we were discussing the importance of saving often when working on a computer? The save process reads information stored temporarily in RAM, transports the information to the disk controller, which in turn, under the guidance of the operating system, transmits the information to the write heads, which in turn write the bits to the disk surface by magnetizing the iron oxide surface. Of course, once the bits have been written to the disk, it's important to keep track of where the information is stored on the disk. This is a function of the *operating system* (OS).

Have you ever inserted a floppy into a drive or (far less fun) a new hard drive into a computer, as I recently had to do, and had the computer ask you if you're sure you want it to format the drive? To keep track of where files are stored on a disk, whether it is a hard drive, a CD, a Zip drive, or a floppy, the operating system marks the disk with a collection of road markers that help it find the "beginning" of the disk so that it can use that as a reference. Obviously, there is no beginning on a circle by design. By creating an arbitrary start point, however, the operating system can then find the files it stores on the drive. This start point is called the *File Allocation Table* (FAT). If the FAT goes away for some reason, the operating system will not be able to find files stored on the drive. When my hard drive failed, my initial indication that something bad was about to happen was an ominous message that appeared during the boot cycle that said "UNABLE TO FIND FAT TABLE."

When the operating system formats a disk, it logically divides the disk into what are called cylinders, tracks, and sectors, as shown in Figure 4-6. It then uses those delimiters as a way to store and recall files on a drive using three dimensions. When the *operating system* (OS) writes the file to the disk surface, every possibility exists (in fact it is likely) that the file will not be written to the surface in a contiguous stream of bits. Instead, the file may be broken into pieces, each of which may be written on a different part of the disk array. The pieces are linked together by the operating system using a series of pointers, which tell the OS where to go to get the next piece of the file when the time comes to retrieve it. The pointer, of course, is a cylinder: track: sector indication.

Cylinders, tracks, and sectors are relatively easy to understand. A track is a single writeable path on one platter of the disk array. A cylinder is a "stack of tracks" on multiple platters, and a sector is a "pie slice" of the disk array. With a little imagination, it is easy to see how a file can be stored or located on a disk by tracking those three indicators.

It should also be easy to see now how some of those wonderful applications like Norton Utilities work. When you direct your computer to erase a file, it doesn't really erase it; it just removes the pointers so that it is no longer a "registered" file and can no longer be found on the hard drive. What file restore utilities do is remember where the pointers were when you told the computer to erase the file. That way, when you beg the computer to find the file after you've done something stupid (this is where many people kill the chicken and light candles), the utility has a trivial task: simply restore the pointers. As long as there hasn't been too

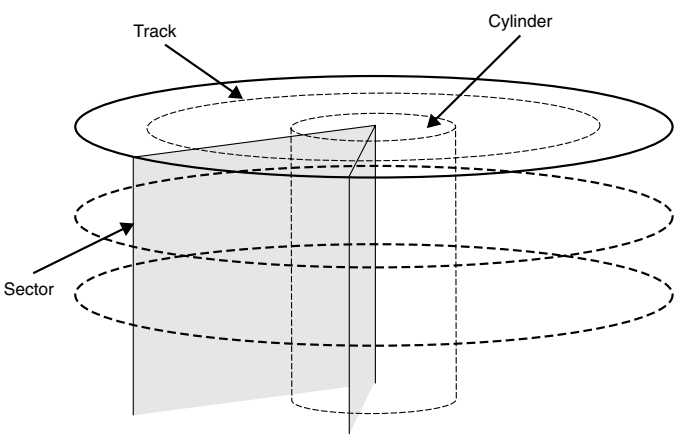


Figure 4-6
Cylinders, tracks, and sectors on a typical disk.

much disk activity since the deletion and the file hasn't been overwritten, it can be recovered.

Another useful tool is the disk optimization utility. It keeps track of the files and applications that you, the user, access most often while also keeping track of the degree of fragmentation that the files stored on the disk are experiencing. Think about it: when disks start to get full, there is less of a chance that the OS will find a single contiguous piece of writeable disk space and will therefore have to fragment the file before writing it to the disk.

Disk optimization utilities perform two tasks. First, they rearrange files on the disk surface so that those accessed most frequently are written to new locations close to the spindle, which spins faster than the outer edge of the disk and are therefore accessible more quickly. Second, they rearrange the file segments and attempt to reassemble files or at least move them closer to each other so that they can be more efficiently managed.

Okay, enough about hard drive anatomy. Other forms of secondary memory include those mentioned earlier: writeable CDs, Zip disks, floppies, and nonvolatile memory arrays. As I mentioned, this has become a big business because these products make it relatively easy for users to back up files and keep their systems running efficiently.

Input/Output (I/O) Devices

I/O devices are those that provide an interface between the user and the computer and include mice, keyboards, monitors, printers, scanners, modems, speakers, and any other devices that take data into or spit data out of the computer.

The Bus

Interconnecting the components of the computer is a cable known as a *parallel bus*. It is called parallel because the bits that make up one or more 8-bit bytes travel down the bus beside each other on individual rather than one after the next as in a serial cable on a single conductor. Both are shown schematically in Figure 4-7.

The advantage of a parallel bus is speed. By pumping multiple bits into a device in the computer simultaneously, the device, such as a CPU, can process them faster. Obviously, the more leads there are in the bus,

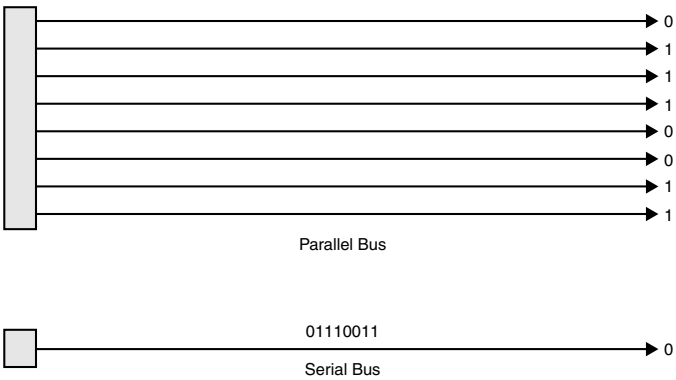


Figure 4-7
Parallel and serial buses.

the more bits can be transported. It should come as no surprise, then, that another differentiator of computers today is the width of the bus. A 32-bit bus is four times faster than an 8-bit bus. As long as the internal device to which the bus is transporting data has as many I/O leads as the bus, it can handle the higher volume of traffic. The parallel bus does not have to be a flexible gray cable; for those devices that are physically attached to the main printed circuit board (often called the motherboard), the parallel bus is extended as wire leads that are etched into the surface of the motherboard. Devices such as I/O cards attach to the board via edge connectors.

Enough about computer internals. A brief word about computer history and evolution is now in order. The work performed by Von Neumann and his contemporaries led to the development of the modern mainframe computer (see Figure 4-8) in the 1960s and its many succeeding machine design generations. Targeted primarily at corporate applications, the mainframe continues to provide computing services required by most corporations: access to enormous databases, security, and support for hundreds of simultaneous users. These systems host enormous disk pools (see Figure 4-9) and tape libraries (see Figure 4-10) and are housed in totally self-contained windowless computer centers. Their components are interconnected by large cables that require that they be installed on raised floors (see Figure 4-11). They produce so much heat that they are fed enormous amounts of chilled air and water, and require constant attention and monitoring. It makes sense; these are very powerful creatures.

Over time, computer technology advanced and soon a new need arose. Mainframes were fine for the computing requirements of large, homogeneous user communities, but as the technology became cheaper and more

Figure 4-8
Mainframe computers in a "clean room" environment. No people work on this floor; the machines are controlled from another area.

Figure 4-9
Mainframe disk pool, sometimes called a "DASD (Direct Access Storage Device) Farm."

ubiquitous, the applications for which computers could be used became more diverse. Soon a need arose for smaller machines that could be used in more specialized departmental applications, and in the 1970s, thanks to companies like Xerox, Digital Equipment Corporation (DEC), and Data General, the minicomputer was born (see Figure 4-12). The minicomputer made it possible for individual departments in a corporation or even small corporations to take charge of their own computer destinies and not be shackled to the centralized data centers of yore. It carried with it a price, of course. Not only did these companies or organizations lose their dependency on the data center, but they also lost the centralized support that came with it. So, this evolution had its downside.

Figure 4-10 Tape library. Many data centers now use cartridges that look like the old 8-track tapes and hold significantly more data than the reels shown here.

Figure 4-11 Raised floor, showing cables below.

The real evolution, of course, came with the birth of the personal computer. Thanks to Bill Gates and his concept of a simple operating system such as DOS and Steve Jobs with his vision of "computing for the masses," truly ubiquitous computing became a reality. From the perspective of the individual user, this evolution was unparalleled. The

Figure 4-12
Minicomputers.

Figure 4-13
The ALTAIR 8800 computer. Photo courtesy Jim Willing, The Computer Garage.

revolution began in January 1975 with the announcement of the MITS Altair (see Figure 4-13). Built by *Micro Instrumentation and Telemetry Systems* (MITS) in Albuquerque, New Mexico, the Altair was designed around the Intel 8080 microprocessor and a specially designed 100-pin connector. The machine ran a BASIC operating system developed by Bill Gates and Paul Allen. In effect, MITS was Microsoft's first customer.

The Altair was really a hobbyist's machine, but soon the market shifted to a small business focus. Machines like the Apple, Osborne, and Kaypro were smaller and offered integrated keyboards and video displays. In 1981, of course, IBM entered the market with the DOS-based personal PC, and soon the world was a very different place. Apple

followed with the Macintosh and the first commercially available *graphical user interface* (GUI), and the rest, as they say, is history. Soon corporations embraced the PC. "A chicken in every pot, a computer on every desk" seemed to be the rallying cry for *information technologies* (IT) departments everywhere.

This evolution also had a downside, of course. The arrival of the PC heralded the arrival of a new era in computing that enabled every individual to have his or her own applications, file structures, and data. The good news was that each person now controlled his or her own individual computer resources; the bad news was that each person now controlled his or her own individual computer resources. Suddenly, the control was gone; instead of having *a copy* of the database, there were now as many copies as there were users. This led to huge problems.

Furthermore, PC proliferation led to another challenge: connectivity, or lack of it. Whereas before, every user had electronic access to every other user via the mainframe or minicomputer-based network that hooked everyone together, the PC did not have that advantage.

PCs also eliminated the efficiency with which expensive network resources such as printers could be shared. Some of you may remember the days when being the person in the office with the laser printer attached to your machine was akin to approaching a state of Nirvana. You were able to do your work and print anytime you wanted, except, of course, for the disruption caused by all of those people standing behind you with floppy disks in their hands promising you that "It's only one page—it'll just take a second."

Thus was born the term *sneakernet*. In order to print something you had to put the document on a diskette (probably a 5¼-inch floppy, back when floppies really were floppy), walk over to the machine with the directly attached printer, and beg and wheedle for permission to print the file, not the most efficient technique for sharing a printer. Something else was needed. That something was the *local area network* (LAN).

LAN Basics

A LAN is exactly what the name implies: a physically small network, typically characterized by high-speed transports, low error rates, and private ownership, which serves the data transport needs of a geographically small community of users. Most LANs provide connectivity, resource sharing, and transport services within a single building,

although they can operate within the confines of multiple buildings on a campus.

When LANs were first created, the idea was to design a network option that would provide a low-cost solution for transport. Up until their arrival, the only transport option available was a dedicated private line from the telephone company or X.25 packet switching. Both were expensive, and X.25 was less reliable than was desired. Furthermore, the devices being connected together were relatively low-cost devices; it simply didn't make sense to interconnect them with expensive network resources. That would defeat the purpose of the LAN concept.

All LANs, regardless of the access mechanism, share certain characteristics. All rely on some form of transmission medium that is shared among all the users on the LAN, all use some kind of interrupt and contention protocol to ensure that all devices get an equal opportunity to use the shared medium, and all have some kind of software called a *Network Operating System* (NOS) that controls the environment.

All LANs have the same basic components, as shown in Figure 4-14. A collection of devices such as PCs, servers, and printers serves as the interface between the human user and the shared medium. Each of these machines hosts a device called a *network interface card* (NIC), which provides the physical connectivity between the user device and the shared medium. The NIC is either installed inside the system or, less commonly, as an external device. In laptop machines, the NIC is a PC card that plugs into a slot in the machine, shown in Figure 4-15.

The NIC device implements the access protocol that devices wanting to access the shared medium use on their particular LAN. These access schemes will be discussed shortly. The NIC also provides the connectivity required to attach a user device to the shared network.

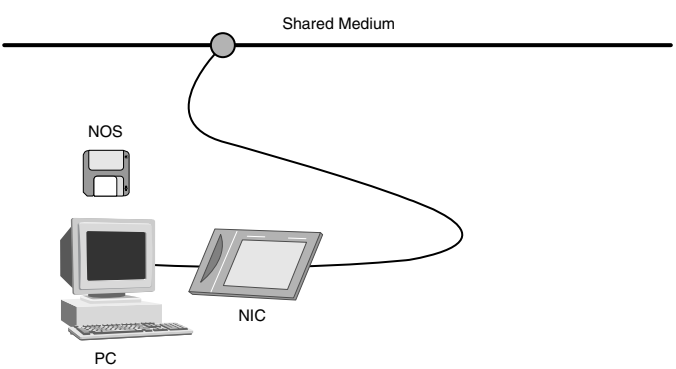


Figure 4-14
Typical LAN components.

Figure 4-15
A PC-card Network Interface Card (NIC).

Topologically, LANs differ greatly. The earliest LANs used a bus architecture, shown in Figure 4-16, so-called because they were literally a long run of twisted pair wire or coaxial cable to which stations were periodically attached. Attachment was easy; in fact, early coax systems relied on a device called a vampire tap, which poked a hole in the insulation surrounding the center conductor in order to suck the digital blood from the shared medium. Later designs such as IBM's Token Ring used a contiguous ring architecture such as that shown in Figure 4-17. Both have their advantages and will be discussed later in this chapter.

Later designs combined the best of both topologies to create star-wired LANs (see Figure 4-18), also discussed later.

LAN Access Schemes

Local area networks have traditionally fallen into two primary categories characterized by the manner in which they access the shared transmission medium (shared among all the devices on the LAN). The first, and most common, is called *contention,* and the second group is called *distributed polling.* I tend to refer to contention-based LANs as the

Figure 4-16
A Bus-based LAN.

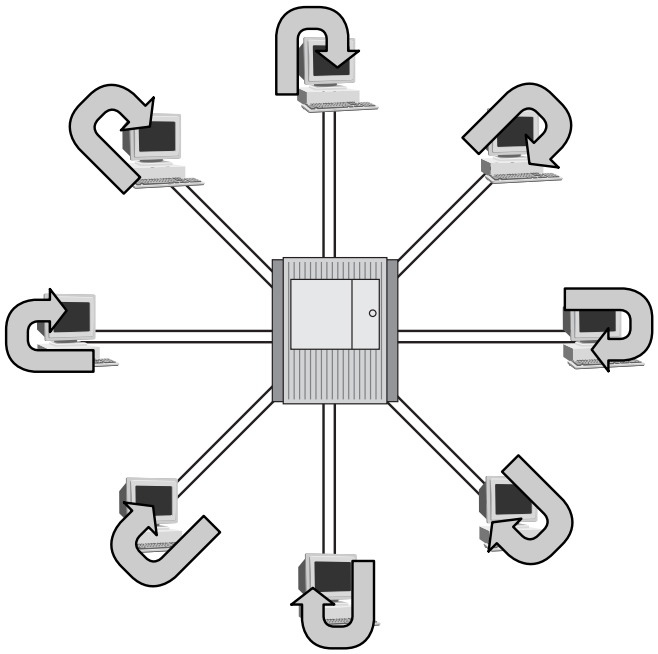


Figure 4-17
A ring-based LAN.

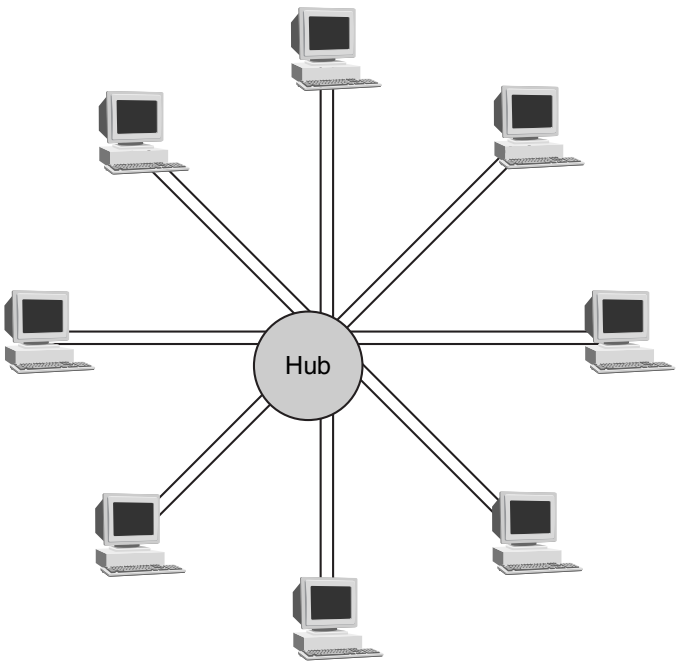


Figure 4-18
A star-wired LAN.

Berkeley Method, while I view distributed polling LANs as users of the Harvard Method. I'll explain in a moment.

Contention-Based LANs

Someday, on a whim, I may send this letter to 3Com fouder Bob Metcalfe:

Dear Mr. Metcalfe,
We're not sure how to break this to you, but we have discovered that your claim of a patent for the invention of Ethernet must be denied after the fact due to its existence prior to the date of your claim of invention. There is a small freshwater fish, Gymnarchus niloticus, that uses an interesting technique for locating mates, food, and simply communicating with peers. The fish's body is polarized, with a "cathode" on its head and an "anode" on its tail. Using special electric cells in its body similar to those employed by the electric eel or the California electric ray, Gymnarchus emits nominal 300-Hz, 10-volt pulses, which reflect back and inform the fish about its immediate environment.

In the event that two Gymnarchus are in the same area, their emissions interfere with one another (intersymbol interference?), rendering their detection mechanisms ineffective. But, being the clever creatures that they are, Gymnarchus has designed a technique to deal with this problem. When the two fish "hear" each other's transmissions, they both immediately stop pulsing. Each fish waits a measurably random period of time while continuing to swim, after which they begin to transmit again, but this time at slightly different frequencies to avoid interference.

We hope that you understand that under the circumstances we cannot in good conscience grant this patent.

Sincerely yours,
U.S. Patent Office

I don't think a fish can hold a patent, but if it could, *niloticus* would hold the patent for a widely used technique called *Carrier Sense Multiple Access with Collision Detection* (CSMA/CD). Please read on.

Perhaps the best-known contention-based medium access scheme is Ethernet, a product developed by 3Com founder and Xerox PARC veteran Bob Metcalfe. In contention-based LANs, devices attached to the network vie for access using the technological equivalent of gladiatorial combat. "If it feels good, do it" is a good way to describe the manner in which they share access (hence, the Berkeley method). If a station wants

to transmit, it simply does so, knowing that there exists the possibility that the transmitted signal may collide with the signal generated by another station that transmits at the same time. Even though the transmissions are electrical and are occurring on a LAN, some delay occurs between the time that both stations transmit and the time that they both realize that someone else has transmitted. This realization is called a collision and it results in the destruction of both transmitted messages, as shown in Figure 4-19.

In the event that a collision occurs as the result of simultaneous transmission, both stations back off by immediately stopping their transmissions, waiting a random amount of time, and trying again. This technique has the wonderful name of *truncated binary exponential backoff*. It's one of those phrases you just have to commit to memory because it sounds so good when you casually let it roll off the tongue in conversation.

Ultimately, each station will get a turn to transmit, although how long they may have to wait is based on how busy the LAN is. Contention-based systems are characterized by what is known as *unbounded delay,* because no upward limit exists on how much delay a station can incur as it waits to use the shared medium. As the LAN gets busier and traffic increases, the number of stations vying for access to the shared medium, which only enables a single station at a time to use it by the way, also goes up, which naturally results in more collisions. Collisions translate into wasted bandwidth, so LANs do everything they can to avoid them.

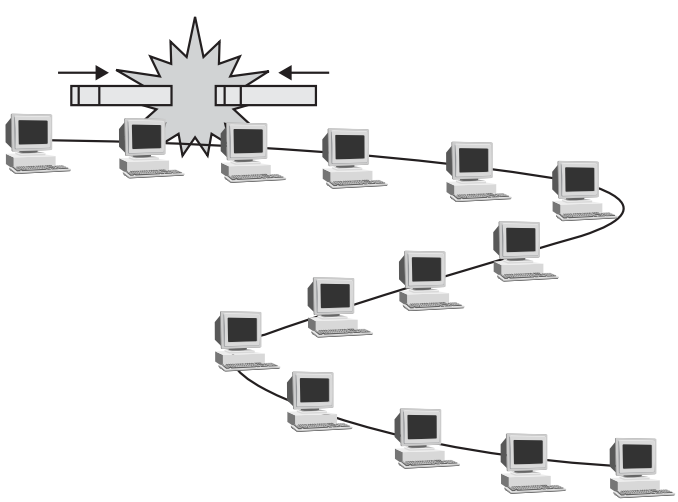


Figure 4-19
A collision on a contention-based LAN.

We will discuss techniques for this in the contention world a bit later in this chapter.

Contention-based LANs employ CSMA/CD, in which a station observes the following guidelines when attempting to use the shared network. First, it listens to the shared medium to determine whether it is in use or not; that's the Carrier Sense part of the name. If the LAN is available (not already in use), it begins to transmit, but continues to listen while it is transmitting, knowing that another station could also choose to transmit at the same time; that's the Multiple Access part. In the event that a collision is detected, usually indicated by a dramatic increase in the signal power measured on the shared LAN, both stations back off and try again. That's the Collision Detection part.

Ethernet is the most common example of a CSMA/CD LAN. Originally released as a 10-Mbps product based on *Institute of Electrical and Electronics Engineers'* (IEEE) standard 802.3, Ethernet rapidly became the most widely deployed LAN technology in the world. As bandwidth-hungry applications such as E-Commerce, *Enterprise Resource Planning* (ERP), and Web access evolved, transport technologies advanced, and bandwidth availability (and capabilities) grew, 10-Mbps Ethernet began to show its age. Today new versions of Ethernet have emerged that offer 100-Mbps (Fast Ethernet) and 1,000-Mbps (Gigabit Ethernet) transport, with plans afoot for even faster versions. Furthermore, in keeping with the demands being placed on LANs by convergence, standards are evolving for LAN-based voice transport that guarantee quality of service for mixed traffic types.

Gigabit Ethernet is still in a somewhat nascent stage, but most believe that it will experience a high uptake rate as its popularity climbs. Dataquest predicts that Gigabit Ethernet sales will grow to $2.5 billion by 2002; this is a reasonable number, considering that 2 million ports were sold in 1999 with expectations of hitting a total installed base of 18 million by 2002. Emerging applications certainly make the case for Gigabit Ethernet's bandwidth capability. LAN telephony, server interconnection, and video to the desktop all demand low-latency solutions, and Gigabit Ethernet may be positioned to provide it. A number of vendors have entered the marketplace, including Alcatel, Lucent Technologies, Nortel Networks, and Cisco Systems.

The other aspect of the LAN environment that has begun to show weaknesses is the overall topology of the network itself. LANs are broadcast environments, which means that when a station transmits, every station on the LAN segment hears the message (see Figure 4-20). Although this is a simple implementation scheme, it is also

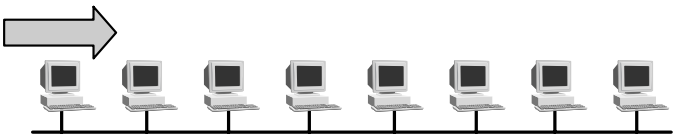


Figure 4-20
When one station transmits, all stations hear the message. This can result in significant waste of bandwidth.

wasteful of bandwidth, since stations hear broadcasts that they have no reason to hear.

In response to this, a technological evolution has occurred. It was obvious to LAN implementers that the traffic on most LANs was somewhat domain-oriented; that is, it tended to cluster into communities of interest based on the work groups using the LAN. For example, if employees in sales shared a LAN with shipping and order processing, three discernible traffic groupings emerged according to what network architects call the 80:20 Rule. The 80:20 Rule simply states that 80 percent of the traffic that originates in a particular work group tends to stay in that work group, an observation that makes network design distinctly simpler. If the traffic naturally tends to segregate itself into groupings, then the topology of the network could change to reflect those groupings. Thus was born the bridge.

Bridges are devices with the responsibility of filtering traffic that has to propagate in the forward direction as well as traffic that does not. For example, if the network described previously were to have a bridge inserted in it (see Figure 4-21), all the employees in each of the three work groups would share a LAN segment, and each segment would be attached to a port on the bridge. When an employee in sales transmits a message to another employee in sales, the bridge is intelligent enough to know that the traffic does not have to be forwarded to the other ports. Similarly, if the sales employee now sends a message to someone in shipping, the bridge recognizes that the sender and receiver are on different segments and thus forwards the message to the appropriate port, using address information in a table that it maintains (the filter/forward database). Bridges operate at layer two of the OSI Model and, as such, are frame switches.

Following close on the heels of bridging is a relatively new technique called *LAN switching*. LAN switching qualifies as "bridging on steroids."

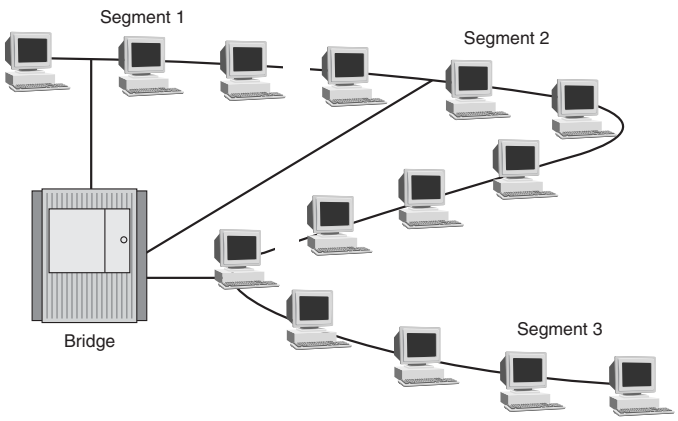


Figure 4-21
Using a bridge to segment a LAN.

In LAN switching, the filter/forward database is distributed; that is, a copy of it exists at each port, which implies that different ports can make simultaneous traffic-handling decisions. This enables the LAN switch to implement full-duplex transmissions, reduce overall throughput delays, and in some cases implement per-port rate adjustments. The first 10-Mbps Ethernet LAN switches emerged in 1993, followed closely by Fast Ethernet (100-Mbps) versions in 1995 and Gigabit Ethernet (1,000-Mbps) switches in 1997. Fast Ethernet immediately stepped up to the marketplace bandwidth challenge and was quickly accepted as the next generation of Ethernet.

LAN switching also helped to propagate the topology called *star wiring*. In a star-wired LAN, all stations are connected by wire runs back to the LAN switch or a hub that sits in the geographical center of the network, as shown in Figure 4-22. Any access scheme (contention-based or distributed polling) can be implemented over this topology, because it defines a wiring plan, not a functional design. Because all stations in the LAN are connected back to a center point, management, troubleshooting, and administration of the network is simplified.

Contention-based LANs are the most commonly deployed LAN topologies. Distributed polling environments, however, do have their place.

Distributed Polling LANs

In addition to the gladiatorial combat approach to sharing access to a transmission facility, a more civilized technique is known as distributed

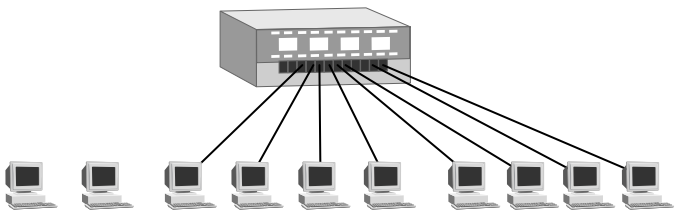


Figure 4-22
LAN switching.

polling or, as it is more commonly known, *token passing*. IBM's token-passing ring is perhaps the best known of these products, followed closely by the *Fiber Distributed Data Interface* (FDDI), a 100-Mbps version occasionally seen in campus and *metropolitan area networks* (MANs), although the sun seems to be setting on FDDI.

In token-passing LANs, stations take turns with the shared medium, passing the right to use it from station to station by handing off a token that gives the bearer the one-time right to transmit while all other stations remain quiescent (thus, the Harvard approach). This is a much fairer way to share access to the transmission medium than CSMA/CD because although every station has to wait for its turn, it is absolutely guaranteed that it will get that turn. These systems are therefore characterized by bounded delays, because any station will only have to wait for the token for a certain amount of time.

Token-passing rings work as shown in Figure 4-23. When a station wants to transmit a file to another station on the LAN, it must first wait for the token, a small and unique piece of code that must be held by a station to validate the frame of data that is created and transmitted.

Let's assume for a moment that a station has secured the token because a prior station has released it. The station places the token in the appropriate field of the frame it builds (actually, the *medium access control* [MAC] scheme, which is implemented on the NIC card that builds the frame), adds the data and address, and transmits the frame to the next station on the ring. The next station, which also has a frame it wants to send, receives the frame, notes that it is not the intended recipient, and also notes that the token is busy. It does not transmit, but instead passes the frame of data from the first station on to the next station.

This process continues, station by station, until the frame arrives at the intended recipient on the ring. The recipient validates that it is the intended recipient, at which time it makes a copy of the received frame, sets a bit in the frame to indicate that it has been successfully received,

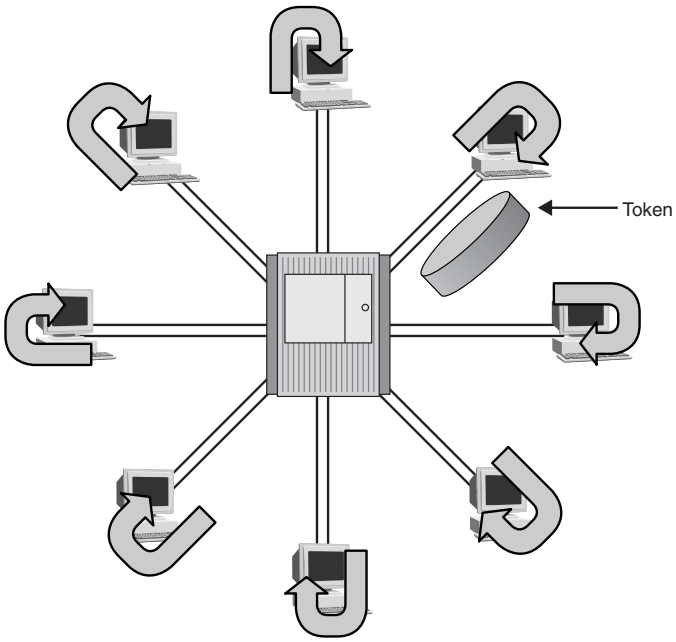


Figure 4-23
A token-passing, distributed polling LAN.

leaves the token set as busy, and transmits the frame on to the next station on the ring. Because the token is still shown as busy, no other station can transmit. Ultimately, the frame returns to the originator, at which time it is recognized as having been received correctly. The station therefore removes the frame from the ring, frees the token, and passes it on to the next station (it is not allowed to send again just because it is in possession of a free token).

This is where the overall fairness scheme of this technique shines through. The very next station to receive a free token is the station that first indicated a need for it. It will transmit its traffic, after which it will pass the token on to the next station on the ring, followed by the next station, and so on.

This technique works very well in situations where high traffic congestion on the LAN is the norm. Stations will always have to wait for what is called *maximum token rotation time,* that is, the amount of time it takes for the token to be passed completely around the ring, but they will *always* get a turn. Thus, for high-congestion situations, a token-passing environment may be better.

Traditional Token Ring LANs operate at two speeds, 4 and 16 Mbps. Like Ethernet, these speeds were fine for the limited requirements of

text-based LAN traffic that was characteristic of early LAN deployments. However, as demand for bandwidth climbed, the need to eliminate the bottleneck in the Token-Ring domain emerged and Fast Token Ring was born. In 1998, the IEEE 802.5 committee (the oversight committee for Token-Ring technology) announced draft standards for 100-Mbps high-speed Token Ring (HSTR 802.5t). A number of vendors stepped up to the challenge and began to produce high-speed Token-Ring equipment, including Madge Networks and IBM.

Gigabit Token Ring is on the horizon as draft standard 802.5v, and although it may become a full-fledged product, many believe that it may never reach commercial status because of competition from the far less expensive Gigabit Ethernet.

Logical LAN Design

One other topic that should be covered before we conclude our discussion of LANs is logical design. Two designs have emerged over the years for LAN data management. The first is called *peer-to-peer*. In a peer-to-peer LAN, shown in Figure 4-24, all stations on the network operate at the same protocol layer, and all have equal access *at any time* to the shared medium and other resources on the network. They do not have to wait for any kind of permission to transmit; they simply do so. Traditional CSMA/CD is an example of this model. It is simple, easy to implement, and does not require a complex operating system to operate. It does, however, result in a free-for-all approach to networking, and in large networks it can result in security and performance problems.

The alternative and far more commonly seen technique is called *client-server*. In a client-server LAN, all data and application resources are archived on a designated server that is attached to the LAN and is accessible by all stations (user PCs) with appropriate permissions, as

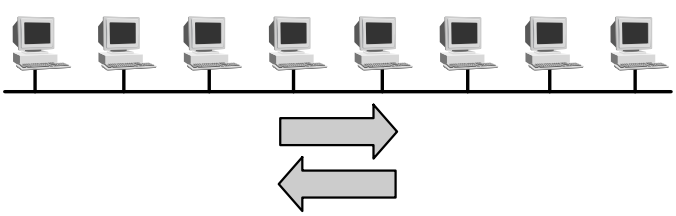


Figure 4-24
A peer-to-peer LAN.

illustrated in Figure 4-25. Because the server houses all of the data and application resources, client PCs do not have to be particularly robust. When a user wants to execute a program such as a word processor, they go through the same keystrokes they would on a standalone PC. In a client-server environment, however, the application actually executes on the server, giving the user the appearance of local execution.

Data files modified by the user are also stored on the server, resulting in a significant improvement in data management, cost control, security, and "software harmonization," compared to the peer-to-peer design. This also means that client devices can be relatively inexpensive, because they need very little in the way of onboard computing resources. The server, on the other hand, is really a PC with additional disk, memory, and processor capacity so that it can handle the requests it receives from all the users that depend on it. Needless to say, client-server architectures are more common today than peer-to-peer in corporate environments.

Deployment

So when should Ethernet be used as opposed to Token Ring? Both have their advantages and disadvantages, both have solid industry support, and both are manufactured by a number of respectable, well-known players. CSMA/CD (for all intents and purposes, Ethernet) is far and away the most widely deployed LAN technology because it is simple, inexpensive, and capable of offering very high bandwidth to any marketplace,

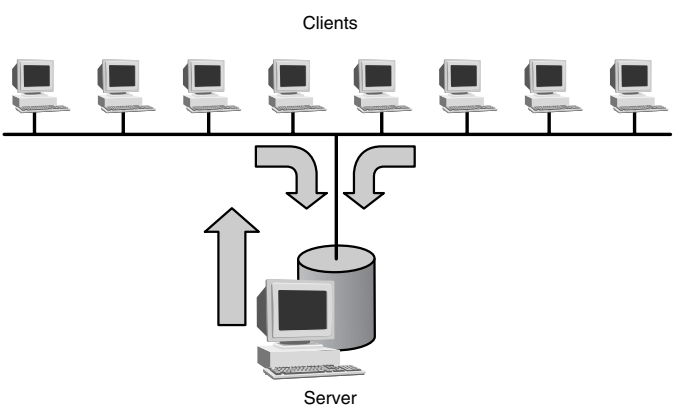


Figure 4-25
A client-server LAN.

including residential. I am writing this in my home office on a PC that is connected to a 100-Mbps Ethernet LAN that ties together three PCs and a couple of printers, and the total cost of the network, including the router and firewall that protects the machines from intrusion due to the always-on connection through the cable modem, is less than $200.

Most businesses use Ethernet today because most businesses have normal traffic flows—office automation traffic and the like. For businesses that experience constant, bandwidth-intensive traffic, such as that found in engineering firms, architectural enterprises, or businesses with other graphics-heavy traffic, Token Ring may be a better choice, although some will argue. Businesses that already have a large installed base of IBM hardware may also be good candidates for Token Ring, since it integrates well (for obvious reasons) into IBM environments. Even still, Ethernet is ruling the roost.

802.11

Another variation on the LAN theme that is experiencing a great deal of attention today is 802.11, the set of standards that address wireless LAN considerations. IEEE 802.11 is a wireless LAN standard developed by the IEEE's 802 committee to specify an air interface between a wireless client and a base station, as well as among a variety of wireless clients. First discussed in 1990, the standard has evolved through six draft versions and won final approval on June 26, 1997.

802.11 Physical Layer

All 802 standards address themselves to both the *Physical* (PHY) and MAC layers. At the PHY layer, IEEE 802.11 identifies three options for wireless LANs: diffused infrared, *direct sequence spread spectrum* (DSSS), and *frequency hopping spread spectrum* (FHSS).

Although the infrared PHY operates at a baseband level, the other two radios operate at 2.4 GHz, part of the *Industrial, Scientific, and Medical* (ISM) band. The ISM band can be used for operating wireless LAN devices and does not require an end-user license. All three PHYs specify support for 1-Mbps and 2-Mbps data rates.

802.11 MAC Layer

The 802.11 MAC layer, like CSMA/CD and token passing, presents the rules used to access the wireless medium. The primary services provided by the MAC layer are as follows:

- **Data transfer** Based on a *Carrier Sense Multiple Access with Collision Avoidance* (CSMA/CA) algorithm as the media access scheme.
- **Association** The establishment of wireless links between wireless clients and *access points* (APs).
- **Authentication** The process of conclusively verifying a client's identity prior to a wireless client associating with an AP. 802.11 devices operate under an open system where any wireless client can associate with any AP without verifying credentials. True authentication is possible with the use of the *Wired Equivalent Privacy Protocol* (WEP), which uses a shared key validation protocol similar to that used in *Public Key Infrastructures* (PKI). Only those devices with a valid shared key can be associated with an AP.
- **Privacy** By default, data is transferred "in the clear." Any 802.11-compliant device can potentially eavesdrop on PHY 802.11 traffic that is within range. WEP encrypts the data before it is transmitted using a 40-bit encryption algorithm known as RC4. The same shared key used in authentication is used to encrypt or decrypt the data; only clients with the correct shared key can decipher the data.
- **Power management** 802.11 defines an *active mode*, where a wireless client is powered at a level adequate to transmit and receive, and a *power save mode*, under which a client cannot transmit or receive, but consumes less power while in a standby mode of sorts.

802.11 has garnered a great deal of attention in recent months, particularly with the perceived competition from Bluetooth, another short-distance wireless protocol. Significantly more activity is underway in the 802.11 space, however, with daily product announcements throughout the industry. Various subcommittees have been created that address everything from security to voice transport to quality of service; it is a technology to watch.

HomePNA

HomePNA is a not-for-profit association founded in 1998 by 11 companies to bring about the creation of uniform standards for the deployment of interoperable in-home networking solutions. The companies, 3Com, AMD, AT&T Wireless, Compaq, Conexant, Epigram, Hewlett-Packard, IBM, Intel, Lucent Technologies, and Tut Systems, are committed to the design of in-home communications systems that will enable the transport of LAN protocols across standard telephone "inside wire."

HomePNA operates at 1 Mbps and enables the user to employ every RJ-11 jack in the house as both telephone and data ports for the interconnection of PCs, peripherals, and telephones. The standard enables interoperability with existing access technologies such as xDSL and ISDN, and therefore provides a good migration strategy for *Small Office/Home Office* (SOHO) and telecommuter applications. The initial deployment utilizes Tut Systems' HomeRun product, which enables telephones and computers to share the same wiring and to simultaneously transmit. Extensive tests have been performed by the HomePNA, and although some minor noise problems caused by AC power and telephony-coupled impedance have resulted, they have been able to eliminate the effect through the use of low-pass filters between the devices causing the noise and the jack into which they are plugged.

Content

It would be irresponsible of me to write a book like this without at least mentioning the content that rides on today's networks. The section that follows explores multimedia and all its many flavors. Multimedia is the primary driving force for bandwidth today. An understanding of what it is and where it is going is important. Besides, it's fascinating stuff.

The World of Multimedia

In the last decade a revolution has taken place in visual applications. Starting with simple, still image-based applications such as grayscale facsimile, the technology has diverged into a collection of visually oriented applications that include video and virtual reality. Driven by

aggressive demands from sophisticated, applications-hungry users and fueled by network and computer technologies capable of delivering such bandwidth- and processor-intensive services, the telecommunications industry has undergone a remarkable metamorphosis as industry players battle for the pole position.

Why this rapid growth? Curt Carlson, Vice-President of Information Systems at the David Sarnoff Research Institute in Princeton, New Jersey, observes that more than half of the human brain is devoted to vision-related functions, an indication that vision is our single most important sense. He believes that this rapid evolution in image-based systems is occurring because those are the systems that people actually need.

"First, we invented radio," he observes, "then we invented television. Now we are entering what we call the age of interactivity, in which we will take and merge all of those technologies and add the element of user interaction. Vision is one of the key elements that allow us to create these exciting new applications." Indeed, many new applications depend on the interactive component of image-based technologies. Medical imaging, interactive customer service applications, and multimedia education are but a few.

Still Images

Still-image applications have been in widespread use for quite some time. Initially, photocopy machines were used. They did not provide document storage, nor did they offer the capability to electronically transport them from one place to another. That capability arrived on a limited basis with the fax machine.

Although a fax transmission enables a document to be moved from one location to another, what actually moves is not document content, but rather an *image* of the document's content. This is important, because no element of flexibility inherent in this system enables the receiver to make immediate and easy changes to the document. The image must be converted into machine-readable data, a capability that is just now becoming possible with *Optical Character Recognition* (OCR) software.

As imaging technology advanced and networks grew more capable, other technological variations emerged. The marriage of the copy machine and the modem yielded the scanner, which enables high-quality images to be incorporated into documents or stored on a machine-accessible medium such as a hard drive.

Other advances followed. The emergence of *high-quality television* (HQTV) coupled with high-bandwidth, high-quality networks led to the development and professional acceptance of medical imaging applications, with which diagnosis-quality X-Ray images can be used for remote teleradiology applications. This made possible the delivery of highly specialized diagnostic capabilities to rural areas, a significant advancement and extension of medicine.

Equally important are imaging applications that have emerged for the banking, insurance, design, and publishing industries. Images convey enormous amounts of information. By digitizing them, storing them online, and making them available simultaneously to large numbers of users, the applications for which the original image was intended are enhanced. Distance ceases to be an issue, transcription errors are eliminated, and the availability of expertise becomes a non-problem.

Imaging applications also have downsides, of course. Image-based applications require expensive end-user equipment. Image files tend to be large, so storage requirements are significant. Furthermore, because of the bandwidth-intensive nature of transmitted image files, network infrastructures must be re-examined.

The Arrival of Compression

To deal with the storage and transmission issues associated with image-based applications, corollary technologies such as digital compression have emerged. The main technique used today for still image compression is JPEG, developed by the Joint Photographic Experts Group, a cooperative effort between the *International Organization for Standardization* (ISO), the *International Telecommunication Union Standardization Sector* (ITU-T), and the *International Electrotechnical Commission* (IEC).

JPEG, discussed briefly in an earlier chapter, works as follows. Digital images, composed of thousands of picture elements (pixels), are "dissolved" into a mosaic of 16-pixel $\times$ 16-pixel blocks. These blocks are then reduced to 8 $\times$ 8 blocks by removing every other pixel value. JPEG software then calculates an average brightness and color value for each block, which is stored and used to reconstruct the original image during decompression.

Today still-image technologies remain in widespread use and will continue to play a key role in the application of visual technologies. But others have emerged as well. One of the most promising is video.

Video

The video story begins in 1951 at RCA's David Sarnoff Research Institute. During a celebration dinner, Brigadier General David Sarnoff (see Figure 4-26), Chairman of RCA and the founder of NBC, requested that the institute work on three new inventions, one of them called a *videograph*. In his mind, a videograph was a device capable of capturing television signals on some form of inexpensive medium, such as tape.

Remember the time frame that we're talking about. Thanks to Philo T. Farnsworth who invented the predecessor of today's *cathode ray tube* (CRT, and yes, that's his real name), electronic television became a reality in the 1920s. By the early 1950s, black and white television was widespread in America. The gap between the arrival of television and the demand for video therefore was fairly narrow.

Work on the Videograph began almost immediately and a powerful cast of characters was assembled. One unlikely member of this cast served as a catalyst: Bing Crosby. Keenly interested in broadcast technologies, Crosby wanted to be able to record his weekly shows for later transmission. The Bing Crosby Laboratories played a key role in the development and testing of video technology.

The Sarnoff Institute called upon the capabilities of several companies to reach its goal of creating what Sarnoff dubbed the *Hear-See machine*. One of them was Ampex, developer of the first commercial audio tape recorder. The Sarnoff team believed that audiotape technology could be applied to video recording.

To a certain extent, they were correct. Marvin Camras, a Sarnoff team member and scientist who developed the capability to record audio signals on steel wire used during WWII, soon discovered that the video signal was dramatically broader than the relatively narrow spectrum of the audio signal. Early audio tape machines typically moved the tape

Figure 4-26
Brig. General David Sarnoff.

along at a stately 15 *inches per second* (IPS). To meet the bandwidth requirements of the video signal, the tape had to be accelerated to somewhere between 300 and 400 inches per second, roughly 25 miles per hour.

To put this into perspective, a tape that would accommodate an hour's worth of audio in those days would hold *one minute* of video, which did not take into account the length of the leader that had to be in place to enable the recorder to reach its ridiculously high tape transport speed. To hold 15 minutes of video, a reel of quarter-inch tape would have had to be three feet in diameter, not exactly portable. Put another way, a one-hour show would require 25 miles of tape!

To get around this problem, Camras invented the spinning record head. Instead of moving the tape rapidly past the recording head, he moved the tape slowly and rapidly spun the head. By attaching the head to a 20,000-rpm Hoover vacuum cleaner motor (stolen, by the way, from his wife's vacuum cleaner), he was able to use two-inch tape and reduce the tape transport speed to 30 to 40 inches per second, a dramatic improvement.

The first video demonstrations were admirable, but rather funny. First of all, the resolution of the television was only 40 lines per inch compared to more than 250 on modern systems. The images were so poor that audiences required a narrator to tell them what they were seeing on the screen.

Luckily, other advances followed. The original video systems rendered black-and-white images, but soon a color system was developed. It recorded five tracks (red, blue, green, synch, and audio) on half-inch tape and ran at the original speed of 360 ips. The system was a bit unwieldy. It required a *mile* of color tape to capture a four-minute recording.

Obviously, mile-long tapes were unacceptable, especially if they would only yield four-minute programs. As a result, the Sarnoff/Ampex team reexamined the design of the recording mechanism. Three scientists, Charles Ginsburg, Alex Maxey, and Ray Dolby (later to be known for his work in audio), redesigned the rotating record head, rotating it about 90 degrees so that the video signal was now written on the tape in a zigzag design. This redesign, combined with FM instead of AM signal modulation, enabled the team to reduce the tape speed to a remarkable 17½ inches per second. For comparison's sake, modern machines consume tape at about 2½ inches per second. This, by the way, is why the record head in your home VCR sits at a funny angle (it's that big silver cylinder you see when you open the slot where the tape is inserted, as shown in Figure 4-27).

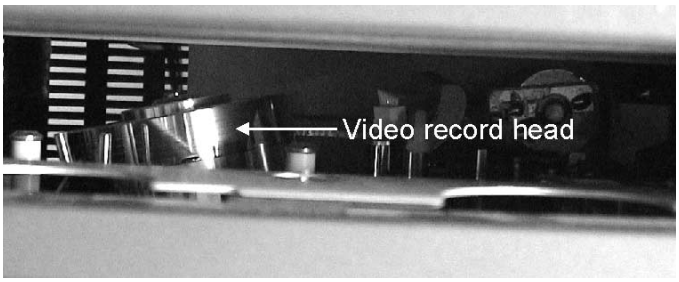


Figure 4-27 Video record head in modern VCR. Note angle of head.

By 1956, Sarnoff and Ampex had created a commercially viable product. They demonstrated the Mark IV to 200 CBS affiliate managers in April of that year. When David Sarnoff walked out on the stage and stood next to his own prerecorded image playing on the television next to him, the room went berserk. In four days, Ampex took $5M in video machine orders.

Modern Video Technology

Today's palm-size videotape recorders are a far cry from the washer-dryer-size Mark IV of 1956. But physical dimensions are only a piece of the video story.

The first video systems were analog and relied on a technique called *composite video*. In composite video, all of the signal components, such as color, brightness, audio, and so on, are combined into a single multiplexed signal. Because of the interleaved nature of this technique, a composite signal is not particularly good and suffers from such impairments as clarity loss between generations (in much the same way an analog audio signal suffers over distance) and color bleeding. Unfortunately, bandwidth at the time was extremely expensive and the cost to transport five distinct high-bandwidth channels was inordinately high. Composite video therefore was a reasonable alternative.

As the cost of bandwidth dropped in concert with advances in transmission technology, *component video* emerged, in which the signal components were transported separately, each in its own channel. This eliminated many of the impairments that plagued composite systems.

Several distinct component formats have emerged, including RGB (for red-green-blue), YUV (for Luminance [Y], Hue [U], and Saturation [V]), YIQ, and a number of others. An interesting aside: luminance is analogous to brightness of the video signal, whereas hue and saturation make up the chrominance (color) component.

All these techniques accomplish the task of representing the RGB components needed to create a color video signal. In fact, they are mathematical permutations of one another.

One final observation is that RGB, YUV, and the others previously mentioned are *signal formats*, a very different beast from *tape formats*, such as D1, D2, Betacam, VHS, and S-VHS. Signal formats describe the manner in which the information that represents the captured image is created and transported, while tape formats define how the information is encoded on the storage medium.

Of course, these signal formats are analog and therefore still suffer from analog impairments such as quality loss, as downstream generations are created. Something better is needed.

Digital Video

In the same way that digital data transmission was viewed as a way to eliminate analog signal impairments, digital video formats were created to do the same for video. Professional formats such as D1, D2, and Digital Betacam (the latter often discounted because it incorporates a form of compression), and even High-8 and MiniDV, virtually eliminate the problem of generational loss.

One downside is that even though these formats are digital, they still record their images sequentially on videotape. Today video and computer technologies are being married as nonlinear video systems for editing and management ease. Because the video signal can be digitized ("bits is bits"), it can be stored on a large hard drive just as easily as a text or image file can be. Of course, these files tend to be large and therefore require significant amounts of hard drive space. For example, a full-motion, full-color, TV-screen-size, two-hour movie requires 26 MB per second of storage capacity, a total of nearly 24 GB of storage.

Today the market demands an inexpensive, high-quality solution to the storage of video; CD-ROM is a popular target for such files. Although this is an appealing concept, let's explore what it takes to put video on a CD-ROM.

The Video Process

The signal that emerges from a video camera, although it can be either analog or digital, is typically analog. The signal is laid down on either

analog (Betacam, VHS, S-VHS) or digital tape (D1, D2, Digital Betacam). Digital tape is a quite expensive medium, but it eliminates generational loss and is therefore popular in commercial video.

To create a digital representation of analog video, the analog signal is typically sampled at three to four times the bandwidth of the video channel (unlike audio, which typically relies on a 2x sample). As a result, the output bandwidth for digital tape machines is quite high: 411 Mbps for D1, 74 Mbps for D2.

A single CD-ROM drive will hold approximately 650 MB of data. The best numbers available today, including optimal sampling and compression rates (discussed a bit later), indicate that VHS-quality recording requires roughly 5 MB of storage per second of a recorded movie. That's 7,200 seconds for a two-hour movie, or roughly 30 CD-ROM discs. Finally, the maximum transfer rate across a typical bus in a PC is 420 KB per second, somewhat less than that required for a full-motion movie.

What the Market Wants, the Market Gets: Compression

Growth in desktop video applications for videoconferencing, on-demand training, and gaming is fueling the growth in digital video technology, but the problems mentioned previously still loom large. Recent advances have had an impact; for example, storage and transport limitations can often be overcome with compression.

The most widely used compression standard for video is MPEG, created by the Moving Pictures Expert Group, the joint ISO/IEC/ITU-T organization that oversees standards developments for video. MPEG is relatively straightforward. In its initial compression step, MPEG creates what is called a *reference frame*, an actual copy of the original frame of video. It intersperses these so-called I-frames every 15 frames in the transmission. Because they are used as a reference point, they are only minimally compressed.

MPEG assumes (correctly) that a relatively small amount of the information in a series of video frames changes from frame to frame. The background, for example, stays relatively constant in most movies for long periods of time. Therefore, only a small amount of the information in each frame needs to be recaptured, recompressed, and restored.

Two additional frame types are created in the MPEG process. Predicted frames use information contained in past frames to "predict" the content of the next frame in the series, thus reducing the amount of

information required. These predicted frames experience medium to significant compression.

MPEG can also create bi-directional interpolated frames that are interspersed between the original I-frames and the predicted frames. They require input from both and, because they constitute the bulk of the transmitted frame stream, are subject to the most compression. In fact, compression ratios of 200:1 are not uncommon in MPEG. An 18-GB movie can be reduced to a somewhat more manageable 90 MB.

Several different versions of MPEG compression are available. MPEG I was created to solve the transmission and storage challenges associated with relatively low-bandwidth situations, such as PC-to-CD-ROM or low-bit-rate data circuits. MPEG II, on the other hand, is designed to address much more sophisticated transmission schemes in the 6 to 40 Mb-per-second range. This positions it to handle such applications as broadcast television and HDTV, as well as variable bit rate video delivered over packet, Ethernet, and Token Ring networks. MPEG II has the attention of both the telephone and the cable television industries as the near-term facilitator of video-on-demand services.

MPEG III, also known as MP3, has become both famous and infamous of late and has made the terms Napster and Metallica household names. MPEG layer 3 is a type of audio *compressor*/*decompressor* (CODEC) that delivers significant compression of as much as 12:1 of an audio signal with very little degradation of sound quality. Higher compression levels can be achieved, but sound quality suffers.

The standard bit rates used in MP3 CODECs are 128 and 112 Kbps. One advantage of MP3 is that a sound file can be broken into pieces and each piece remains independently playable. The feature that makes this possible means that MP3 files can be streamed across the net in real-time, although network latency can limit the quality of the received signal.

The only real disadvantage of MP3 compression is that significant processor power is required to encode and play files. Dedicated MP3 players have recently emerged on the market and are proving to be quite popular. I have an MP3 player with 6 GB of storage that I have encoded and loaded more than 170 CDs at CD quality into and still have over a gigabyte of space left.

MPEG IV is a specially designed standard for lower bit rate transmissions such as dial-up video.

Other compression schemes are available for video. Motion JPEG, for example, is an intra-frame compression technique (unlike MPEG, which is inter-frame) that compresses and stores each and every image

as a separate entity. This is different from MPEG. Compression ratios with Motion JPEG are considerably lower than MPEG's 200:1 numbers. Ratios of 20:1 are about the limit, assuming equivalent image quality.

Other techniques exist, but they are largely proprietary. These include PLV, Indeo, RTV, Compact Video, AVC, and a few others.

Television Standards

It's interesting to note that in the drive toward digitization the ultimate goal is to create a video storage and transport technology that will yield as good a representation of the original image as analog transmission does.

Two primary governing organizations dictate television standards. One is the *National Television System Committee* (NTSC), sometimes said to stand for "never twice the same color," based on the sloppy color management that characterizes the standard). The other organization, used primarily in Europe, is the *Phased Alternate Line* (PAL) system. NTSC is built around a 525-line-per-frame, 30-frame-per-second standard, while PAL uses 625 lines-per-frame and 25 frames-per-second. Although technically different, both address the same concerns and rely on the same characteristics to guarantee image quality.

Video Quality Factors

Four factors influence the richness of the video signal. They are the frame rate, color resolution, image quality, and spatial resolution.

Frame rate is a measure of the refresh rate of the actual image painted on the screen. The NTSC video standard is 30 frames per second, meaning that the image is updated 30 times every second. Each frame consists of odd and even fields. The odd field contains the odd-numbered screen lines, while the even field contains the even-numbered screen lines that make up the picture.

Television sets paint the screen by first painting the odd field and then the even. They repeat this process at the rate of 60 fields, or 30 frames, per second. The number 60 is chosen to coincide with the frequency of electricity in the U.S. By the same token, PAL relies on a scan rate that is very close to 50 Hz, the standard in Europe. This odd-even alternation of fields is called *interlaced video.*

Many monitors, on the other hand, use a technique called *progressive scan,* in which the entire screen is painted 30 times per second from top to bottom. This is referred to as *non-interlaced video.* Non-interlaced systems tend to demonstrate less flicker than their interlaced counterparts.

Computers often rely on *Variable Graphics Array* (VGA) monitors, which are much sharper and clearer than television screens. This is due to the density of the phosphor dots on the inside of the screen face that yield color when struck by the deflected electron beams, as well as a number of other factors. The scan rate of VGA is much higher than that of traditional television and can therefore be non-interlaced to reduce screen flicker.

Another quality factor is *color resolution*. Most systems resolve color images using the RGB technique. Although video does rely on RGB, it also uses a variety of other resolution techniques, including YUV and YIQ. YUV is a color scheme used in both PAL and NTSC. Y represents the luminance component, while U and V, hue and saturation, respectively, make up the color component. Varying the hue and saturation components changes the color.

Image quality plays a critical role in the final outcome, and the actual resolution varies by application. For example, the user of a slow-scan desktop videoconferencing application might be perfectly happy with a half-screen, 15-frame-per-second, 8-bit image, whereas a physician using a medical application might require a full-frame, 768×484 (the NTSC standard screen size) pixel image, with 24-bit color for perfect accuracy. Both the frame rate (frames per second) and color density (bits per pixel) play a key role.

Finally, *spatial resolution* comes into the equation. Many PCs have displays that measure 640×480 pixels. This is considerably smaller than the NTSC standard of 768×484, or even the slightly different European PAL system. In modern systems, the user has great control over the resolution of the image, because he or she can vary the number of pixels on the screen. The pixels on the screen are simply memory representations of the information displayed. By selecting more pixels, and therefore better resolution, the graininess of the screen image is reduced. Some VGA adapters, for example, have resolutions as dense as 1024×768 pixels, or higher.

The converse, of course, is also true. By selecting less pixels, and therefore increasing the graininess of the image, special effects can be created, such as pixelization or tiling.

Video Summary

Let's review the factors and choices involved in creating video.

The actual image is captured by a camera that is either analog or digital. The resulting signal is then encoded on either analog or digital tape. If a VHS tape is to be the end result, it will be created directly from the original tape.

If desktop video or CD-ROM video is the end result, then additional factors come into play. Because of the massive size of the original file, it must be modified in some way to make it transportable to the new medium. It might be compressed, in which case a 200:1 reduction in size (or greater) could occur, with a resulting loss of quality (rain, for example, because it is a random event, tends to disappear in MPEG-compressed movies). The file also might be sampled less frequently, thus lowering the total number of frames, but causing the animation-like jerkiness that results from lower sampling rates. The screen size could also be reduced, thus reducing the total number of pixels that need to be encoded.

During the last decade, video has achieved a role of some significance in a wide variety of industries, finding a home in medicine, travel, engineering, and education. It provides a medium not only for the presentation of information, but, combined with telecommunications technology, it makes possible such applications as distance learning, video teleconferencing, and desktop video. The capability to digitize video signals has brought about a fundamental change in the way video is created, edited, transported, and stored.

Its emergence has also changed the players in the game. Once the exclusive domain of filmmakers and television studios, video is now fought over by creative companies and individuals who want to control its content, cable and telephone companies who want to control its delivery, and a powerful market that wants it to be ubiquitous, richly featured, and cheap. Regulators are in the mix as well, trying to make sense of a telecommunications industry that, once designed to transport voice, now carries a broad mix of fundamentally indistinguishable data types.

Virtual Reality

Asking for a definition of virtual reality is reminiscent of the parable of the five blind men and the elephant. In the story, each of the blind men

is asked to approach and examine an elephant, and then describe the creature. One approached and felt the elephant's leg; another, its trunk; the others, its ear, tail, and broad side. Their descriptions of the elephant were all quite different.

Today virtual reality has the interest of a fair number of companies and industries. Over the last few years, video has brought significant change to the business and academic community; today VR provides a new focus.

Virtual reality is different things to different people. To some, virtual reality is a computer application that provides a doorway into imaginary worlds. To others, it is the remarkable collection of hardware and software that provides the portal mentioned previously. Others escape reality through books, movies, and fantasy games, such as Dungeons and Dragons™; to them, that's another virtual reality. Whatever the case, virtual reality is a marriage of technology and human imagination that is insinuating itself into some remarkable, and perhaps surprising, applications.

So, what is virtual reality? One text on the subject defines it as "a way for humans to visualize, manipulate, and interact with computers and extremely complex data." This definition actually describes virtual reality fairly well. Virtual reality relies on computer-generated visual and auditory sensory information about a world that only exists within the computer. This world could be a CAD drawing of a cathedral, a model showing chemicals interacting, or air flowing across the wings of an aircraft. Obviously, the data required to drive the virtual reality engine is massively complex and requires sophisticated computing capabilities.

To some, virtual reality is something of an oxymoron (Mark Weiser of Xerox PARC, a pioneer in VR, called it "real virtuality"). Indeed, early systems were not particularly convincing. The bandwidth and computer power required for the computer software to keep up with the user's complex movements were not up to the task, and typically a lot of latency occurred.

Today things are quite different. Not only are the graphics significantly cleaner, the computers' orders of magnitude faster, and the equipment sleek and comfortable, but some systems have now added a third, tactile element. Special gloves and suits are available that actually give the user tactile feedback in addition to sound and vision. Virtual surgery applications, for example, provide sensation to the surgeon, giving the actual *feel* of the real procedure. VR body suits, using servos and microbladders that rapidly fill and deflate with air, can be tied into applications to yield a wide variety of (interesting) tactile sensations ranging from the punch of a boxer to, well, use your imagination.

VR Techniques

Today six distinct "flavors" of virtual reality exist. The first flavor, often called *Window on the World* (WoW), first emerged in early 1965 and is certainly the least complex. In WoW, a standard computer screen displays two-dimensional application graphics and serves as a window into the virtual environment that the application creates. Sound is provided by adjacent speakers.

The second technique is called *video mapping* and is a variation of WoW. In a video-mapping system, the application overlays a video image of the user's silhouette on the graphics, and the user watches his or her own image as it winds its way through the virtual world. As with WoW systems, it is still a two-dimensional application, but is improved by the addition of the user.

Video mapping emerged in the late 1960s. Several early commercial virtual reality applications used video mapping, including Mandala, which relied on a modified Commodore Amiga, and the TV station Nickelodeon, which used a video-mapping application on its Nick Arcade to overlay competitors on a giant video arcade game.

A third technique, and perhaps the most widely used, is called *immersive VR*. Immersive systems typically use some kind of *head-mounted display* (HMD) to provide three-dimensional video and stereophonic sound, thus immersing the user in the world created by the application. The helmet also houses motion-detection devices, which tell the application where the user is, what direction they are looking, and what they should be seeing and hearing. The helmet is usually tethered by a cable back to the computer, although some new systems rely on wireless connectivity.

A variation of HMD-reliant systems is the so-called "Cave," like the one conceived and created at the University of Illinois at Chicago's Electronic Visualization Laboratory. "Virtual reality is the descendent of a long line of computer graphics research that tries to incorporate more modalities of perception and interaction into our interface with computers," says Dan Sandin, Co-Director of the Lab. "Many people believe that VR systems have to use helmets and data gloves, which are actually somewhat restrictive. We created the Cave as a solution to the problem of reduced fields of vision that plague many of the HMD-type VR systems.

"The Cave is a projection-based virtual reality system, in which three-dimensional images are projected on all six sides (four walls, the ceiling and the floor). The user wears a pair of lightweight polarized glasses that

also house a very small, wireless motion and location sensor (they look like the nerdy black horn rims of the '60s). When the Cave is activated, the user suddenly finds himself or herself immersed in a seemingly endless school of sharks, or floating in space outside the shuttle, or dancing with an indescribable, three-dimensional polygon. It's quite a remarkable thing."

Perhaps the best-known "virtual" virtual reality application is the Holodeck used on "Star Trek: The Next Generation." Sandin smiles at the comparison to the Cave. "The thing that differentiates the Cave from the Holodeck is that you can't sit in the chairs in the cave. They look pretty good, and they're there, but don't try to sit in them."

The fourth major application of VR is called *virtual telepresence*. In these systems, the user's senses are electronically linked to remote sensors, giving the user the sensation of actually being, and feeling, where the remote sensors are. In remote surgery applications (mentioned previously), systems are designed to give physicians tactile feedback as they operate. Firefighters and bomb squad personnel use remote telepresence applications in very delicate, and potentially dangerous, procedures. NASA and the Woods Hole Oceanographic Institute (Outer Space and Inner Space) use telepresence applications for the robotic exploration of deep space and the deep ocean. In fact, a joint U.S./Russian robotic space rover program is already underway.

The fifth flavor of virtual reality is called *mixed reality*. In mixed-reality applications, real-world inputs are combined with computer-generated images to facilitate whatever task is being attempted. In medicine, for example, a surgeon's video image of the actual organ might be overlaid with a CT scan image to help best target the procedure. Video mapping, mentioned earlier, combines virtual reality imagery with CT scan images to create a three-dimensional view of the patient's internal organs. In combat aviation, images of the ground are combined with terrain and elevation information, and are then displayed on the pilot's heads-up display, or the inside of the helmet visor.

The last form of virtual reality is called *fishtank virtual reality*. It is the newest technique and is perhaps the most promising. In fishtank systems, the user wears a pair of lightweight glasses, similar to the Polaroid glasses worn in the Cave. These, however, have color *liquid crystal display* (LCD) lenses that provide wide-field stereoscopic vision and include a mechanical head tracker unit.

Virtual Reality Equipment

Six principal hardware components make up a virtual reality system. These include the computer that generates the images, manipulation devices, position trackers, vision systems, sound drivers, and the HMD.

Computer complexity ranges from inexpensive PC systems to Silicon graphics machines costing well over $100,000. Obviously, the more complex the graphics being generated, the more capable and powerful the image generator needs to be.

Manipulation and control devices provide the means of tracking the position of a real object within a virtual world. Because the real world is three-dimensional, tracking devices must be able to respond to roll, pitch, and yaw movements.

These devices come in many different versions. The simplest are mice, trackballs, and joysticks; they provide the least control over virtual motion. A step above them is the instrumented glove, in which the fingers are equipped with sensors that notify the computer of movement and hand action. These range in complexity from gloves that use fiber optic sensors for finger motion and magnetic trackers that detect general position, to less complex devices that provide limited sensing with strain gauges on the fingers and ultrasonic overall position detectors.

Today full-body suits and electronic exoskeletons are used to capture full-character motion for animation applications, the control of musical synthesizers, and some advanced games. One airline in-flight catalog sells a $10,000 body suit that can be connected to existing video games, such as Nintendo, 3DO, and Sega, for the person that has *virtually* everything.

Position trackers can be as simple as a mechanical arm that follows the user around the virtual environment or as complex as full-body exoskeletons like those mentioned previously. Some companies offer a body suit that not only provides position information to the application, but delivers force feedback to the wearer of the suit to simulate real interaction with objects in the virtual world (an area of research known as *haptics*). Logitech is a well-known manufacturer of these devices.

The actual tracking units rely on a variety of technologies. *Ultrasonic sensors* pulse at a known repetitive frequency, and the latency between pulse and pickup is used to track locations like sonar. *Magnetic sensors* use coils that produce magnetic fields that can be tracked by the pickup

unit. The best known manufacturer of magnetic units is Polhemus in Colchester, Vermont.

A third tracking system relies on *optical pickups* to determine location. Using a grid of ceiling-mounted *light-emitting diodes* (LEDs) that flash in a known pattern, helmet-mounted video cameras can track the wearer's location under the grid. Origin Instruments is the primary manufacturer of these systems.

Finally, a limited number of *inertial trackers* can be used in virtual reality systems. They typically only detect rotational movement, but in some systems, this is adequate.

We've already discussed many of the *vision systems* used in virtual reality. These include rear-projection systems, such as those in the UIC Cave, dual screens placed before the eyes to yield stereoscopic vision, and a split-screen technique, in which the user wears a hood, and images are painted on the screen in two parts, thus simulating stereoscopic vision.

True immersive systems require some sort of *head-mounted display*. These can be as complex as a helmet containing stereophonic sound speakers, stereoscopic vision screens, and complex motion detection devices, to the pair of nerdy black polarized glasses with a small motion sensor connected via a fine optical cable. These devices are currently expensive ($3K to $10K) but are expected to plummet in the next few years as entertainment companies announce virtual reality-based video games. Both Nintendo and SEGA have plans underway to create and release an entire line of virtual reality-dependent games within the next year.

An Image of the Future: Back to *Real* Reality

So, where is all this image-based technology going? In *Snow Crash,* author Neal Stephenson describes what is perhaps the ultimate marriage of virtual reality and the Information Superhighway. In his world, users log on to the network through a low-power wireless terminal that sports a lightweight head-mounted display about the size of a pair of glasses. Instead of using a *video display terminal* (VDT) or LCD displays, the HMD uses low-power, multicolored lasers to paint three-dimensional images on the retinas of both eyes. The lasers have tracking circuitry that enables them to follow the minute movements of the user's eyes, thus guaranteeing a perfect set of images from any position.

Once logged on (or "jacked in," to use the appropriate terminology), the user finds him- or herself in a virtual world. The world, known as a metaverse, consists of a main street with shops, bars, and businesses—the databases of the more routine Web—that the user can stop in and visit. Furthermore, rather than talking to other users via the crude medium of typed text, users actually "see" other users in the virtual world. These manifestations of the real users are called *avatars*, a word that means "the physical manifestation of a god."

Obviously, we're quite a ways from this level of capability, but not all *that* far. Still-image applications are firmly entrenched and offer a broad variety of capabilities that have in many ways revolutionized banking, medicine, insurance, and architecture, to name a few. Video, too, has revolutionized many fields, but in certain tantalizing ways, technology has revolutionized video. Modern non-linear systems digitally encode the video images captured on tape, store them on disk, and enable editors to manipulate the footage very easily. Home-based systems are now freely available and are well within the price range of the average hobbyist.

Furthermore, because the images are digitized, they can be artistically altered to create remarkable special effects. Remember the doctored video in *Rising Sun?* Industrial Light and Magic and other movie studios rely on these techniques to create virtual realities for the world's theaters.

The exciting part of all this is the ultimate combination of virtual reality and digital video, high-bandwidth transport technologies, and emerging applications. Dan Sandin: "Not only will VR provide entertainment value, it will also become firmly entrenched in business. As businesses continue to realize how expensive and time-consuming it is to move people around the country for meetings, and as the VR technology gets better and better, eventually there will be this mass realization that virtual presence—called telepresence in the jargon—is good enough, and perhaps better, if you factor in travel costs and time away from work." Add the further enhancement of desktop video, and the future is here.

The delivery mechanism for all these visually oriented systems is equally complex and exciting. One area that is as yet undefined is the whole question of who the network players will be and telephone companies, cable providers, and application designers are all jockeying for position. Already alliances are emerging that will help determine the shape of the interactive, entertainment-oriented future.

And what about the non-entertainment market? Indeed, applications are out there, built around images, video, and virtual reality. Medicine

and aviation, for example, enhance safety through the use of these technologies, while chemistry and architecture use them to enhance the understanding of highly complex structures and interactions. In education, the virtual classroom delivers teachers and schoolrooms to far-flung locations.

Today the cost of these technologies is somewhat prohibitive because they are new and are provided by a relatively small number of pioneer manufacturers. As applications and the market drive them toward commodity, the cost will come down, and digital video and virtual reality will become mainstream technologies.

Ellen Beth Van Buskirk, former Director of Corporate Communications for the SEGA Channel, agrees. "Video games have long been the bastion of teenage boys," she says. These new technologies will offer entire families the opportunity to interact together in virtual worlds. It's going to be a very exciting future.

Summary

Premises technologies, including LANs, wireless solutions, and the content that rides on both of them, are the most visible components of the overall network to a customer. In the next chapter, we dive into the network itself and explore the access technologies that provide the bridge between premises technologies and the transport network.

CHAPTER 5

Access Technologies

For the longest time, "access" described the manner in which customers reached the network for the transport of voice services. In the last 20 years, however, that definition has changed dramatically. In 1981 (*20 years ago*), IBM changed the world when it introduced the PC, and in 1984 the Macintosh arrived, bringing well-designed and organized computing power to the masses. Shortly thereafter, hobbyists began to take advantage of emergent modem technology and created online databases, the first bulletin board systems that enabled people to send simple text messages to each other. This accelerated the modem market dramatically, and before long, data became a common component of local loop traffic. At that time, there was no concept of Instant Messenger or of the degree to which e-mail would fundamentally change the way people communicate and do business. At the same time, the business world found more and more applications for data, and the need to move that data from place to place became a major contributor to the growth in data traffic on the world's telephone networks.

In those heady, early days, data did not represent a problem for the bandwidth-limited local loop. The digital information created by a computer and intended for transmission through the telephone network was received by a modem, converted into a modulated analog waveform that fell within the 4-KHz voice band, and fed to the network without incident. As we mentioned in a previous chapter, the modem's job was (and is) quite simple. Invoke the Wizard of Oz protocol: when a computer is doing the talking, the modem must make the network think it is talking to a telephone. "Pay no attention to that man behind the curtain!"

Over time, modem technology advanced, enabling the local loop to provide higher and higher bandwidth. This increasing bandwidth was made possible through clever signaling schemes that enabled a single signaling event to transport more than a single bit. These modern modems, often called Shannon-busting modems because they defy the limits of signaling defined by Shannon, are commonplace today. They enable baud levels to reach unheard-of extremes and permit the creation of very high bit-per-signal rates.

The analog local loop is used today for various voice and data applications in both business and residence markets. The new lease on life that it enjoys, thanks to advanced modem technology as well as a focus by installation personnel on the need to build clean, reliable outside plant, has resulted in the development of faster access technologies designed to operate across the analog local loop. This includes traditional high-speed modem access and such options as the *Digital Subscriber Line* (DSL).

Marketplace Realities

According to a number of demographic studies conducted in the last 18 months, approximately 70 million households today host home office workers, and the number is growing rapidly. These include both telecommuters and those who are self-employed and work out of their homes. They require the ability to connect to remote *local area networks* (LANs) and corporate databases, retrieve e-mail, access the Web, and in some cases conduct videoconferences with colleagues and customers. The traditional bandwidth-limited local loop is not capable of satisfying these requirements with traditional modem technology. The dedicated private line service, which would solve the problem, is far too expensive as an option, and because it is dedicated, it is not particularly efficient.

Other solutions are required, and these have emerged in the form of access technologies that take advantage of either a conversion to end-to-end digital connectivity (*Integrated Services Digital Network* [ISDN]) or expanded capabilities of the traditional analog local loop (DSL or 56K modems). In some cases, a whole new architectural approach is causing excitement in the industry (*Wireless Local Loop* [WLL]). Finally, cable access has become a popular option as the cable infrastructure has evolved to a largely optical, all-digital system with high-bandwidth, two-way capabilities. We will discuss each of these options in the pages that follow.

56-Kbps Modems

One of the most important words in telecommunications is *virtual*. It is used in a variety of ways, but in reality only has one meaning. If you see the word "virtual" associated with a technology or product, you should immediately say to yourself, "it's a lie."

A 56-Kbps modem is a good example of a virtual technology. These devices have attracted a great deal of interest since they were introduced a few years ago. Under certain circumstances, they do offer higher access speeds designed to satisfy the increasing demands of bandwidth-hungry applications and increasingly graphics-oriented Web pages. The problem they present is that they do not really provide true 56K access, even under the best of circumstances.

56K modems provide asymmetric bandwidth, with 56 Kbps delivered downstream toward the customer (sometimes) and significantly less

bandwidth (33.6 Kbps) in the upstream direction. Although this may seem odd, it makes sense given the requirements of most applications today that require modem access. A Web session, for example, requires very little bandwidth in the upstream direction to request that a page be downloaded. The page itself, however, may require significantly more, since it may be replete with text, graphics, Java applets, and even small video clips. Since the majority of modem access today is for Internet surfing, asymmetric access is adequate for most users.

The limitations of 56K modems stem from a number of factors. One of them is the fact that under current FCC regulations (specifically Part 68), line voltage supplied to a communications facility is limited such that the maximum achievable bandwidth is 53 Kbps in the downstream direction. Another limitation is that these devices require that only a single analog-to-digital conversion occur between the two end points of the circuit. This typically occurs on the downstream side of the circuit and usually at the interface point where the local loop leaves the *central office* (CO). Consequently, downstream traffic is less susceptible to the noise created during the analog-to-digital conversion process, while the upstream channel is affected by it and is therefore limited in terms of the maximum bandwidth it can provide. In effect, 56K modems, in order to achieve their maximum bandwidth, require that one end of the circuit, typically the CO end, be digital.

The good news with regard to 56K modems is that even in situations where the 56Kbps speed is not achievable, the modem will fall back to whatever maximum speed it can fulfill. Furthermore, no premises wiring changes are required, and because this device is really nothing more than a faster modem, the average customer is comfortable with migration to the new technology. This is certainly demonstrated by sales volume. As was mentioned before, most PCs today are automatically shipped with a 56K modem.

ISDN

ISDN has been the proverbial technological roller coaster since its arrival as a concept in the late 1960s. Often described as "the technology that took 15 years to become an overnight success," ISDN's level of success has been all over the map. Internationally, it has enjoyed significant uptake as a true, digital local loop technology. In the United States, however, because of competing and often incompatible hardware implementations, high

cost, and spotty availability, its deployment has been erratic at best. In market areas where providers have made it available at reasonable prices, it has been quite successful. Furthermore, it is experiencing something of a renaissance today because of DSL's failure to capture the market. ISDN is tested, well understood, available, and fully functional. It can offer 128 Kbps of bandwidth *right now,* whereas DSL's capability to do so is less certain. More on DSL later.

ISDN Technology

The typical non-ISDN local loop is analog. Voice traffic is carried from an analog telephone to the central office using a frequency-modulated carrier. Once at the CO, the signal is typically digitized for transport within the digital network cloud. On the one hand, this is good because it means that the overall transmission path has a digital component. On the other hand, the loop is still analog and, as a result, the true promise of an end-to-end digital circuit cannot be realized. The circuit is only as "good" as the weakest link in the chain, and the weakest link is clearly the analog local loop.

In ISDN implementations, local switch interfaces must be modified to support a digital local loop. Instead of using analog frequency modulation to represent voice or data traffic carried over the local loop, ISDN digitizes the traffic at the origination point, either in the voice set itself or in an adjunct device known as a *terminal adapter* (TA). The digital local loop then uses time division multiplexing to create multiple channels over which the digital information is transported and that provide for a wide variety of truly integrated services.

The Basic Rate Interface (BRI)

ISDN offers two well-known implementations. The most common (and the one intended primarily for residence and small business applications) is called the *Basic Rate Interface* (BRI). In BRI, the two-wire local loop supports a pair of 64-Kbps digital channels known as B-channels and a 16-Kbps D-channel, which is primarily used for signaling but can also be used by the customer for low-speed (up to 9.6 Kbps) packet data. The B-channels can be used for voice and data, and in some implementations can be bonded together to create a single 128-Kbps channel for videoconferencing or other higher bandwidth applications.

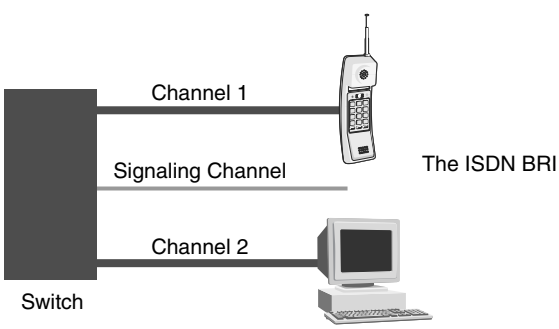
Figure 5-1 shows the layout of a typical ISDN BRI implementation, including the alphabetic reference points that identify the "regions" of the circuit and the generic devices that make up the BRI. In this diagram, the LE is the local exchange, or switch. The NT1 is the network termination device that serves as the demarcation point between the customer and the service provider. Among other things, the NT1 converts the two-wire local loop to a four-wire interface on the customer's premises. The *terminal equipment, type 1* (TE1) is an ISDN-capable device such as an ISDN telephone. This simply means that the phone is a digital device and is therefore capable of performing the voice digitization itself. A *terminal equipment, type 2* (TE2) is a non-ISDN-capable device, such as a *Plain Old Telephone Service* (POTS) telephone. In the event that a TE2 is used, a *terminal adapter* (TA) must be inserted between the TE2 and the NT1 to perform analog-to-digital conversions and rate adaptations.

The reference points mentioned earlier identify circuit components between the functional devices just described. The U reference point is the local loop, the S/T reference point sits between the NT1 and the TEs, and the R reference point is found between the TA and the TE2.

BRI Applications

Although BRI does not offer the stunning bandwidth that other more recent technologies (such as DSL) do, its bondable 64-Kbps channels provide reasonable capacity for many applications. The two most common today are remote LAN and Internet access. For the typical remote worker, the bandwidth available through BRI is more than adequate, and new video compression technology even puts reasonable quality

Figure 5-1
The ISDN BRI.



videoconferencing within the grasp of the end user at an affordable price. 64 Kbps makes short shrift of LAN-based text file downloads and reduces the time required for graphics-intensive Web page downloads to reasonable levels.

The Primary Rate Interface (PRI)

The other major implementation of ISDN is called the *Primary Rate Interface* (PRI). The PRI is really nothing more than a T-Carrier in that it is a four-wire local loop, uses AMI and B8ZS for ones-density control and signaling, and provides 24- to 64-Kbps channels that can be distributed among a collection of users as the customer sees fit (see Figure 5-2).

In PRI, the signaling channel operates at 64 Kbps (unlike the 16-Kbps D-channel in the BRI) and is not accessible by the user. It is used solely for signaling purposes; that is, it cannot carry user data. The primary reason for this is service protection. In the PRI, the D-channel is used to control the 23 B-channels and therefore requires significantly more bandwidth than the BRI D-channel. Furthermore, the PRI standards enable multiple PRIs to share a single D-channel, which makes the D-channel's operational consistency all the more critical.

The functional devices and reference points are not appreciably different from those of the BRI. The local loop is still identified as the U reference point. In addition to an NT1, we now add an NT2, which is a service distribution device, usually a *Private Branch Exchange* (PBX), which allocates the PRI's 24 channels to customers. This makes sense because PRIs are typically installed at businesses that employ PBXs for voice distribution. The S/T reference point is now divided; the S reference point sits between the NT2 and TEs, whereas the T reference point is found between the NT1 and the NT2.

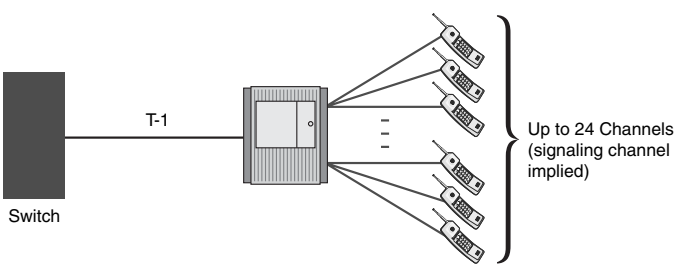


Figure 5-2
The ISDN PRI.

PRI service also has the capability to provision B-channels as super-rate channels to satisfy the bandwidth requirements of higher bit rate services. These are called H-Channels and are provisioned as shown in the following minitable.

Channel	Bandwidth
H0	384 Kbps (6B)
H10	1.472 Mbps (23B)
H11	1.536 Mbps (24B)
H12	1.920 Mbps (30B)

PBX Applications

The PRI's marketplace is the business community, and its primary advantage is pair gain, that is, to conserve copper pairs by multiplexing the traffic from multiple user channels onto a shared, four-wire circuit. Inasmuch as a PRI can deliver the equivalent of 23 voice channels to a location over a single circuit, it is an ideal technology for a number of applications. These include the interconnection of a PBX to a local switch, dynamic bandwidth allocation for higher-end videoconferencing applications, and an interconnection between an *Internet Service Provider's* (ISP's) network and that of the local telephone company.

Some PBXs are ISDN-capable on the line (customer) side, meaning that they have the capability to deliver ISDN services to users that emulate the services that would be provided over a direct connection to an ISDN-provisioned local loop. On the trunk (switch) side, the PBX is connected to the local switch via one or more T1s, which in turn provide access to the telephone network. This arrangement results in significant savings, faster call setup, a more flexible administration of trunk resources, and the capability to offer a diversity of services through the granular allocation of bandwidth as required.

Videoconferencing Videoconferencing, an application that now enjoys widespread acceptance in the market thanks to service providers like Proximity Systems and affordable, effective video *compressor/decompressors* (CODECs) from companies like PolyCom and Tandberg, has moved from the boardroom to the home office and everywhere in between. Although BRI provides adequate bandwidth for casual conferencing on a reduced-size PC screen, PRI is preferable for high-quality,

television-scale sessions. Its capability to provision bandwidth on demand makes it an ideal solution. All major videoconferencing equipment manufacturers have embraced PRI as an effective connectivity solution for their products and have consequently designed their products in accordance with accepted international standards, specifically H.261 and H.320.

Automatic Call Distribution (ACD) Another significant application for PRI is call routing in the call center environment. Ultimately, call centers represent critical decision points within a corporate environment, and the degree to which they are successful at what they do translates directly into visible manifestations of customer service. If calls are routed quickly and accurately based on some well-designed internal decision-making process, customers are happy, and the call center provides an effective image of the corporation and its services before the customer.

Automatic Call Distribution (ACD) is a popular switch feature that enables a customer to create custom routing tables in the switch so that incoming calls can be handled most effectively on a call-by-call basis. The ACD feature often relies on information culled from both corporate sources and the *Signaling System 7* (SS7) network's *Service Control Point* (SCP) databases, but the ultimate goal is to provide what appears to each caller to be customized answering.

For example, some large call centers handle incoming calls from a variety of countries and therefore potentially different language groups. Using caller ID information, an ACD can filter calls as they arrive and route them to language-appropriate operators. Similarly, the ACD can change the assignment of voice channels on a demand basis. If the call center is large and receives calls from multiple time zones simultaneously, there may be a need to add incoming trunks to one region of the call center based on time-of-day call volumes, while reducing the total coverage in another. By reallocating the 64K channels of the PRI(s), bandwidth can be made available as required. Furthermore, it can be done automatically, triggered by time of day or some other pre-identified event.

ISDN is only one of the so-called twisted pair solutions that extend the capacity and lifetime of the local loop. Another is DSL, a technology family that has achieved significant attention in the last couple of years. The attention is due to both successes and failings on the part of the technology. When it works, it works extremely well. When it doesn't, it tends to fail loudly and publicly.

Digital Subscriber Line (DSL)

The access technology that has enjoyed the greatest amount of attention in recent times is DSL. It provides a good solution for remote LAN access, Internet surfing, and access for telecommuters to corporate databases.

DSL came about largely as a direct result of the Internet's success. Prior to its arrival, the average telephone call lasted approximately four minutes, a number that CO personnel used while engineering switching systems to handle expected call volumes. This number was arrived at after nearly 125 years of experience designing networks for voice customers. They knew about Erlang theory, loading objectives, and peak-calling days/weeks/seasons, and had decades of trended data to help them anticipate load problems. So in 1993, when the Internet—and with it, the World Wide Web— arrived, network performance became unpredictable as callers began to surf, often for hours on end. The average four-minute call became a thing of the past as online service providers such as AOL began to offer flat rate plans that did not penalize customers for long connect times. Then the unthinkable happened: switches in major metropolitan areas, faced with unpredictably high call volumes and hold times, began to block during normal business hours, a phenomenon that only occurred in the past during disasters or on Mother's Day.

A number of solutions were considered, including charging different rates for data calls than for voice calls, but none of these proved feasible until a technological solution was proposed. That solution was DSL.

It is commonly believed that the local loop is incapable of carrying more than the frequencies required to support the voice band. This is a misconception. ISDN, for example, requires significantly high bandwidth to support its digital traffic. When ISDN is deployed, the loop must be modified in certain ways to eliminate its designed-in-bandwidth limitations. For example, some long loops are deployed with load coils that "tune" the loop to the voice band. They make the transmission of frequencies above the voice band impossible but enable the relatively low-frequency voice band components to be carried across a long local loop. High-frequency signals tend to deteriorate faster than low-frequency signal components, so the elimination of the high frequencies extends the transmission distance and reduces transmission impairments that would result from the uneven deterioration of a rich, multi-frequency signal. These load coils therefore must be removed if digital services are to be deployed.

A local loop is only incapable of transporting high-frequency signal components if it is *designed* not to carry them. The capacity is still there; the network design, through load coil deployment, simply makes that additional bandwidth unavailable. DSL services, especially the *Asymmetric Digital Subscriber Line* (ADSL), take advantage of this "disguised" bandwidth.

DSL Technology

In spite of the name, DSL is an analog technology. The devices installed on each end of the circuit are sophisticated high-speed modems that rely on complex encoding schemes to achieve the high bit rates that DSL offers. Furthermore, several of the DSL services, specifically ADSL, g.lite, *Very high-speed Digital Subscriber Line* (VDSL), and *Rate Adaptive Digital Subscriber Line* (RADSL), are designed to operate in conjunction with voice across the same local loop. ADSL is the most commonly deployed service and offers a great deal to both business and residence subscribers.

XDSL Services

DSL comes in a variety of flavors designed to provide flexible, efficient, high-speed service across the existing telephony infrastructure. From a consumer point-of-view, DSL, especially ADSL, offers a remarkable leap forward in terms of available bandwidth for broadband access to the Web. As content has steadily moved away from being largely text-based and has become more graphical, the demand for faster delivery services has grown for some time now. DSL may provide the solution at a reasonable cost to both the service provider and the consumer.

Businesses will also benefit from DSL. Remote workers, for example, can rely on DSL for LAN and Internet access. Furthermore, DSL provides a good solution for *virtual private network* (VPN) access as well as for ISPs looking to grow the bandwidth available to their customers. It is available in a variety of both symmetric and asymmetric services and therefore offers a high-bandwidth access solution for a variety of applications. The most common DSL services are ADSL, *High-bit-rate Digital Subscriber Line* (HDSL), HDSL-2, RADSL, and VDSL. The special case of g.lite, a form of ADSL, will also be discussed.

Asymmetric Digital Subscriber Line (ADSL)

When the World Wide Web and flat rate access charges arrived, the typical consumer phone call went from roughly four minutes in duration to several times that. All the engineering that led to the overall design of the network based on an average four-minute hold time went out the window as the switches staggered under the added load. Never was the expression, "in its success lie the seeds of its own destruction," more true. When ADSL arrived, it provided the offload required to save the network.

A typical ADSL installation is shown in Figure 5-3. No change is required to the two-wire local loop, but minor equipment changes, however, are required. First, the customer must have an ADSL modem at their premises. This device enables both the telephone service and a data access device, such as a PC, to be connected to the line.

The ADSL modem is more than a simple modem, in that it also provides the frequency division multiplexing process required to separate the voice and data traffic for transport across the loop. The device that actually does this, shown in Figure 5-4, is called a splitter, in that it splits the voice traffic away from the data. It is usually bundled as part of the ADSL modem, although it can also be installed as a card in the PC, as a standalone device at the demarcation point, or on each phone at the premises.

The most common implementation is to integrate the splitter as part of the DSL modem. This, however, is the least desirable implementation because this design can lead to crosstalk between the voice and data circuitry inside the device. When voice traffic reaches the ADSL modem, it is immediately encoded in the traditional voice band and is handed off to the local switch when it arrives at the CO. The modem is often referred to as an *ADSL transmission unit for remote use* (ATU-R). Similarly, the device in the CO is often called an ATU-C .

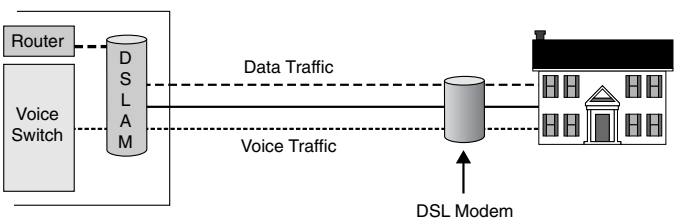


Figure 5-3 Layout of typical DSL.

Figure 5-4
DSL Splitter.

When a PC wants to transmit data across the local loop, the traffic is encoded in the higher frequency band reserved for data traffic. The ADSL modem knows to do this because the traffic is arriving on a port reserved for data devices. Upon arrival at the CO, the data traffic does not travel to the local switch; instead, it stops at the ADSL modem that has been installed at the CO end of the circuit. In this case, the device is actually a bank of modems that serves a large number of subscribers and is known as a *Digital Subscriber Line Access Multiplexer* (DSLAM) (pronounced "dee-slam"). A DSLAM is shown in Figure 5-5.

Instead of traveling on to the local switch, the data traffic is now passed around the switch to a router, which in turn is connected to the Internet. This process is known as a *line-side redirect*.

The advantages of this architecture are fairly obvious. First, the redirect offloads the data traffic from the local switch so that it can go back to doing what it does best, switching voice traffic. Second, it creates a new line of business for the service provider. As a result of adding the router and connecting the router to the Internet, the service provider instantly becomes an ISP. This is a near-ideal combination, because it enables the service provider to become a true service provider by offering much more than simple access and transport.

As the name implies, ADSL provides two-wire asymmetric service; that is, the upstream bandwidth is different from the downstream. In the upstream direction, data rates vary from 16 to 640 Kbps, whereas the downstream bandwidth varies from 1.5 to 8 Mbps. Because most applications today are asymmetric in nature, this disparity poses no problem for the average consumer of the service.

Figure 5-5
A bay of DSLAMs.

A Word about the DSLAM

This device has received a significant amount of attention recently because of the central role that it plays in the deployment of broadband access services. Obviously, the DSLAM must interface with the local switch so that it can pass voice calls on to the *Public Switched Telephone Network* (PSTN). However, the DSLAM often interfaces with a number of other devices as well. For example, on the customer side, the DSLAM may connect to a standard ATU-C, directly to a PC with a built-in *Network Interface Card* (NIC), to a variety of DSL services, or to an integrated access device of some kind. On the trunk side (facing the switch), the DSLAM may connect to IP routers as described, to an *Asynchronous Transfer Mode* (ATM) switch, or to some other broadband service

provider. It therefore becomes the focal point for the provisioning of a wide variety of access methods and service types.

High Bit Rate Digital Subscriber Line (HDSL)

The greatest promise of HDSL is that it provides a mechanism for the deployment of four-wire T1 and E1 circuits without the need for span repeaters, which can add significantly to the cost of deploying data services. It also means that service can be deployed in a matter of days rather than weeks, something customers certainly applaud.

DSL technologies in general enable repeaterless facilities as far as 12,000 feet, while traditional four-wire data circuits such as T1 and E1 require repeaters every 6,000 feet. Consequently, many telephone companies are now using HDSL "behind the scenes" as a way to deploy these traditional services. Customers do not realize that the T1 facility that they are plugging their equipment into is being delivered using HDSL technology. The important thing is that they don't *need* to know. All the customer should have to care about is that a SmartJack is installed in the basement, and through that jack they have access to 1.544 Mbps or 2.048 Mbps of bandwidth, period.

HDSL2

HDSL2 offers the same service that HDSL offers, with one added (and significant) advantage: it does so over a single pair of wire, rather than two. It also provides other advantages. First, it was designed to improve vendor interoperability by requiring less equipment at either end of the span (transceivers or repeaters). Second, it was designed to work within the confines of standard telephone company *carrier serving area* (CSA) guidelines by offering a 12,000-foot wire-run capability that matches the requirements of CSA deployment strategies. (See the discussion on CSA guidelines later in this section.)

A number of companies have deployed T-1 access over HDSL2 at rates 40 percent lower than typical T-Carrier prices. Furthermore, a number of vendors including 3Com, Lucent, Nortel Networks, and Alcatel have announced their intent to work together to achieve interoperability among DSL modems.

Rate Adaptive Digital Subscriber Line (RADSL)

RADSL (pronounced "rad-zel") is a variation of ADSL designed to accommodate changing line conditions that can affect the overall performance of the circuit. Like ADSL, it relies on DMT encoding, which selectively "populates" subcarriers with transported data, thus allowing for granular rate-setting.

Very High-Speed Digital Subscriber Line (VDSL)

VDSL is the newest DSL entrant in the bandwidth game and shows promise as a provider of extremely high levels of access bandwidth, as much as 52 Mbps over a short local loop. VDSL requires *Fiber-to-the-Curb* (FTTC) architecture and recommends ATM as a switching protocol. From a fiber hub, copper tail circuits deliver the signal to the business or residential premises. The bandwidth available through VDSL ranges from 1.5 to 6 Mbps on the upstream side, and from 13 to 52 Mbps on the downstream side. Obviously, the service is distance-sensitive and the actual achievable bandwidth drops as a function of distance. Nevertheless, even a short loop is respectable when such high bandwidth levels can be achieved. With VDSL, 52 Mbps can be reached over a loop length of up to 1,000 feet, not an unreasonable distance by any means.

g.lite

Because the installation of splitters has proven to be a contentious and problematic issue, the need has arisen for a version of ADSL that does not require them. That version is known as either ADSL Lite or g.lite (after the ITU-T G-Series standards that govern much of the ADSL technology). In 1997, Microsoft, Compaq, and Intel created the *Universal ADSL Working Group* (UAWG),[1] an organization that grew to nearly 50

[1] The group "self-dissolved" in the summer of 1999 after completing what they believed their charter to be.

members dedicated to the task of simplifying the rollout of ADSL. In effect, the organization had four stated goals:

- To ensure that analog telephone service will work over the g.lite deployment without remote splitters, in spite of the fact that the quality of the voice may suffer slightly due to the potential for impedance mismatch.
- To maximize the length of deployed local loops by limiting the maximum bandwidth provided. Research indicates that customers are far more likely to notice a performance improvement when migrating from 64 Kbps to 1.5 Mbps than when going from 1.5 Mbps to higher speeds. Perception is clearly important in the marketplace, so the UADSL Working Group chose 1.5 Mbps as their downstream speed.
- To simplify the installation and use of ADSL technology by making the process as "plug-and-play" as possible.
- To reduce the cost of the service to a perceived reasonable level.

Of course, g.lite is not without its detractors. A number of vendors have pointed out that if g.lite requires the installation of microfilters at the premises on a regular basis, then true splitterless DSL is a myth, because microfilters are in effect a form of splitter. They contend that if the filters are required anyway, then they might as well be used in full-service ADSL deployments to guarantee a high-quality service delivery.

Unfortunately, this flies in the face of one of the key tenets of g.lite, which is to simplify and reduce the cost of DSL deployment by eliminating the need for an installation dispatch (a "truck roll" in the industry's parlance). The key to g.lite's success in the eyes of the implementers is to eliminate the dispatch, minimize the impact on traditional POTS telephones, reduce costs, and extend the achievable drop length. Unfortunately, customers still have to be burdened with the installation of microfilters, and coupled noise on POTS is higher than expected. Many vendors argue that these problems largely disappear with full-feature ADSL using splitters; a truck dispatch is still required, but again, it is often required to install the microfilters anyway, so there is no net loss. Furthermore, a number of major semiconductor manufacturers support both g.lite and ADSL on the same chipset, so the decision to migrate from one to the other is a simple one that does not necessarily involve a major replacement of internal electronics.

DSL Market Issues

DSL technology offers advantages to both the service provider and the customer. The service provider benefits from successful DSL deployment because it serves not only as a cost-effective technique for satisfying the bandwidth demands of customers in a timely fashion, but also because it provides a Trojan horse approach to the delivery of certain pre-existing services. As we noted earlier, many providers today implement T-1 and E-1 services over HDSL because it offers a cost-effective way to do so. Customers are blissfully unaware of that fact; in this case, it is the service provider rather than the customer who benefits most from the deployment of the technology. From a customer point-of-view, DSL provides a cost-effective way to buy medium-to-high levels of bandwidth and, in some cases, embedded access to content.

Provider Challenges

The greatest challenges facing those companies looking to deploy DSL are competition from cable and wireless, pent-up customer demand, installation issues, and plant quality.

Competition from cable and wireless companies represents a threat to wireline service providers on several fronts. First, cable modems enjoy a significant amount of press and are therefore gaining well-deserved marketshare. The service they provide is for the most part well received and offers high-quality, high-speed access. Wireless, on the other hand, is a slumbering beast. It has largely been ignored as a serious competitor for data transport, but recent announcements prove that its viability as a contender is real. In July of 2001, AT&T announced that it will begin offering 40-Kbps service to Motorola handsets in the Seattle area immediately and will offer 384-Kbps service early in 2002.

The second challenge is unmet customer demand. If DSL is to satisfy the broadband access requirements of the marketplace, it must be made available throughout ILEC service areas. This means that incumbent providers must equip their central offices with DSLAMs that will provide the line-side redirect required as the initial stage of DSL deployment. The law of primacy is evident here; the ILECs must get to market first with broadband offerings if they are to achieve and keep a place in the burgeoning broadband access marketplace.

The third and fourth challenges to rapid and ubiquitous DSL deployment are installation issues and plant quality. A significant number of impairments have proven to be rather vexing for would-be deployers of widespread DSL. These challenges fall into two categories: electrical disturbances and physical impairments.

Electrical Disturbances

The primary cause of electrical disturbance in DSL is crosstalk, caused when the electrical energy carried on one pair of wires "bleeds" over to another pair and causes interference (noise) there. Crosstalk exists in several flavors. *Near-end crosstalk* (NEXT) occurs when the transmitter at one end of the link interferes with the signal received by the receiver at the same end of the link. *Far-end crosstalk* (FEXT) occurs when the transmitter at one end of the circuit causes problems for the signal sent to a receiver at the far end of the circuit.

Similarly, problems can occur when multiple DSL services of the same type exist in the same cable and interfere with one another. This is referred to as *self-NEXT* or *self-FEXT*. When different flavors of DSL interfere with one another, the phenomenon is called *Foreign-NEXT* or *foreign-FEXT*.

Another problem that can cause errors in DSL and therefore a limitation in the maximum achievable bandwidth of the system is *radio frequency interference* (RFI), which can find its way into the system. Other problems include impulse, Gaussian, and random noises that exist in the background but can affect signal quality even at extremely low levels.

Physical Impairments

The physical impairments that can have an impact on the performance of a newly deployed DSL circuit tend to be characteristics of the voice network that typically have a minimal effect on simple voice and low-speed data services. These include load coils, bridged taps, splices, mixed gauge loops, and weather conditions.

Load Coils and Bridged Taps

We have already mentioned the problems that load coils can cause for digital transmission; because they limit the frequency range that is

allowable across a local loop, they can seriously impair transmission. Bridged taps are equally problematic. When a multipair telephone cable is installed in a newly built-up area, it is generally some time before the assignment of each pair to a home or business is actually made.

To simplify the process of installation when the time comes, the cable's wire pairs are periodically terminated in terminal boxes (sometimes called B-boxes) installed every block or so. As we discussed in Chapter 3, "Telephony," there may be multiple appearances of each pair on a city street, waiting for assignment to a customer. When the time comes to assign a particular pair, the installation technician will simply go to the terminal box where that customer's drop appears and cross-connect the loop to the appearance of the cable pair (a set of lugs) to which that customer has been assigned. This eliminates the need for the time-consuming process of splicing the customer directly into the actual cable.

Unfortunately, this efficiency process also creates a problem. Although the customer's service has been installed in record time, each of the terminal boxes along the street contain unterminated appearances of the customer's cable pair. These so-called bridged taps present no problem for analog voice, yet they can be a catastrophic source of noise due to signal reflections that occur at the copper-air interface of each bridged tap. If DSL is to be deployed over the loop, the bridged taps must be removed. Although the specifications indicate that bridged taps do not cause problems for DSL, actual deployment says otherwise. To achieve the bandwidth that DSL promises, the taps must be terminated.

Splices and Gauge Changes

Splices can result in service impairments due to cold solder joints, corrosion, or weakening effects caused by the repeated bending of wind-driven aerial cable.

Gauge changes tend to have the same effects that plague circuits with unterminated bridged taps. When a signal traveling down a wire of one gauge jumps to a piece of wire of another gauge, the signal is reflected, resulting in an impairment known as an *intersymbol interference*. The use of multiple gauges is common in a loop deployment strategy because it enables outside plant engineers to use lower-cost small gauge wire where appropriate, cross-connecting it to larger-gauge, lower-resistance wire where necessary.

Weather

Weather is perhaps a bit of a misnomer; the real issue is moisture. One of the greatest challenges facing DSL deployment is the age of the outside plant. Much of the older distribution cable uses inadequate insulation between the conductors (paper in some cases). In some instances, the outer sheath has cracked, allowing moisture to seep into the cable itself. The moisture causes crosstalk between wire pairs that can last until the water evaporates. Unfortunately, this can take a considerable amount of time and result in extended outages.

Solutions

All of these factors have solutions. The real question is whether they can be remedied at a reasonable cost. Given the growing demand for broadband access, there seems to be little doubt that the elimination of these factors would be worthwhile at all reasonable costs, particularly considering how competitive the market for the local loop customer has become.

The electrical effects, largely caused by various forms of crosstalk, can be reduced or eliminated in a variety of ways. Physical cable deployment standards are already in place that, when followed, help to control the amount of near and far-end crosstalk that can occur within binder groups in a given cable. Furthermore, filters have been designed that eliminate the background noise that can creep into a DSL circuit.

Physical impairments can be controlled to a point, although to a certain extent the service provider is at the mercy of their installed network plant. Obviously, older cable will present more physical impairments than newer cable, but the service provider can take steps to maximize their success rate when entering the DSL marketplace. The first step is to pre-qualify local loops for DSL service to the greatest extent possible. This means running a series of tests using *mechanized loop testing* (MLT) to determine whether each loop's transmission performance falls within the bounds established by the service provider and the standards and industry-support organizations.

For DSL pre-qualification, MLT tests the following performance indicators (and others as required):

- Cable architecture
- Loop length
- Crosstalk and background noise

56K modems, ISDN, and DSL represent the primary access technologies that the telephone companies offer. Recently, however, a new contender has entered the game: the cable provider. The section that follows describes the technology they offer and the role that they play in the evolving access marketplace.

Cable-Based Access Technologies

In 1950, Ed Parsons placed an antenna on a hillside above his home in Washington State, attached it to a coaxial cable distribution network, and began to offer television service to his friends and neighbors. Prior to his efforts, the residents of his town were unable to pick up broadcast channels because of the blocking effects of the surrounding mountains. Thanks to Parsons, *community antenna television* (CATV) was born; from its roots came cable television.

Since that time, the cable industry has grown into a $35-billion industry. In the United States alone, 10,000 head-ends deliver content to 60 million homes in more than 22,000 communities over more than 1 million miles of coaxial and fiber-optic cable. As the industry's network has grown, so too have the aspirations of those deploying it. Their goal is to make it much more than a one-way medium for the delivery of television and pay-per-view; they want to provide a broad spectrum of interactive, two-way services that will enable them to compete head-to-head with the telephony industry. To a large degree, they are succeeding. The challenges they face, however, are daunting.

Playing in the Broadband Game

Unlike the telephone industry that began its colorful life under the scrutiny of a small number of like-minded individuals (Alexander

Graham Bell and Theodore Vail, among others), the cable industry came about thanks to the combined efforts of hundreds of innovators, each building on Parson's original concept. As a consequence, the industry, while enormous, is in many ways fragmented. Powerful industry leaders like John Malone and Gerald Levine were able to exert "Tito-like"[2] powers to unite the many companies, turning a loosely cobbled-together collection of players into cohesive, powerful corporations with a shared vision of what they were capable of accomplishing.

Today the cable industry is a force to be reckoned with, and upgrades to the original network are underway. This is a crucial activity that will ensure the success of the industry's ambitious business plan and provide a competitive balance for the traditional telcos.

The Cable Network

The traditional cable network is an analog system based on a tree-like architecture. The head-end, which serves as the signal origination point, serves as the signal aggregation facility. It collects programming information from a variety of sources, including satellite and terrestrial feeds. Head-end facilities often look like a mushroom farm; they are typically surrounded by a variety of satellite dishes (see Figures 5-6 and 5-7).

The head-end is connected to the downstream distribution network by a 1-inch diameter rigid coaxial cable, as shown in Figure 5-8. That cable delivers the signal, usually a 450-MHz collection of 6-MHz channels, to a neighborhood where splitters divide the signal and send it down half-inch diameter semi-rigid coax that typically runs down a residential street. At each house, another splitter (see Figure 5-9) pulls off the signal and feeds it to the set-top box in the house over the drop wire, a "local loop" of flexible quarter-inch coaxial cable.

Although this architecture is perfectly adequate for the delivery of one-way television signals, its shortcomings for other services should be fairly obvious to the reader. First of all, it is, by design, a broadcast system. It does not typically have the capability to support upstream traffic (from the customer toward the head-end) and is therefore not suited for interactive applications.

[2] Josip Broz Tito was able to stitch a handful of independent Balkan countries into the Federation of Yugoslavia for many years because of his strength of character and vision.

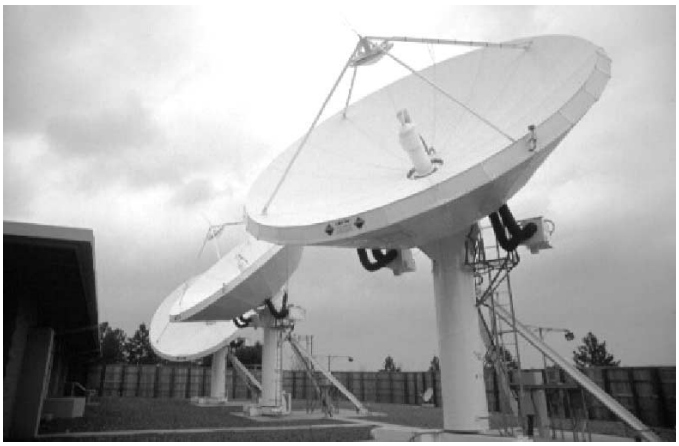


Figure 5-6
Satellite receive antennas at cable head end facility.

Figure 5-7
Smaller satellite receive antennas at cable head end facility.

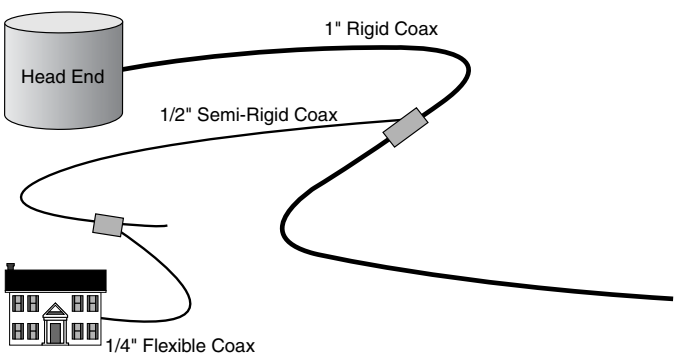


Figure 5-8
Layout of typical cable distribution network.

Figure 5-9
Signal splitter in residential cable installation.

Second, because of its design, the network is prone to significant failures that have the potential to affect large numbers of customers. The tree structure, for example, means that if a failure occurs along any "branch" in the tree, every customer from that point downward loses service. Contrast this with the telephone network where customers have a dedicated local loop over which their service is delivered. Also, because the system is analog, it relies on amplifiers to keep the signal strong as it is propagated downstream. These amplifiers are powered locally; they do not have access to "CO power" as devices in the telephone network do. Consequently, a local power failure can bring down the network's ability to distribute service in that area.

The third issue is one of customer perception. For any number of reasons, the cable network is generally perceived to not be as capable or reliable as the telephone network. As a consequence of this perception, the cable industry is faced with the daunting challenge of convincing potential voice and data customers that they are in fact capable of delivering high-quality service.

Some of the concerns are justified. In the first place, the telephone network has been in existence for almost 125 years, during which time its operators have learned how to optimally design, manage, and operate it

in order to provide the best possible service. The cable industry, on the other hand, came about 50 years ago and didn't benefit from the rigorously administered, centralized management philosophy that characterized the telephone industry. Additionally, the typical 450-MHz cable system did not have adequate bandwidth to support the bidirectional transport requirements of new services.

Furthermore, the architecture of the legacy cable network, with its distributed power delivery and tree-like distribution design, does not lend itself to the same high degree of redundancy and survivability that the telephone network offers. Consequently, cable providers have been hard-pressed to convert customers who are vigorously protective of their telecommunications services.

Evolving Cable Systems

Faced with these harsh realities and the realization that the existing cable plant could not compete with the telephone network in its original analog incarnation, cable engineers began a major rework of the network in the early 1990s. Beginning with the head-end and working their way outward, they progressively redesigned the network to the extent that in many areas of the country their coaxial local loop was capable of competing on equal footing with the telco's twisted pair, and in some cases beating it.

The process they have used in their evolution consists of four phases. In the first phase, they converted the head-end from analog to digital. This enabled them to digitally compress the content, resulting in a far more efficient utilization of available bandwidth.

Then they undertook an ambitious physical upgrade of the coaxial plant, replacing the 1-inch trunk and half-inch distribution cable with optical fiber. This brought about several desirable results. First, by using a fiber feeder, network designers were able to eliminate a significant number of the amplifiers responsible for the failures the network experienced due to power problems in the field. Second, the fiber makes it possible to provision significantly more bandwidth than coaxial systems enable. Third, because the system is digital, it suffers less from noise-related errors than its analog predecessor did.

Finally, an upstream return channel was provisioned, as shown in Figure 5-10, which makes possible the delivery of true interactive services such as voice, Web surfing, and videoconferencing.

The third phase of the conversion has to do with the equipment provisioned at the user's premises. The analog set-top box has now been

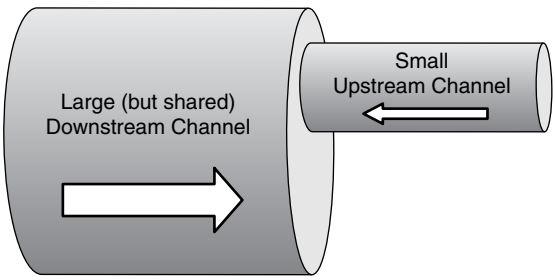


Figure 5-10 Upstream and downstream channels in modern cable systems.

replaced with a digital device that has the capability to take advantage of network capabilities, including access to the upstream channel. It decompresses digital content, performs content ("stuff") separation, and provides the network interface point for data and voice devices.

The final phase is business conversion. Cable providers look forward to the day when their networks will compete on equal footing with the twisted pair networks of the telephone company, and customers will see them as viable competitors. In order for this to happen, cable providers must demonstrate that their network is capable of delivering a broad variety of competitive services and that the network is robust. They also must prove that they have *operations support systems* (OSSs) that will guarantee the robustness of the infrastructure and that they are cost-competitive with incumbent providers. Cable providers must also create a presence for themselves in the business centers of the world. Today they are almost exclusively residential service providers; if they are to break into the potentially lucrative business market, they must have a presence there.

Cable Modems

As cable providers have progressively upgraded their networks to include more fiber in the backbone, their plan to offer two-way access to the Internet has become a reality. Cable modems offer access speeds of up to 10 Mbps, and so far the market uptake has been spectacular.

Cable modems provide an affordable option to achieve high-speed access to the Web, with current monthly subscription rates in the neighborhood of $40. They offer asymmetric access, that is, a much higher downstream speed than upstream, but for the majority of users, this does not represent a problem since the bulk of their use will be for

Web surfing during which the bulk of the traffic travels in the downstream direction anyway.

Although cable modems do speed up access to the Web and other online services by several orders of magnitude, a number of downsides must be considered. The greatest concern that has been voiced about cable modems is security. Because cable modems are "always on," they represent an easy entry point for hackers looking to break into machines. It is therefore *critical* that cable subscribers use some form of firewall software or a router that has the capability to perform filtering.

Data over Cable Standards

As interest grew in the late 1990s for broadband access to data services over cable television networks, CableLabs®, working closely with the ITU and major hardware vendors, crafted a standard known as the *Data Over Cable Service Interface Specification* (DOCSIS). The standard is designed to ensure interoperability among cable modems as well as to assuage concerns about data security over shared cable systems. DOCSIS has done a great deal to resolve marketplace issues.

Under the standards, CableLabs® crafted a cable modem certification standard called DOCSIS 1.0 that guarantees that modems carrying the certification will interoperate with any head-end equipment, are ready to be sold in the retail market, and will interoperate with other certified cable modems. Engineers from Askey, Broadcom, Cisco Systems, Ericsson, General Instrument, Motorola, Philips, 3Com, Panasonic, Digital Furnace, Thomson, Terayon, Toshiba, and Com21 participated in the development effort.

The DOCSIS 1.1 specification was released in April 1999 and included two additional functional descriptions that began to be implemented in 2000. The first specification details procedures for guaranteed bandwidth as well as a specification for *Quality of Service* (QoS) guarantees. The second specification is called *Baseline Privacy Interface Plus* (BPI+) and it enhances the current security capability of the DOCSIS standards through the addition of digital certificate-based authentication and support for multicast services to customers.

Although the DOCSIS name is in widespread use, CableLabs now refers to the overall effort as the CableLabs Certified Cable Modem Project.

Wireless Access Technologies

It is only in the last few years that wireless access technologies have advanced to the point that they are being taken seriously as contenders for the broadband local loop market. Traditionally, a minimal infrastructure was in place, and it was largely bandwidth-bound and error-prone to the point that wireless solutions were not considered serious contenders.

Wireless Access

To understand wireless communications, it is necessary to examine both radio and telephone technologies, because the two are inextricably intertwined. In 1876, Alexander Graham Bell, a part-time inventor and a teacher of hearing-impaired students, invented the telephone while attempting to resolve the challenge of transmitting multiple telegraph signals over a shared pair of wires. His invention changed the world forever.

In 1896, a mere 20 years later, Italian engineer and inventor Guglielmo Marconi developed the spark gap radio transmitter, which eventually enabled him to transmit long-wave radio signals across the Atlantic Ocean as early as 1901. Like Bell, his invention changed the world; for his contributions, he was awarded the Nobel Prize in 1909.

It wasn't until the 1920s, though, when these two technologies began to dovetail, that their true promise was realized. Telephony provided interpersonal, two-way, high-quality voice communications, but required the user to be stationary. Radio, on the other hand, provided mobile communications, but was limited by distance, environmentally induced signal degradation, and spectrum availability. Although telephony was advertised as a universally available service, radio was more of a catch-as-catch-can offering that was subject to severe blocking. If a system could be developed that combined the signal quality and ubiquity of telephony with the mobility of radio, however, a truly promising new service offering could be made available.

Today cellular telephony (and other services like it) provides high-quality, *almost* ubiquitous, wireless telephone service. Thanks to advances in digital technology, wireless telephony also offers services identical to those provided by the wired network. Pricing for wired and wireless services is also now reaching parity; flat rate nationwide pricing models are commonplace today that have no roaming or long-distance restrictions.

A Bit of History

The road to the modern wireless communications network was fraught with technical, bureaucratic, and social speed bumps. In 1905, listeners in New York City, accustomed to the staccato beat of Morse code broadcasts spewing from their radios, were astounded to hear music and voice as Reginald Fessenden, a local radio commentator, broadcast the results of the annual New York City yacht races. Listeners could hear the results immediately, instead of waiting for the late edition of the paper. Public perception of the possibilities of radio suddenly began to grow.

At roughly the same time, the U.S. military, recognizing the potentially strategic value of radio communications in the armed forces, helped to create the *Radio Corporation of America* (RCA), ushering wireless technology into the technological forefront.

The first wireless applications were developed in 1915 and 1916 for ship-to-ship and ship-to-shore communications. In 1921, the Detroit Police Department inaugurated the first land-based mobile application for radio communications when they installed one-way radios in patrol cars, the original "calling all cars" application. The system required police officers to stop at a phone (see Figure 5-11) to place a call to their precinct when a call came in. However, the ability to quickly and easily communicate with roving officers represented a giant step forward for the police and their ability to respond quickly to calls.

Unfortunately, the system was not without its problems. Even though the transmitter was powerful, Detroit's deep concrete canyons prevented the signal from reaching many areas. Equally vexing was the problem of motion. The delicate vacuum tubes, subjected to the endless vibrations stemming from life in the trunk of a moving vehicle, caused both physical and electronic problems that were so bad that in 1927 the Detroit Police Department shut down the station out of sheer frustration. It wasn't until 1928, when Purdue University student Robert Batts developed a superheterodyne radio that was somewhat resistant to buffeting and vibration, that Detroit reinaugurated its radio system.

Other cities followed in Detroit's footsteps. By 1934, nearly 200 radio-equipped city police departments were communicating with nearly 5,000 roving vehicles. Radio had become commonplace, and in 1937 the FCC stepped in and allocated 19 additional radio channels to the 11 that they had already made available for police department use. No one realized it, but the spectrum battles had begun.

Early radio systems were based on *amplitude modulation* (AM) technology. One drawback of AM radio is the fact that the strength of the

Figure 5-11
Police call box.

transmitted signal diminishes according to the square of the distance. A signal measured at 20 watts and one mile from the transmitter will be *one quarter* that strength, or five watts, at *two* miles from the transmitter. When Edwin Armstrong (refer to Chapter 1, "First Things First") announced and demonstrated his invention of frequency-modulated radio in 1935, he turned the broadcast industry on its ear. He offered a technology that not only eliminated the random noise and static that plagued AM radio, but also lowered transmitter power requirements and improved the capability of receivers to lock onto a weak signal.

World War II provided an ideal testing ground for FM. AM radio, used universally by the Axis powers during the war, was easily jammed by powerful Allied transmitters. FM, on the other hand, used only by Allied forces, was unaffected by AM jamming techniques. As we mentioned earlier, many historians believe that FM radio was crucially important to the Allies' success in World War II.

Radio's Evolution

Radio is often viewed as having evolved in two principal phases. The first was the pioneer phase, during which the fundamental technologies were developed, initial technical bugs were ironed out, applications were created (or at least conceived), and bureaucratic and governmental haranguing over the roles of various agencies was initiated. This phase was characterized by the development and acceptance of FM transmission, the dominance of military and police usage of radio, and the challenge of building a radio that could withstand the rigors of mobile life. The pioneer phase lasted until the early 1940s when the commercial phase began.

During the 1940s, radio technology advanced to the point that FM-based car phones were commercially available. Initially, AT&T provided mobile telephone service under the umbrella of its nationwide monopoly. In 1949, however, the Justice Department filed suit against AT&T, settling the case with the Consent Decree of 1956. Under this Consent Decree, AT&T kept its telephone monopoly, but was forced to give up a number of other lines of business, including the manufacture of mobile radiotelephones. This enabled companies like Motorola to enter the fray and paved the way for the creation of *radio common carriers* (RCCs), much to AT&T's chagrin. These RCCs were typically small businesses that offered wireless service to several hundred people in a fixed geographical area.

A Touch of Technology

Before proceeding further, let's introduce some fundamentals of radio transmission.

For radio waves to carry information such as voice, data, music, or images, certain characteristics of the waves are changed or *modulated.* Those characteristics include the amplitude, or loudness, of the wave; the frequency, or pitch, of the wave; and the phase, or angle of inflection, of the wave. By modulating these characteristics, a *carrier wave* can be made to transport information, whether it is a radio broadcast, a data stream, or a telephone conversation. (Please review this topic in Chapter 1 for more information.)

Transmission "space" is allocated based on ranges of available frequency. This range is known as a spectrum, a word that means "a range of values." The radio spectrum represents a broad span of

electromagnetic frequencies between one kilohertz (kHz, 1,000 cycles per second) and 10 *quintillion* (that's 10 followed by 19 zeroes) cycles per second. Most radio-based applications operate at frequencies between 1 kHz and 300 GHz.

One concern that has surfaced repeatedly over the years since the inception of radio is spectrum availability. Different services require differing amounts of spectrum for proper operation. For example, a modern FM radio channel requires 30 kHz of bandwidth, whereas an AM channel only requires 3 kHz. Television, on the other hand, requires 6 MHz. As you might imagine, battles between the providers of these disparate services over spectrum allocation became quite heated in the years that followed.

Improving the Model

The first FM radiotelephone systems were massively inefficient. They required 120 kHz of channel bandwidth to transport a 3-kHz voice signal. As the technology advanced, though, this requirement was reduced. In the 1950s, the FCC mandated that channels be halved to 60 kHz, and by the 1960s things had advanced to the point that the spectrum could be further reduced to 30 kHz, where it remains today in analog systems. Realize that this is *still* a 10:1 ratio.

AT&T introduced the first commercial mobile telephone service in St. Louis in 1946. It relied on a single, high-power transmitter placed atop one of the city's tallest buildings and had an effective service range of about 50 miles. This FM system was fully interconnected with AT&T's wireline telephone network.

The service was not cheap. The monthly charge was $15, and usage was billed at a flat 15¢ per minute. In spite of the cost, the service was quite popular, a fact that led to its undoing.

System engineers based their design on existing radio systems that were primarily designed for dispatch applications. The traffic patterns of radio dispatches are different than telephony: a dispatch occupies several seconds of airtime, while a telephone call typically lasts several minutes. Almost immediately, blocking became a serious problem. In fact, in New York City, where the service quickly became popular, AT&T had 543 active subscribers in 1976 and a waiting list of nearly 4,000 anxious-to-be-connected customers that the system's limited capacity could not accommodate.

Radio design played a role in improving spectrum utilization. The first systems, such as the one in St. Louis, used a scheme called *nontrunked radio.* In nontrunked radio systems, the available spectrum was divided into channels and groups of users were assigned to those channels. The advantage of this technique is that non-trunked radios were relatively inexpensive. The downside was that certain channels could become severely overloaded, while others remained virtually unused.

The invention of *trunked radio* relieved this problem immensely. Trunked radios were *frequency agile,* meaning that all radios could access all channels. When a user placed a call, the radio unit would search for an available channel and use it. With the arrival of this capability, blocking became a non-issue. The downside, of course, was that frequency-agile radios, because of their more complex circuitry, were significantly more expensive than their nontrunked predecessors.

Most of this work was conducted during the turbulent 1960s and led to Bell Labs' introduction of *Improved Mobile Telephone Service* (IMTS). IMTS used two 30-kHz, narrowband FM channels for each conversation and provided full-duplex talk paths, direct dialing, and automatic trunking. Introduced commercially in 1965, IMTS is considered to be the predecessor of modern cellular telephony.

The Spectrum Battles Heat up

Starting in the mid-1940s, mobile telephony went head to head against the television industry in a pitched battle for spectrum. In 1947, the Bell System proposed to the FCC a plan for a large-scale mobile telephone system, asking them to allocate 150 two-way, 100-kHz channels. The proposal was not accepted.

In 1949, while the FCC wrestled with the assignment of spectrum in the 470- to 890-MHz range that would become *Ultra-High Frequency* (UHF) television, the telephone industry argued that they should be granted a piece of the electromagnetic pie. Their issue was that the 6 MHz of bandwidth required for a single TV channel was more than had *ever* been allocated for mobile telephony. Unfortunately, television had penetrated the American household; Captain Kangaroo, Roy Rogers, and Winky-Dink captivated viewers; and consumers were hungry for additional programming. Wireless telephony wasn't even on their radar screens; it would have to wait.

In the 20 years that followed, mobile telephony continued to take a backseat to television. UHF usage grew slowly; in 1957, the Bell System petitioned the FCC to give them a piece of the earmarked spectrum in the 800-MHz range that was virtually unused. But television was still the darling of the nation, and the FCC was ferociously dedicated to expanding the deployment of UHF television. In 1962, the government signed into law the All Channels Receiver Act that mandated that all new televisions must have both *Very High Frequency* (VHF) and UHF receivers. Remember when televisions had two tuner knobs on them? TV won again.

Between 1967 and 1968, the FCC and the House of Representatives, under pressure from the telephone industry, studied the issue of spectrum allocation once again. In 1968, the FCC convened the "Cellular Docket," a contentious and highly visible collection of lawmakers who eventually ruled that mobile telephony's concerns could only be solved by giving them spectrum. In 1970, the FCC reallocated UHF channels 70 to 83 from television to mobile services. From the resulting 115-MHz electromagnetic chunk, 75 MHz was allocated to mobile telephony, with 40 MHz available immediately and 35 MHz held in reserve.

Once the spectrum was allocated, the political games began. It was roundly assumed that AT&T would design, install, and operate the wireless network as an extension of its own universal wireline network. After all, the spectrum allocation was "deeded" to the wireline telephone companies, and because AT&T provided service to roughly 85 percent of the market, this assumption was somewhat natural. Their *Advanced Mobile Phone System* (AMPS) architecture, based on the same design philosophy as the wireline network, relied on a massively expensive switching infrastructure, hundreds of cells, and centralized control of all functions.

AT&T's only competitors in this market were the RCCs, mentioned earlier. Among them were Motorola, even then a large player in the industry. Initially, Motorola sided with AT&T, but when AT&T chose other vendors to manufacture the equipment required to establish the network, Motorola changed its spots and sided with the other 500 and some-odd RCCs in the country to sue the FCC for unfair treatment. Their suit called for the Commission to deny AT&T's application for the development of AMPS and to re-examine the spectrum allocation. In 1970, Motorola, in partnership with another large RCC, applied for permission to offer wireless service in Washington, D.C. After examining the petition, the courts decided that the answer to the industry's woes lay in a competitive market. In 1980, they began another cellular rulemaking

effort to determine the regulatory structure of the market they were attempting to create.

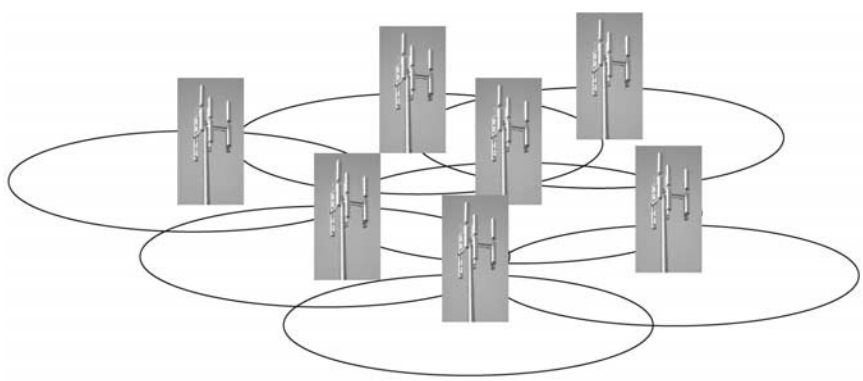
Three options emerged from their discussions. The first was preservation of the monopolistic, single-operator concept, while the second advocated an open market, in which competition was opened to all comers and the market would sort itself out. The third involved a duopoly approach, in which two systems would be allowed in each major market area. After long debate, regulators and lawmakers decided on the duopoly concept, with two 20-MHz systems (A frequencies and B frequencies) allocated in each market. The A frequencies were allocated to the nonwireline company, whereas the B frequencies went to the wireline carrier.

The first commercial cellular telephone system became operational in October of 1983. By 1985, there were 340,000 cellular subscribers; today there are over 16 million, with annual revenues of nearly $11 billion. It's interesting to note that in 1982, AT&T proudly predicted that there would be over 100,000 cellular subscribers by 1990.

Cellular Telephony

As modern as cellular telephony is considered to be, it was originally conceived in the 1940s at Bell Labs as part of a plan to overcome the congestion and poor service issues associated with mobile telephone systems.

Figure 5-12 *An array of low-power cells in a cellular network. Notice how the coverage areas overlap, allowing handoff of a call to occur from one cell to another. Also, because of low power and distance, frequencies can be reused.*



Cellular systems have four key design principles, shown in Figure 5-12, which are the same today as they were in the 1940s. These design principles consist of the use of many low-power, small coverage area transmitters instead of a single, powerful, monolithic transmitter to cover a wide area; frequency reuse; the concept of cell splitting; and central control and cell-to-cell handoff of calls. These concepts are fairly straightforward. The first relies on the philosophy that the whole is greater than the sum of its parts. By using a large number of low-power transmitters scattered across a broad coverage zone, each capable of handling multiple simultaneous calls, more users can be supported than with a single, monolithic transmitter.

The second, frequency reuse, takes into account the fact that cellular telephony, like all radio-based services, has been allocated a limited number of frequencies by the FCC. By using geographically small, low-power cells, frequencies can be reused by non-adjacent cells.

When usage areas become saturated by excessive usage, cells can be split. When traffic engineers observe that the number of callers refused service because congestion reaches a critical level, they can split the original cell into two cells by installing a second site within the same geographical area that uses a different set of non-adjacent frequencies. This has an extended impact; as the cells become smaller, the total number of calls that the aggregate can support climbs dramatically. Because of cellular geometry, if the radius of the cell is halved, the number of supported calls is quadrupled. The smaller the cell, therefore, the larger the total number of simultaneous callers can be accommodated. Of course, this also causes the cost of deployment to climb dramatically. Although the architectural goal of most cellular providers is to create a mosaic of thousands of very small cells, called microcells or picocells, that's an expensive proposition and will not happen immediately.

Finally, cellular systems rely on a technique called cell-to-cell handoff, which simply means that the cellular network has the capability to track a call (using relative signal strength as an indicator) as the user moves across a cell. When the signal strength detected by the current cell is perceived by the system to be weaker than that detected by the cell the user is approaching, the call is handed off to the second cell. Ideally, the user hears nothing. Cell handoff and other cellular system capabilities are under the central control of a *Mobile Telephone Switching Office* or (MTSO, sometimes pronounced "Mitso").

OK, But How Does It Work?

When a user turns a cellular phone on, several things happen. First, the phone identifies itself to anyone willing to listen (hopefully, a local cell) by transmitting a unique identification code on a frequency that is designated as a *control channel.* The control channel is used for the transmission of operations and maintenance messages between cellular telephones and cell sites. If the phone is within the operating area of a cell site, the site registers the presence of the phone within its operating area, notifies the MTSO that all the cells in an area are connected to, and tracks its position, based on signal strength, as it moves around the cell.

When the user wants to place a call, he or she simply pushes the right buttons, which create simulated touch-tone sounds. Once dialing is complete, the user pushes the Send button, which causes the handset to transmit the buffered digits across the control channel to the local cell. The local cell hands the call off to the MTSO. The MTSO analyzes the digits, instructs the handset and the cell to use a particular set of frequencies for the call, and routes the call to the appropriate destination. MTSOs are interconnected to the wireline network and can therefore terminate calls at any location, including to another cellular user.

If driving while talking, the user may approach a cell boundary. The MTSO, which tracks the relative signal strength of each user as he or she moves among the various cells within its domain, will effect the handoff of a call from one cell to another if the user's movement (based on signal strength) indicates that he or she is approaching a cell boundary.

Access Methods

Traditional analog cellular telephony relies on a technique called *Frequency Division Multiple Access* (FDMA) as the access and frequency sharing scheme between mobile users and the cellular network. In FDMA systems, the available spectrum is divided into channels that are assigned to users on demand. One or more of the channels is reserved and set aside as control channels, used to transmit maintenance and operations information between the mobile phone and the network.

Each conversation requires two 30-kHz channels, one for the *forward,* or base-to-mobile direction, and one for the *reverse,* or mobile-to-base station direction. This pairing of channels permits true, full-duplex telephony.

In the same way that carrier systems evolved from analog to digital transmission, cellular telephony systems have evolved from analog, FDMA-based access schemes to digital access. Two schemes show the most promise.

The first, *Time-Division Multiple Access* (TDMA), resembles FDMA in that it divides the available frequency spectrum into channels. That, however, is where the resemblance ends. In TDMA, each of the analog channels carries telephone circuits that are time division multiplexed; that is, they share access to the channel. As in FDMA, a control channel is reserved for communication between the network and mobile users.

The biggest advantage that TDMA systems have over FDMA systems is that they support significantly more users. If each channel is divided into four time slots, then the system capacity is quadrupled. Although TDMA electronics are significantly more complex, the fact that they are digital means that they can easily evolve as technology advances.

The second digital access technique is called *Code-Division Multiple Access* (CDMA). CDMA systems are dramatically different from FDMA and TDMA systems in that they do not channelize the available bandwidth; instead, they enable all users to access and use the available spectrum simultaneously. This technique is called *spread spectrum transmission.* Unlike the traditional narrowband channels of FDMA and TDMA, CDMA channels are typically 1 to 10 MHz wide. Readers might be interested to know that spread spectrum transmission was coinvented during World War II by an electrical engineer who later became famous as a star of the silver screen, Hedy Lamarr. She was awarded the patent in 1941.

In CDMA systems, each mobile unit is assigned a unique random code sequence. Each machine uses this random code to uniquely identify its transmission and distinguish it from all other users.

Two distinct forms of spread spectrum access exist. The first, *Frequency Hopping Spread Spectrum* (FH/SS), uses the mobile unit's random code sequence to generate a series of unpredictable frequency hops. The unit literally jumps from frequency to frequency very quickly, in a pseudo-random fashion—pseudo-random because only the base unit and the network know the hopping pattern.

The second technique, called *Direct Sequence Spread Spectrum* (DSSS), uses the mobile unit's random code to convert the relatively low-bit-rate signal of the conversation into a high-bit-rate signal that sounds like noise to anyone else who is listening. Again, only the mobile unit and the network are capable of decoding the message stream. As a result, both FHSS and DSSS systems are highly secure.

Not only are these systems more secure than narrowband technologies, they also support significantly larger numbers of simultaneous users. In fact, whereas FDMA systems support a single-user-per-frequency slot, CDMA systems can support hundreds.

Radio-based telephony has enjoyed a wild, tumultuous ride along the way to its position today as a mainstream, foundation-level technology. Starting in the late 1800s with the parallel work of Marconi and Bell, radio and telephony wandered down different paths until fairly recently, when they converged and joined forces, leading to the development of cellular telephony.

The story doesn't end with cellular telephony, however. Today mobile users are clamoring for the ability to extend the reach of LANs, videoconferencing systems, medical image devices, and database access, without having to deal with the restrictions of a copper tether. Developing nations have realized that with cellular technology, telephony infrastructures can be installed in countries in a fraction of the time it takes to install a wired network. Alternatives such as infrared, microwave, satellite, and other radio technologies are providing wireless access in ways that weren't dreamed of 10 years ago.

Spectrum continues to be an issue, but advances in technology and forward-thinking legislators will help to overcome the problems of availability and management. In today's increasingly mobile society and a business environment that demands instantaneous, "anywhere, anytime" access to information, wireless communications is no longer an option or luxury. It is a business imperative.

Today, wireless is in the throes of a reinvention of itself in terms of both technology and services. Four evolutionary phases have taken place so far. *First-generation* (1G) systems, which originated in the late 1970s and continued in service widely throughout the 1980s, were entirely analog and supported almost exclusively voice with very little data. These systems are characterized by the use of FDMA technology.

Second-generation (2G) systems, which came about beginning in the 1990s, were all-digital and were still primarily voice-oriented, although data transport became more accepted. In 2G systems, digital access became the norm through such technologies as TDMA and CDMA.

The third phase, which many believe robs from the second phase, is called 2.5G. 2.5G represents a service awareness that is largely missing in 1G and 2G systems. The first two are largely technology implementations, while 2.5G solutions such as the *Global System for Mobile Communications* (GSM) represent a combination of multiple services delivered over a TDMA-like infrastructure. Many industry pundits are

actually referring to 2.5G as *third-generation* (3G), claiming that it already offers the full suite of services that most customers want.

I have conducted a very informal study of my own involving interviews with several hundred people, but the results do not differ significantly from the more formal studies conducted by large research organizations. In a nutshell, customers indicate that they want the following: ubiquitous roaming, reasonable usage prices, simplified billing, acceptable voice quality, and instant messaging. GSM offers those capabilities right now; many question the reason for 3G.

One reason is bandwidth. In true 3G systems, we see the emergence of broadband access and the promise of high-speed data in addition to voice. Access technologies for broadband include *Wideband CDMA* (W-CDMA) and enhancements to GSM-like networks such as the *General Packet Radio Service* (GPRS) and the *Enhanced Data for Global Evolution* (EDGE).

In late 1999, the ITU created a comprehensive set of 3G standards designed to harmonize the various technological directions that implementers have taken and to ensure that current systems can gracefully evolve to new 3G standards. These standards are called IMT2000 and may well overcome the challenge of interoperability among wireless standards. If 3G lives up to its promise, it will provide 2 Mbps to a stationary user, 384 Kbps to a walking user, and 128 Kbps to a user driving in a car. As if we don't have enough problems, it's bad enough that people try to drive while they're talking on the phone. Now they'll be surfing the Web. Super.

A new family of broadband wireless technologies has emerged that poses a threat to traditional wired access infrastructures. These include the *Local Multipoint Distribution Service* (LMDS), the *Multichannel Multipoint Distribution Service* (MMDS), and *Geosynchronous Earth Orbit* (GEO) and *Low Earth Orbit* (LEO) satellites.

Local Multipoint Distribution Service (LMDS)

LMDS is a bottleneck resolution technology, designed to alleviate the transmission restriction that occurs between high-speed LANs and *wide area networks* (WANs). Today local networks routinely operate at speeds of 100 Mbps (Fast Ethernet) and even 1,000 Mbps (Gigabit Ethernet), which means that any local loop solution that operates slower than either of those poses a restrictive barrier to the overall performance of

the system. LMDS offers a good alternative to wired options. Originally offered as CellularVision, it was seen by its inventor, Bernard Bossard, as a way to provide cellular television as an alternative to cable.

Operating in the 28-GHz range, LMDS offers data rates as high as 155 Mbps, the equivalent of SONET OC-3c. Because it is a wireless solution, it requires a minimal infrastructure and can be deployed quickly and cost-effectively as an alternative to the wired infrastructure provided by incumbent service providers. After all, the highest cost component (more than 50 percent) when building networks is not the distribution facility, but rather the labor required to trench it into the ground or build aerial facilities. Thus, any access alternative that minimizes the cost of labor will garner significant attention.

LMDS relies on a cellular-like deployment strategy under which the cells are approximately three miles in diameter. Unlike cellular service, however, users are stationary. Consequently, LMDS cells do not need to support roaming. Antenna/transceiver units are generally placed on rooftops, as they need unobstructed line-of-sight to operate properly. In fact, this is one of the disadvantages of LMDS (and a number of other wireless technologies): besides suffering from unexpected physical obstructions, the service suffers from "rain fade" caused by the absorption and scattering of the transmitted microwave signal by atmospheric moisture. Even some forms of foliage will cause interference for LMDS, so the transmission and reception equipment must be mounted high enough to avoid such obstacles, hence the tendency to mount the equipment on rooftops.

Because of its high-bandwidth capability, many LMDS implementations interface directly with an ATM backbone to take advantage of both its bandwidth and its diverse QoS capability. If ATM is indeed the transport fabric of choice, then the LMDS service becomes a broadband access alternative to a network capable of transporting a full range of services including voice, video, image, and data—the full suite of multimedia applications.

Multichannel, Multipoint Distribution System (MMDS)

MMDS got its start as a wireless cable television solution. In 1963, a spectrum allocation known as the *Instructional Television Fixed Service* (ITFS) was carried out by the FCC as a way to distribute educational content to schools and universities. In the 1970s, the FCC established a two-channel metropolitan distribution service called the *Multipoint*

Distribution Service (MDS). It was to be used for the delivery of pay-TV signals, but with the advent of inexpensive satellite access and the ubiquitous deployment of cable systems, the need for MDS went away.

In 1983, the FCC rearranged the MDS and ITFS spectrum allocation, creating 20 ITFS education channels and 13 MDS channels. In order to qualify to use the ITFS channels, schools had to use a minimum of 20 hours of airtime, which meant that ITFS channels tended to be heavily, albeit randomly, utilized. As a result, MMDS providers that use all 33 MDS and ITFS channels must be able to dynamically map requests for service to available channels in a completely transparent fashion, which means that the bandwidth management system must be reasonably sophisticated.

Because MMDS is not a true cable system (in spite of the fact that it has its roots in television distribution), no franchise issues surround its use (of course, licensing requirements are necessary). However, the technology is also limited in terms of what it can do. Unlike LMDS, MMDS is designed as a one-way broadcast technology and therefore does not typically enable upstream communication. Many contend, however, that the bandwidth in MMDS is adequate to provision two-way systems, which would make it suitable for voice, Internet access, and other data-oriented services.

So What's the Market?

Service providers looking to sell LMDS and MMDS technologies into the marketplace should target small and medium-sized businesses that experience measurable peak data rates and that are looking to move into the packet-based transport arena. Typical applications for the technologies include LAN interconnections, Internet access, and cellular backhauls between MTSOs and newly deployed cell sites. LMDS tends to offer higher data rates than MMDS. LMDS peaks out at a whopping 1.5 Gbps, while MMDS can achieve a maximum transmission speed of about 3 Mbps. Nevertheless, both have their place in the technology pantheon.

Satellite Technology

In October 1945, Arthur C. Clarke published a paper in *Wireless World* entitled, "Extra-Terrestrial-Relays: Can Rocket Stations Give World-Wide Radio Coverage?" In his paper, Clarke proposed the concept of an orbiting platform that would serve as a relay facility for radio signals

sent to it that could be turned around and retransmitted back to Earth with far greater coverage than was achievable through terrestrial transmission techniques. His platform would orbit at an altitude of 42,000 kilometers (25,200 miles) above the equator where it would orbit at a speed identical to the rotation speed of the Earth. As a consequence, the satellite would appear to be stationary to Earth-bound users.

Satellite technology may prove to be the primary communications gateway for regions of the world that do not yet have a terrestrial wired infrastructure, particularly given the fact that they are now capable of delivering broadband services. In addition to the United States, the largest markets for satellite coverage are Latin America and Asia, particularly Brazil and China.

Geosynchronous Satellites

Clarke's concept of a stationary platform in space forms the basis for today's geostationary or geosynchronous satellites. Ringing the equator like a string of pearls, these devices provide a variety of services including 64-Kbps voice, broadcast television, video-on-demand services, broadcast and interactive data, and point-of-sale applications, to name a few. Although satellites are viewed as technological marvels, the real magic lies more with what it takes to harden them for the environment in which they must operate and what it takes to get them there than it does their actual operational responsibilities. Satellites are, in effect, nothing more than a sophisticated collection of assignable, on-demand repeaters—in a sense, the world's longest local loop.

From a broadcast perspective, satellite technology has a number of advantages. First, its one-to-many capabilities are unequaled. Information from a central point can be transmitted to a satellite in geostationary orbit; the satellite can then rebroadcast the signal back to Earth, covering an enormous service footprint.

Because the satellites appear to be stationary, the Earth stations actually *can* be. One of the most common implementations of geosynchronous technology is seen in the *Very Small Aperture Terminal* (VSAT) dishes that have sprung up like mushrooms on a summer lawn. These dishes are used to provide both broadcast and interactive applications. The small DBS dishes used to receive TV signals are examples of broadcast applications, while the dishes seen on the roofs of large retail establishments, automobile dealerships, and convenience stores are typically used for interactive applications, such as credit card veri-

fication, inventory queries, e-mail, and other corporate communications. Some of these applications use a satellite downlink, but rely on a telco return for the upstream traffic; that is, they must make a telephone call over a land line to offer two-way service.

One disadvantage of geosynchronous satellites has to do with their orbital altitude. On the one hand, because they are so high, their service footprint is extremely large. On the other hand, because of the distance from the Earth to the satellite, the typical transit time for the signal to propagate from the ground to the satellite (or back) is about half a second, which is a significant propagation delay for many services. Should an error occur in the transmission stream during transmission, the need to detect the error, ask for a retransmission, and wait for the second copy to arrive could be catastrophic for delay-sensitive services like voice and video. Consequently, many of these systems rely on forward-error-correction transmission techniques that enable the receiver to not only detect the error, but correct it as well.

An interesting observation is that because the satellites orbit above the equator, dishes in the Northern Hemisphere always face south. The farther north a user's receiver dish is located, the lower it has to be oriented. Where I live in Vermont, the satellite dishes are practically lying on the ground; they almost look as of they are receiving signals from the depths of the mountains instead of a satellite orbiting 23,000 miles above the Earth.

Low/Medium Earth Orbit (LEO/MEO) Satellites

In addition to the geosynchronous satellite arrays, a variety of lower orbit constellations are deployed, known as *Low* and *Medium Earth Orbit* (LEO/MEO) satellites. Unlike the geosynchronous satellites, these orbit at lower altitudes, 400 to 600 miles, far lower than the 23,000-mile altitude of the typical GEO bird. As a result of their lower altitude, the transit delay between an Earth station and a LEO satellite is virtually nonexistent.

However, another problem exists with LEO technology. Because the satellites orbit pole to pole, they do not appear to be stationary, which means that if they are to provide uninterrupted service they must be able to hand off a transmission from one satellite to another before the first bird disappears below the horizon. This has resulted in the development of sophisticated satellite-based technology that emulates the

functionality of a cellular telephone network. The difference is that in this case, the user does not appear to move; the cell does.

Iridium

Perhaps the best-known example of LEO technology is Motorola's ill-fated Iridium deployment. Comprising 66 satellites[3] in a polar array, Iridium was designed to provide voice service to any user, anywhere on the face of the Earth. The satellites would provide global coverage and would hand off calls from one to another as the need arose.

Unfortunately, Iridium's marketing strategy was flawed; their prices were high, their phones large and cumbersome (one newspaper article referred to them as "manly phones"), and their market significantly overestimated. Additionally, their system was only capable of supporting 64-Kbps voice services, a puny bandwidth allocation in these days of customers with broadband desires. In the last year, the company failed but was pulled from the ashes. In June of 2001, the company announced a resumption of service, but many still question the technology's viability. Iridium offers a maximum bandwidth level of 10 Kbps for $1.50 per minute. With the right kind of coaxing, most traditional, terrestrial providers (AT&T, Sprint, or Worldcom) offer comparable prices but significantly higher bandwidth.

Iridium is not alone. ICO Global Communications, another satellite-based global communications company, filed for bankruptcy in August of 1999. In November of that same year, Craig McCaw, Teledesic, and Eagle River offered salvation for the company with an investment package valued at as much as $1.2 billion.

Globalstar

Others have been successful, however. Globalstar's 48-satellite array offers voice, short messaging, roaming, global positioning, fax, and data transport up to 9600 bps. Although the data rates are miniscule by comparison to other services, the converged collection of services they

[3] The system was named Iridium because in the original design the system was to require 77 satellites, and 77 is the atomic number of that element. Shortly after naming it Iridium, however, the technologists in the company determined that they would only need 66 birds. They did not rename the system Dysprosium.

provide is attractive to customers who want to reduce the number of devices they must carry with them in order to stay connected.

ORBCOMM

ORBCOMM is a partnership jointly owned by Orbital Sciences Corporation and Teleglobe Canada. Their satellites are nothing more than extraterrestrial routers that interconnect vehicles and Earth stations to facilitate deployment of such packet-based applications as two-way short messaging, e-mail, and vehicle tracking. Their constellation has a total of 35 satellites.

Teledesic

After Iridium, the best-known LEO satellite services company is Teledesic. Started in 1990 by Craig McCaw and Bill Gates, Teledesic will comprise an array of 288 satellites capable of providing up to 64 Mbps downstream and 2 Mbps upstream for voice, videoconferencing, and data, with plans in place to offer symmetric 64-Mbps service sometime in the future. In 1998, Motorola joined the Teledesic team, and in 1999 the company signed a launch agreement with Lockheed Martin. They plan to be fully operational by 2005.

Sky Station International

No discussion of wireless technology would be complete without a mention of Sky Station International. Founded by Alexander Haig (still in charge) and satellite visionary Martine Rothblatt, the company takes a completely different approach to wireless connectivity. Instead of fixed towers or satellites, Skystation uses—get ready—helium balloons. Capable of transporting a 1,000-Kg payload, the balloons are huge, over 500 feet long and 300 feet in diameter, and have an expected lifespan of about 10 years.

As wacky as the technology sounds, it has merit. First, the balloons require no launch vehicle. They are flown into position by remote control. Second, they will initially offer as much as 2 Mbps of bandwidth for pennies per minute with greater bandwidth planned in the not-too-distant future. They will float at an altitude of 21 miles, far lower than the lowest

satellites and therefore offering virtually instantaneous responses. Two hundred and fifty such platforms are planned, with the first balloons launching in 2002. Finally, the system is designed to interconnect to the broadband terrestrial network, thereby offering an end-to-end transport scheme.

This is a company to pay attention to. The technology is not new; the military has used *High-Altitude, Long-Endurance* (HALE) technology for years. High-flying aircraft simply orbit at reduced power for many hours, providing message relay services to a very large footprint. When the orbiting aircraft runs low on fuel, another plane flies into orbit to take the first plane's place. A handoff occurs and connectivity is seamless. What *is* new, however, is the application; this is a commercial offering.

As a service-provisioning technology, satellites may seem so far out (no pun intended) that they may not appear to pose a threat to more traditional telecommunications solutions. At one time, that is, before the advent of LEO technology, this was largely true. Geosynchronous satellites were extremely expensive, offered low bit rates, and suffered from serious latency that was unacceptable for many applications.

Today this is no longer true. Today GEO satellites offer high-quality, two-way transmission for certain applications. LEO technology has advanced to the point that it now offers low-latency, two-way communications at broadband speeds, is relatively inexpensive, and, as a consequence, poses a clear threat to terrestrial services.

On the other hand, the best way to eliminate an enemy is to make the enemy a friend. Many traditional service providers have entered into alliances with satellite providers. Consider the agreements that exist between DirecTV, a high-quality, wireless alternative to cable, and Bell Atlantic, GTE, Cincinnati Bell, and SBC corporations. By joining forces with satellite providers, service providers create a market block that will help them stave off the short-term incursion of cable. Between the minimal infrastructure required to receive satellite signals and the soon-to-be ubiquitous deployment of DSL over twisted pair, incumbent local telephone companies and their alliance partners are in a reasonably good position to counter the efforts of cable providers wanting to enter the local services marketplace. In the long term, however, wireless will win the access game.

Other Wireless Access Solutions

A number of other wireless technologies have emerged in the last few years that are worth mentioning, including 802.11, Bluetooth, and the *Wireless Application Protocol* (WAP).

802.11

IEEE 802.11, discussed earlier, is a wireless LAN standard developed by the *Institute of Electrical and Electronic Engineering's* (IEEE's) 802 committee to specify an air interface between a wireless client and a base station, as well as among a variety of wireless clients. First discussed in 1990, the standard has evolved through six draft versions and won final approval on June 26, 1997.

Bluetooth

Bluetooth has been referred to as the *personal area network* (PAN). It is a wireless LAN on a chip that operates in the unlicensed 2.4-GHz band at 768 Kbps, relatively slow compared to 802.11's 11 Mbps. It does, however, include a 56-Kbps backward channel and three voice channels, and it can operate at distances of up to 100 feet (although most pundits claim 25 feet for effective operation). According to a report from Allied Business Intelligence, the Bluetooth devices' market will reach $2 billion by 2005, a non-trivial number.

The service model that Bluetooth supporters propose is one built around the concept of the mobile appliance. Consider the following scenario. As you walk around your house with your Palm Pilot or Pocket PC, the device is in constant communication with Bluetooth-equipped devices throughout the house. As you pass by the refrigerator on the way through the kitchen, the fridge transmits a message to your device telling it that the milk is low and should be added to the shopping list. It knows this because infrared sensors inside the refrigerator have detected that the level of milk in the container is below a certain predetermined level. The mobile appliance adds milk to the shopping list in the mobile device. The next time you are out and pass the grocery store,

the mobile appliance receives a transmission from the store, wakes up, and notifies you to stop and buy the items on the list.

Good application? Maybe. Bluetooth, named for a tenth-century Danish king (no, I don't know whether he had a blue tooth), is experiencing growing pains and significant competition for many good reasons from 802.11. Whether Bluetooth succeeds or not is a matter still open for discussion. It's far too early to tell.

Wireless Application Protocol (WAP)

Originally developed by Phone.com, WAP has proven to be a disappointment for the most part. Because it is designed to work with 3G wireless systems, and because 3G systems have not yet materialized, some have taken to defining WAP to mean "wrong approach to portability." Germany's D2 network reports that the average WAP customer uses it less than two minutes per day, which is tough to make money on when service is billed on a usage basis. 3G will be the deciding factor; when it succeeds, WAP will succeed, unless 802.11's success continues to expand.

The Mobile Appliance

The mobile appliance concept is enjoying a significant amount of attention of late because it promises to herald in a whole new way of using network and computer resources, *if it works as promised.* The problem with so many of these new technologies is that they overpromise and underdeliver, precisely the opposite of what they're supposed to do for a successful rollout.

3G, for example, has been billed as "the wireless Internet." Largely as a result of that billing, it has failed. It is *not* the Internet, far from it. The bandwidth isn't there, nor does it offer a device that can even begin to offer the kind of image quality that Internet users have become accustomed to. Furthermore, the number of screens that a user must go through to reach a desired site (I have heard estimates as high as 22) is far too high. Therefore, until the user interface, content, and bandwidth challenges are met and satisfied, the technology will remain exactly that—a technology. No application exists yet, and *that's* what people are willing to pay money for.

Summary

Access technologies, used to connect the customer to the network, come in a variety of forms and offer a broad variety of connectivity options and bandwidth levels. The key to success is to *not* be a bottleneck. Access technologies that can evolve to meet the growing customer demands for bandwidth will be the winners in the game. DSL holds an advantage as long as it can overcome the availability challenge and the technology challenge of loop carrier restrictions. Wireless is hobbled by licensing and spectrum availability, both of which are regulatory and legal in nature, rather than technology limitations.

In Chapter 6, "Transport Technologies," we will discuss transport technologies, including private line, Frame Relay, ATM, and optical networking.

CHAPTER 6

Transport Technologies

We have now discussed the premises' environment and access technologies. The next area we'll examine is *transport*.

Because businesses are rarely housed in a single building, and because their customers are typically scattered across a broad geographical area (particularly multinational customers), a growing need exists for high-speed, reliable wide-area transport. "Wide-area" can take on a variety of meanings. For example, a company with multiple offices scattered across the metropolitan expanse of a large city requires interoffice connectivity in order to do business properly. On the other hand, a large multinational with offices and clients in Madrid, San Francisco, Hamburg, and Singapore requires connectivity to ensure that the offices can exchange information on a 24-hour basis.

These requirements are satisfied through the proper deployment of wide-area transport technologies. These can be as simple as a dedicated private line circuit or as complex as a virtual installation that relies on *Asynchronous Transfer Mode* (ATM) for high-quality transport.

Dedicated facilities are excellent solutions because they are dedicated. They provide fixed bandwidth that never varies and they guarantee the quality of the transmission service. Because they are dedicated, however, they suffer from two disadvantages. First, they are expensive and only cost-effective when highly utilized. The pricing model for dedicated circuits includes two components: the mileage of the circuit and the bandwidth. The longer the circuit, and the faster it is, the more it costs. Second, because they are not switched and are often not redundant because of cost, dedicated facilities pose the potential threat of a prolonged service outage should they fail. Nevertheless, dedicated circuits are popular for certain applications and are widely deployed. They include such solutions as T-1, which offers 1.544 Mbps of bandwidth; DS-3, which offers 44.736 Mbps of bandwidth; and the *Synchronous Optical Network* (SONET), which offers a wide range of bandwidth from 51.84 Mbps to as much as 40 Gbps.

The alternative to a dedicated facility is a switched service, such as Frame Relay or ATM. These technologies provide virtual circuits. Instead of dedicating physical facilities, they dedicate logical timeslots to each customer who then shares access to physical network resources. In the case of Frame Relay, the service can provide bandwidth as high as DS-3, thus providing an ideal replacement technology for lower-speed dedicated circuits. ATM, on the other hand, operates hand-in-glove with SONET and is thus capable of providing transport services at gigabit speeds. Finally, the new field of optical networking is carving out a large niche for itself as a bandwidth-rich solution with the potential for inherent *quality of service* (QoS).

We begin our discussion with dedicated private line, otherwise known as point-to-point.

Point-to-Point Technologies

Point-to-point technologies do exactly what their name implies: they connect one point directly with another. For example, it is common for two buildings in a downtown area to be connected by a point-to-point microwave or infrared circuit, because the cost of establishing it is far lower than the cost to put in physical facilities in a crowded city. Many businesses rely on dedicated, point-to-point optical facilities to interconnect locations, especially businesses that require dedicated bandwidth for high-speed applications. Of course, point-to-point does not necessarily imply high-bandwidth; many locations use 1.544-Mbps T-1 facilities for interconnection, and some rely on lower-speed circuits where higher bandwidth is not required.

Dedicated facilities provide bandwidth from as low as 2,400 bps to as high as multiple gigabits per second. 2,400-bps analog facilities are not commonly seen but are often used for alarm circuits and telemetry, whereas circuits operating at 4,800 and 9,600 bps are used to access interactive, host-based data applications.

Higher-speed facilities are usually digital and are often channelized by dedicated multiplexers and shared among a collection of users or by a variety of applications. For example, a high-bandwidth facility that interconnects two corporate locations might be dynamically subdivided into various-sized channels for use by a *Private Branch Exchange* (PBX) for voice, a videoconferencing system, and data traffic.

Dedicated facilities have the advantage of always being available to the subscriber. However, they also have the *disadvantage* of being there and accumulating charges whether they are being used or not. For the longest time, dedicated circuits represented the only solution that provided guaranteed bandwidth; switched solutions simply weren't designed for the heavy service requirements of graphical and data-intensive traffic. Over time, however, that has changed. A number of switched solutions have emerged in the last few years that provide guaranteed bandwidth and only accumulate charges when they are being used (although some of them offer very reasonable fixed-rate service). The two most common of these are Frame Relay and ATM; we begin with Frame Relay.

Before we do, however, let's spend a few minutes discussing the hierarchy of switching. Part of this is a review of prior material. Most of it, though, is preparation for our discussion of Frame Relay and ATM, the so-called "fast-packet" switching technologies.

The Switching Hierarchy

The switching hierarchy, shown in Figure 6-1, has two major subheadings: circuit switching and store-and-forward switching. Circuit switching is something of an evolutionary dead end in that it will not become something else. The only evolution for circuit switching is an evolution toward packet switching at this point.

Packet switching evolved as one of the two descendents of store-and-forward technology. Message switching, the alternative and another evolutionary dead end, is inefficient and not suited to the bursty nature of most data services today. Packet switching continues to hold sway and, because of its many forms, is a valid solution for most data applications.

Packet switching has three major forms, two of which were discussed in earlier chapters. Connection-oriented packet switching manifests itself as a virtual circuit service that offers the appearance and behavior of a dedicated circuit when, in fact, it is a switched service. It creates a path through the network that all packets from the same source (and going to the same destination) follow, the result of which is constant transmission latency for all packets in the flow. Both

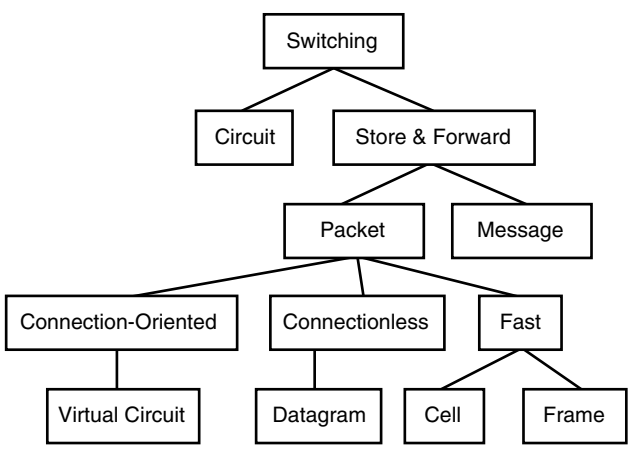


Figure 6-1
The switching hierarchy.

Frame Relay and ATM, discussed later in this chapter, are virtual circuit technologies.

Connectionless packet switching does not establish a virtual dedicated path through the network; instead, it hands the packets to the ingress switch and enables the switch to determine the optimum routing on a packet-by-packet basis. This is extremely efficient from a network point of view, but is less favorable for the client in that every packet is treated slightly differently, the result of which can be unpredictable delays and out-of-order delivery.

The third form of packet switching is called *fast packet,* two forms of which are Frame Relay and ATM. The technique is called fast packet because the processing efficiency is far better than traditional packet switching because of reduced overhead.

Fast-packet technologies are characterized by low error rates, significantly lower processing overhead, high transport speed, minimal delay, and relatively low cost. The switches accomplish this by making several assumptions about the network. First, they assume (correctly) that the network is digital and based largely on a fiber infrastructure, the result of which is an inordinately low error rate. Second, they assume that, unlike their predecessors, the end-user devices are intelligent and therefore have the capability to detect and correct errors on an end-to-end basis (at a higher protocol layer), rather than stopping every packet at every node to check it for errors and correct them. These switches still check for errors, but if they find errored packets, they simply discard them, knowing that the end devices will realize that a problem exists and take corrective measures on an end-to-end basis. Think back to Chapter 2, "Protocols," for a moment: this is the difference between layer two error-detection and layer four error-detection.

Frame Relay

Frame Relay came about as a private-line replacement technology and was originally intended as a data-only service. Today it carries not only data, but voice and video as well, and although it was originally crafted with a top speed of T-1 E-1, it now provides connectivity at much higher bandwidth levels.

In Frame Relay networks, the incoming data stream is packaged as a series of variable-length frames that can transport any kind of data: *local area network* (LAN) traffic, *Internet Protocol* (IP) packets, *Systems*

Network Architecture (SNA) frames, and even voice and video. In fact, it has been recognized as a highly effective transport mechanism for voice, enabling Frame Relay-capable PBXs to be connected to a Frame Relay *permanent virtual circuit* (PVC), which can cost-effectively replace private-line circuits used for the same purpose. When voice is carried over Frame Relay, it is usually compressed for transport efficiency and packaged in small frames to minimize the processing delay of the frames. According to the Frame Relay Forum, as many as 255 voice channels can be encoded over a single PVC, although the number is usually smaller when actually implemented.

Frame Relay is a virtual circuit service. When customers want to connect two locations using Frame Relay, they contact their service provider and tell the service representative where the endpoints are located and the bandwidth they require. The service provider issues a service order to create the circuit. If, at some point in the future, the customer decides to change the circuit endpoints or upgrade the bandwidth, another service order must be issued, which would be PVC and is the most commonly deployed Frame Relay solution.

Frame Relay is also capable of supporting *Switched Virtual Circuit* (SVC) service, but SVCs are for the most part not available from service providers. With SVC service, customers can make their own modifications to the circuit by accessing the Frame Relay switch in the *central office* (CO) and requesting changes. However, service providers do not currently offer SVC service because of billing and tracking concerns (customer activities are difficult to monitor). Instead, they enable customers to create a fully meshed network between all locations for a very reasonable price. Instead of making routing changes in the switch, the customer has a circuit between every possible combination of desired endpoints. As a result, customers get the functionality of a switched network, while the service provider avoids the difficulty of administering a network within which the customer is actively making changes.

In Frame Relay, PVCs are identified using an address called a *Data Link Connection Identifier* (DLCI, pronounced "delsie"). At any given endpoint, the customer's router can support multiple DLCIs, and each DLCI can be assigned varying bandwidths based upon the requirements of the device/application on the router port associated with that DLCI.

In Figure 6-2, the customer has purchased a T-1 circuit to connect his or her router to the Frame Relay network. The router is connected to a videoconferencing unit at 384 Kbps, a Frame Relay-capable PBX at 768 Kbps, and a data circuit for Internet access at 512 Kbps.

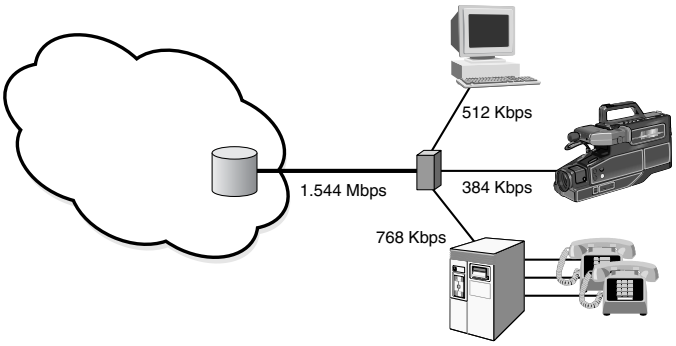


Figure 6-2
Frame relay service delivery.

Note that the aggregate bandwidth assigned to these devices exceeds the actual bandwidth of the access line by 128 Kbps (1664–1536). Under normal circumstances, this would not be possible, but Frame Relay assumes that the traffic it will normally be transporting is bursty by nature. If the assumption is correct (and it usually is), it is not likely that all three devices will burst at the same instant in time.

As a consequence, the circuit's operating capacity can actually be overbooked, a process known as *oversubscription*. Most service providers allow as much as 200 percent oversubscription, something customers clearly benefit from, provided the circuit is designed properly. This means that the salesperson must carefully assess the nature of the traffic that the customer will be sending over the link and ensure that enough bandwidth is allocated to support the requirements of the various devices that will be sharing access to the link. Failure to do so can result in an underengineered facility that will not meet the customer's throughput requirements. This is a critical component of the service delivery formula.

The throughput level, that is, the bandwidth that Frame Relay service providers absolutely guarantee on a PVC-by-PVC basis, is called the *Committed Information Rate* (CIR). In addition to CIR, service providers will often support an *Excess Information Rate* (EIR), which is the rate above the CIR that they will attempt to carry, assuming the capacity is available within the network. However, all frames above the CIR are marked as eligible for discard, which simply means that the network will do its best to deliver them but makes no guarantees. If push comes to shove, and the network finds itself to be congested, the frames marked *discard eligible* (DE) are immediately discarded at their point of ingress.

This CIR/EIR relationship is poorly understood by many customers because the CIR is taken to be an indicator of the absolute bandwidth of the circuit. Although bandwidth is typically measured in bits per second, CIR is a measure of *bits in one second*. In other words, the CIR is a measure of the average throughput that the network will guarantee. The actual transmission volume of a given CIR may be higher or lower than the CIR at any point in time because of the bursty nature of the data being sent, but in aggregate the network will maintain an average, guaranteed flow volume for each PVC.

This is a selling point for Frame Relay. In most cases, customers get more than they actually pay for, and as long as the switch loading levels are properly engineered, the switch (and therefore the Frame Relay service offering) will not suffer adversely from this charitable bandwidth allocation philosophy. The key to success when selling Frame Relay is to have a clear understanding of the applications the customer intends to use across the link so that the access facility can be properly sized for the anticipated traffic load.

Managing Service in Frame Relay Networks

Frame Relay does not offer a great deal of granularity when it comes to QoS. The only inherent mechanism is the DE bit described earlier as a way to control network congestion. However, the DE bit is binary. It has two possible values, which means that a customer has two choices: the information being sent is either important or it isn't—not particularly useful for establishing a variety of QoS levels.

Consequently, a number of vendors have implemented proprietary solutions for QoS management. Within their routers (sometimes called *Frame Relay Access Devices* [FRADs]) they have established queuing mechanisms that enable customers to create multiple priority levels for differing traffic flows. For example, voice and video, which don't tolerate delay well, could be assigned to a higher-priority queue than the one to which asynchronous data traffic would be assigned. This enables Frame Relay to provide highly granular service. The downside is that this approach is proprietary, which means that the same vendor's equipment must be used on both ends of the circuit. Given the strong move toward interoperability, this is not an ideal solution because it locks the customer into a single-vendor situation.

Congestion Control in Frame Relay

Frame Relay has two congestion control mechanisms. Embedded in the header of each Frame Relay frame are two additional bits called the *Forward Explicit Congestion Notification bit* (FECN) and the *Backward Explicit Congestion Notification bit* (BECN). Both are used to notify devices in the network of congestion situations that could affect throughput.

Consider the following scenario. A Frame Relay frame arrives at the second of three switches along the path to its intended destination, where it encounters severe local congestion (see Figure 6-3). The congested switch sets the FECN bit to indicate the presence of congestion and transmits the frame to the next switch in the chain. When the frame arrives, the receiving switch takes note of the FECN bit, which tells the switch the following: "I just came from that switch back there, and it's extremely congested. You can transmit stuff back there if you want to, but there's a good chance that anything you send will be discarded, so you might want to wait awhile before transmitting." In other words, the switch has been notified of a congestion condition, to which it may respond by throttling back its output to enable the affected switch time to recover.

On the other hand, the BECN bit is used to flow-control a device that is sending too much information into the network. Consider the situation shown in Figure 6-4, where a particular device on the network is transmitting at a high volume level, routinely violating the CIR and perhaps the EIR level established by mutual consent. The ingress switch—that is, the first switch the traffic touches—has the capability to set the BECN bit on frames going toward the offending device, which carries the

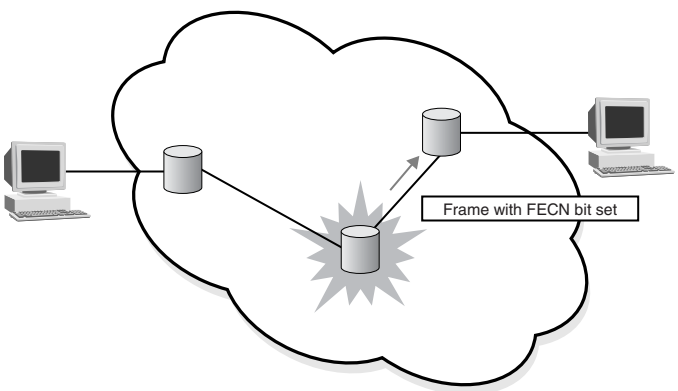


Figure 6-3
A frame encounters congestion in transit.

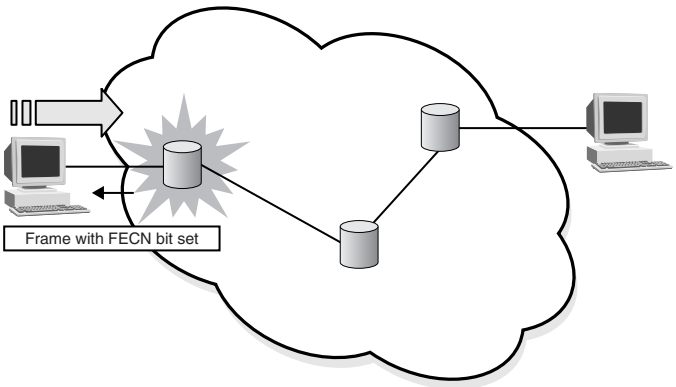


Figure 6-4 BECN bit used to warn a station that is transmitting too much data (in violation of its agreement with the switch).

implicit message, "cut it out or I'm going to hurt you." In effect, the BECN bit notifies the offending device that it is violating protocol, and continuing to do so will result in every frame from that device being discarded without warning or notification. If this happens, it gives the ingress switch the opportunity to recover. However, it doesn't fix the problem; it merely forestalls the inevitable, because sooner or later the intended recipient will realize that frames are missing and will initiate recovery procedures, which will cause resends to occur. However, it may give the affected devices time to recover before the onslaught begins anew.

The problem with FECN and BECN lies in the fact that many devices choose not to implement them. They do not necessarily have the inherent capability to throttle back upon receipt of a congestion indicator, although devices that can are becoming more common. Nevertheless, proprietary solutions are in widespread use and will continue to be for some time to come.

Frame Relay Summary

Frame Relay is clearly a Cinderella technology, evolving quickly from a data-only transport scheme to a multiservice technology with diverse capabilities. For data and some voice and video applications, it shines as a *wide area network* (WAN) offering. In some areas, however, Frame Relay is lacking. Its bandwidth is limited to DS-3, and its ability to offer standards-based QoS is limited. Given the focus on QoS that is so much a part of customers' chanted mantra today, and the flexibility that a switched solution permits, something else is required. That something is ATM.

Asynchronous Transfer Mode (ATM)

Network architectures often develop in concert with the corporate structures that they serve. Companies with centralized management authorities such as utilities, banks, and hospitals often have centralized and tightly controlled hierarchical data-processing architectures to protect their data. On the other hand, organizations that are distributed in nature such as research and development facilities and universities often have highly distributed data processing architectures. They tend to share information on a peer-to-peer basis and their corporate structures reflect the fact.

ATM came about not only because of the proliferation of diverse network architectures, but also because of the evolution of traffic characteristics and transport requirements. To the well-known demands of voice, we now add various flavors of data, video, MP3, an exponentially large variety of IP traffic, interactive real-time gaming, and a variety of other content types that place increasing demands on the network. Further, we have seen a requirement arise for a mechanism that can transparently and correctly transport the mix of various traffic types over a single network infrastructure while at the same time delivering granular, controllable, and measurable QoS levels for each service type. In its original form, ATM was designed to do exactly that, working with SONET or the *Synchronous Digital Hierarchy* (SDH) to deliver high-speed transport and switching throughout the network in the wide area, the metropolitan area, the campus environment, and the LAN, right down to the desktop, seamlessly, accurately, and fast.

Today, because of competition from such technologies as QoS-aware IP transport, proprietary high-speed mesh networks, and Fast and Gigabit Ethernet, ATM has for the most part lost the race to the desktop. ATM is a cell-based technology, which simply means that the fundamental unit of transport—a frame of data, if you will—is of a fixed size, which enables switch designers to build faster, simpler devices, because they can always count on their switched payload being the same size at all times. That cell comprises a 5-octet header and a 48-octet payload field, as shown in Figure 6-5. The payload contains user data and the header contains information that the network requires to both transport the payload correctly and ensure proper quality of service levels for the payload.

ATM accomplishes this task well, but at a cost. The 5-octet header comprises nearly 10 percent of the cell, a rather significant price to pay,

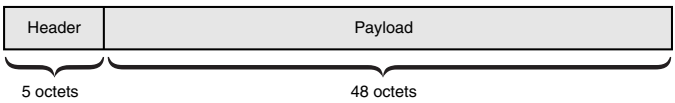


Figure 6-5
The ATM cell.

particularly when other technologies such as IP and SONET add their own significant percentages of overhead to the overall payload. This reality is part of the problem. ATM's original claims to fame, and the reasons it rocketed to the top of the technology hit parade, were its capability to switch cells at tremendous speeds through the fabric of the WAN and the ease with which the technology could be scaled to fit any network situation. Today, however, given the availability of high-speed IP routers that routinely route packets at terabit rates, ATM's advantages have begun to pale to a certain degree.

ATM Evolution

ATM has, however, emerged from the flames in other ways. Today many service providers see ATM as an ideal aggregation technology for diverse traffic streams that need to be combined for transport across a WAN that will most likely be IP-based. ATM devices then will be placed at the edge of the network, where they will collect traffic for transport across the Internet or (more likely) a privately owned IP network. Furthermore, because it has the capability to be something of a chameleon by delivering diverse services across a common network fabric, it is further guaranteed a seat at the technology game.

It is interesting to note that the traditional, legacy telecommunications network comprises two principal regions that can be clearly distinguished from each other: the network itself, which provides switching, signaling, and transport for traffic generated by customer applications; and the access loop, which provides the connectivity between the customer's applications and the network. In this model, the network is considered to be a relatively intelligent medium, whereas the customer equipment is usually considered to be relatively "stupid."

Not only is the intelligence seen as being concentrated within the confines of the network, so too is the bulk of the bandwidth because the legacy model indicates that traditional customer applications don't require much of it. Between CO switches, however, and between the offices themselves, enormous bandwidth is required.

Today this model is changing. Customer equipment has become remarkably intelligent, and many of the functions previously done within the network cloud are now performed at the edge. PBXs, computers, and other devices are now capable of making discriminatory decisions about required service levels, eliminating any need for the massive intelligence embedded in the core.

At the same time, the bandwidth is migrating from the core of the network toward the customer as applications evolve to require it. Massive bandwidth still exists within the cloud, but the margins of the cloud are expanding toward the customer.

The result of this evolution is a redefinition of the network's regions. Instead of a low-speed, low-intelligence access area and a high-speed, highly intelligent core, the intelligence has migrated outward to the margins of the network and the bandwidth, once exclusively a core resource, is now equally distributed at the edge. Thus, we see something of a core and edge distinction evolving as customer requirements change.

One reason for this steady migration is the well-known fact within sales and marketing circles that products sell best when they are located close to the buying customer. They are also easier to customize for individual customers when they are physically closest to the situation for which the customer is buying them.

In "The Rise of the Stupid Network," David Isenberg makes the following observation:

> The Intelligent Network is a straight-line extension of four assumptions—scarcity, voice, circuit switching, and control. Its primary design impetus was not customer service. Rather, the Intelligent Network was a telephone company attempt to engineer vendor independence, more automatic operation, and some "intelligent" new services into existing network architecture. However, even as it rolls out and matures, the Intelligent Network is being superseded by a Stupid Network, with nothing but dumb transport in the middle, and intelligent user-controlled endpoints, whose design is guided by plenty, not scarcity, where transport is guided by the needs of the data, not the design assumptions of the network.

Isenberg continues:

> A new network "philosophy and architecture" is replacing the vision of an Intelligent Network. The vision is one in which the public communications network would be engineered for "always-on" use, not intermittence and scarcity. It would be engineered for intelligence at the end-user's device, not in the network. And the network would be engineered simply to "Deliver the Bits, Stupid," not for fancy network routing or "smart" number translation.

ATM Technology Overview

Because ATM plays such a major role in networks today, it is important to develop at least a rudimentary understanding of its functions, architectures, and offered services.

ATM Protocols

Like all modern technologies, ATM has a well-developed protocol stack, shown in Figure 6-6, which clearly delineates the functional breakdown of the service. The stack consists of four layers: the Upper Services layer, the *ATM Adaptation layer* (AAL), the ATM layer, and the Physical layer.

The Upper Services layer defines the nature of the actual services that ATM can provide. It identifies both constant and *variable bit rate* (VBR) services. Voice is an example of a constant bit rate service, while signaling, IP, and Frame Relay are examples of both connectionless and connection-oriented VBR services.

The AAL has four general responsibilities:

- Synchronization and recovery from errors
- Error-detection and correction
- Segmentation and reassembly of the data stream
- Multiplexing

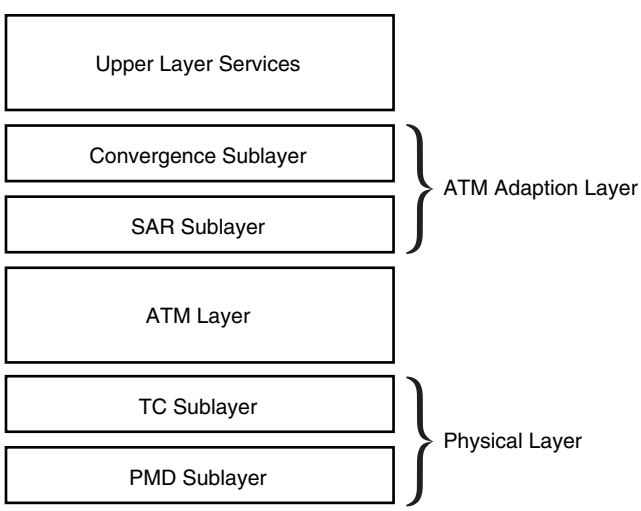


Figure 6-6 ATM protocol stack.

The AAL comprises two functional sublayers. The *Convergence sublayer* provides service-specific functions to the Services layer so that it can make the most efficient use of the underlying cell relay technology that ATM provides. The Convergence sublayer's functions include clock recovery for end-to-end timing management, a recovery mechanism for lost or out-of-order cells, and a timestamp capability for time-sensitive traffic such as voice and video.

The *Segmentation and Reassembly sublayer* (SAR) converts the user's data from its original incoming form into the 48-octet payload chunks that will become cells. For example, if the user's data is arriving in the form of 64KB IP packets, SAR chops them into 48-octet payload pieces. It also has the responsibilities of detecting lost or out-of-order cells that the Convergence sublayer will recover from and detecting single bit errors in the payload chunks.

The ATM layer has five general responsibilities:

- Cell multiplexing and demultiplexing
- Virtual path and virtual channel switching
- Creation of the cell header
- Generic flow control
- Cell delineation

Because the ATM layer creates the cell header, it is responsible for all of the functions that the header manages. The process, then, is fairly straightforward: the user's data passes from the Services layer to the AAL, which segments the data stream into 48-octet pieces. The pieces are handed to the ATM layer, which creates the header and attaches it to the payload unit, thus creating a cell. The cells are then handed down to the Physical layer.

The Physical layer consists of two functional sublayers as well: the Transmission Convergence sublayer and the Physical Medium sublayer. The Transmission Convergence sublayer performs three primary functions. The first is called cell rate decoupling, which adapts the cell creation and transmission rate to the rate of the transmission facility by performing *cell stuffing*, similar to the bit-stuffing process described earlier in the discussion of DS-3 frame creation. The second responsibility is cell delineation, which enables the receiver to delineate between one cell and the next. Finally, it generates the transmission frame in which the cells are to be carried.

The Physical Medium sublayer takes care of issues that are specific to the medium being used for transmission, such as line codes, electrical and optical concerns, timing, and signaling.

The Physical layer can use a wide variety of transport options, including

- DS1/DS2/DS3
- E1/E3
- 25.6-Mbps *User-to-Network Interface* (UNI) over UTP-3
- 51-Mbps UNI over UTP-5 (*Transparent Asynchronous Transmitter/Receiver Interface* [TAXI])
- 100-Mbps UNI over UTP-5
- OC3/12/48c

Others, of course, will follow as transport technologies advance.

The ATM Cell Header

As mentioned before, ATM is a cell-based technology that relies on a 48-octet payload field that contains actual user data, and a five-byte header that contains information needed by the network to route the cell and provide proper levels of service.

The ATM cell header, shown in Figure 6-7, is examined and updated by each switch it passes through and comprises six distinct fields: the *Generic Flow Control* (GFC) field, the *Virtual Path Identifier* (VPI), the *Virtual Channel Identifier* (VCI), the *Payload Type Identifier* (PTI), the *Cell Loss Priority* (CLP) field, and the *Header Error Control* (HEC) field.

- **Generic Flow Control (GFC)** This 4-bit field is used across the UNI for network-to-user flow control. It has not yet been completely defined in the ATM standards, but some companies have chosen to use it for very specific purposes. For example, Australia's Telstra Corporation uses it for flow control in the network-to-user direction and as a traffic priority indicator in the user-to-network direction.
- **Virtual Path Identifier (VPI)** The 8-bit VPI identifies the virtual path over which the cells will be routed at the UNI. It should be noted that because of dedicated, internal flow control capabilities within the network, the GFC field is not needed across the *Network-to-Network Interface* (NNI). It is therefore redeployed; the 4 bits are converted to additional VPI bits, thus extending the size of the virtual path field. This enables the identification of more than 4,000 unique VPs. At the UNI, this number is excessive, but across the NNI, it is necessary because of the number of potential paths that

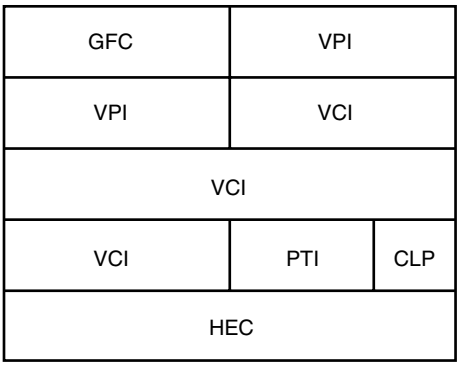


Figure 6-7 ATM cell header details.

might exist between the switches that make up the fabric of the network.

- **Virtual Channel Identifier (VCI)** As the name implies, the 16-bit VCI identifies the unidirectional virtual channel over which the current cells will be routed.
- **Payload Type Identifier (PTI)** The 3-bit PTI field is used to indicate network congestion and cell type, in addition to a number of other functions. The first bit indicates whether the cell is generated by the user or by the network, while the second indicates the presence or absence of congestion in user-generated cells or flow-related *Operations, Administration, and Maintenance* (OAM) information in cells generated by the network. The third bit is used for service-specific, higher-layer functions in the user-to-network direction, such as to indicate that a cell is the last in a *series* of cells. From the network to the user, the third bit is used with the second bit to indicate whether the OAM information refers to segment or the end-to-end related information flow.
- **Cell Loss Priority (CLP)** The single-bit CLP field is a relatively primitive flow control mechanism by which the user can indicate to the network which cells to discard in the event of a condition that demands that some cells be eliminated, similar to the DE bit in Frame Relay. It can also be set by the network to indicate to downstream switches that certain cells in the stream are eligible for discard, should that become necessary.
- **Header Error Control (HEC)** The 8-bit HEC field can be used for two purposes. First, it provides for the calculation of an 8-bit *Cyclic Redundancy Check* (CRC) that checks the integrity of the entire header. Second, it can be used for cell delineation.

Addressing in ATM

ATM is a connection-oriented, virtual circuit technology, meaning that communication paths are created through the network prior to actually sending traffic. Once established, the ATM cells are routed based upon a virtual circuit address. A virtual circuit is simply a connection that gives the user the appearance of being dedicated to that user, when in point of fact the only thing that is actually dedicated is a time slot. This technique is generically known as *label-based switching* and is accomplished through the use of routing tables in the ATM switches that designate input ports, output ports, input addresses, output addresses, and QoS parameters required for proper routing and service provisioning. As a result, cells do not contain explicit destination addresses, but rather contain timeslot identifiers.

Every virtual circuit address has two components, as shown in Figure 6-8. The first is the *virtual channel* (VC), which is a unidirectional conduit for the transmission of cells between two endpoints. For example, if two parties are conducting a videoconference, they will each have a VC for the transmission of outgoing cells that make up the video portion of the conference.

The second level of the ATM addressing scheme is called a *virtual path* (VP). A VP is a bundle of VCs that have the same endpoints, and that, when considered together, make up a bidirectional transport facility. The combination of unidirectional channels that we need in our two-way videoconferencing example makes up a VP.

ATM Services

The basic services that ATM provides are based on three general characteristics: the nature of the connection between the communicating stations (connection-oriented versus connectionless), the timing rela-

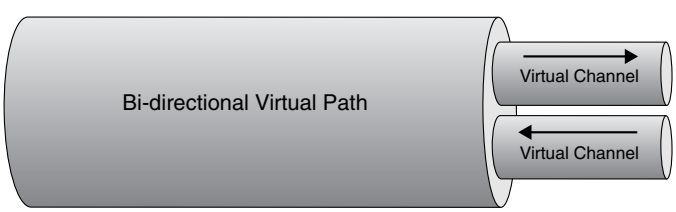


Figure 6-8 *Addressing in ATM with virtual channels, paths.*

tionship between the sender and the receiver, and the bit rate required to ensure proper levels of service quality. Based on those generic requirements, both the *International Telecommunication Union Standardization Sector* (ITU-T) and the ATM Forum have created service classes that address the varying requirements of the most common forms of transmitted data.

ITU-T Service Classes The ITU-T assigns service classes based on three characteristics: connection mode, bit rate, and the end-to-end timing relationship between the end stations. They have created four distinct service classes, based on the model shown in Figure 6-9. Class A service, for example, defines a connection-oriented, constant-bit-rate, timing-based service that is ideal for the stringent requirements of voice service. Class B, on the other hand, is ideal for such services as VBR video, in that it defines a connection-oriented, VBR, timing-based service.

Class C service is defined for such things as Frame Relay, in that it provides a connection-oriented, VBR, timing-independent service. Finally, Class D delivers a connectionless, VBR, timing-independent service that is ideal for IP traffic as well as *Switched Multimegabit Data Service* (SMDS).

In addition to service classes, the ITU-T has defined AAL service types, which align closely with the A, B, C, and D service types described previously. Whereas the service classes (A, B, C, D) describe the capabilities of the underlying network, the AAL types describe the cell format. They are AAL1, AAL2, AAL3/4, and AAL 5. However, only two of them have really "survived" in a big way.

AAL1 is defined for Class A service, which is a constant-bit-rate environment ideally suited for voice and voice-like applications. In AAL1

Figure 6-9 ITU-T ATM service definitions.

	Class A	Class B	Class C	Class D
AAL Type	1	2	5, 3/4	5, 3/4
Connection Mode	Connection-oriented	Connection-oriented	Connection-oriented	Connectionless
Bit Rate	Constant	Variable	Variable	Variable
Timing relationship	Required	Required	Not required	Not required
Service Types	Voice, video	VBR voice, video	Frame relay	IP

cells, the first octet of the payload serves as a payload header that contains cell sequence and synchronization information that is required to provision a constant-bit-rate, fully sequenced service. AAL1 provides circuit emulation service without dedicating a physical circuit, which explains the need for an end-to-end timing relationship between the transmitter and the receiver.

AAL5, on the other hand, is designed to provide both Class C and D services, and although it was originally proposed as a transport scheme for connection-oriented data services, it turns out to be more efficient than AAL3/4 and accommodates connectionless services quite well.

To guard against the possibility of errors, AAL5 has an 8-octet trailer appended to the user data that includes a variable size *pad field* used to align the payload on 48-octet boundaries, a 2-octet *control field* that is currently unused, a 2-octet *length field* that indicates the number of octets in the user data, and, finally, a 4-octet CRC that can check the integrity of the entire payload. AAL5 is often referred to as the *Simple and Easy Adaptation Layer* (SEAL), and it may find an ideal application for itself in the burgeoning Internet arena. Recent studies indicate that TCP/IP transmissions produce comparatively large numbers of small packets that tend to be around 48 octets long. That being the case, AAL5 could well transport the bulk of them in its user data field. Furthermore, the maximum size of the user data field is 65,536 octets, coincidentally the same size as an IP packet.

ATM Forum Service Classes The ATM Forum looks at service definitions slightly differently than the ITU-T, as shown in Figure 6-10. Instead of the A-B-C-D services, the ATM Forum categorizes them as real-time and non-real-time services. Under the real-time category, they define constant-bit-rate services that demand fixed resources with guaranteed availability. They also define real-time VBR service, which provides for statistical multiplexed, variable bandwidth service allocated on demand. A further subset of real-time VBR is peak-allocated VBR, which guarantees constant loss and delay characteristics for all cells in that flow.

Under the non-real-time service class, *unspecified bit rate* (UBR) is the first service category. UBR is often compared to IP in that it is a best-effort delivery scheme in which the network provides whatever bandwidth it has available, with no guarantees made. All recovery functions from lost cells are the responsibility of the end-user devices.

UBR has two subcategories of its own. The first, *non-real-time VBR* (NRT-VBR), improves the impacts of cell loss and delay by adding a

Figure 6-10 ATM Forum service definitions.

Service	Descriptors	Loss	Delay	Bandwidth	Feedback
CBR	PCR, CDVT	Yes	Yes	Yes	No
VBR-RT	PCR, CDVT, SCR, MBS	Yes	Yes	Yes	No
VBR-NRT	PCR, CDVT, SCR, MBS	Yes	Yes	Yes	No
UBR	PCR, CDVT	No	No	No	No
ABR	PCR, CDVT, MCR	Yes	No	Yes	Yes

network resource reservation capability. *Available bit rate* (ABR), UBR's other subcategory, makes use of feedback information from the far end to manage loss and ensure fair access to and transport across the network.

Each of the five classes makes certain guarantees with regard to cell loss, cell delay, and available bandwidth. Furthermore, each of them takes into account descriptors that are characteristic of each service described. These include the *peak cell rate* (PCR), the *sustained cell rate* (SCR), the *minimum cell rate* (MCR), *cell delay variation tolerance* (CDVT), and *burst tolerance* (BT).

ATM Forum Specified Services The ATM Forum has identified a collection of services for which ATM is a suitable, perhaps even desirable, network technology. These include the *cell relay service* (CRS), the *circuit emulation service* (CES), *voice and telephony over ATM* (VTOA), the *Frame Relay bearer service* (FRBS), *LAN emulation* (LANE), *multiprotocol over ATM* (MPOA), and a collection of others.

CRS is the most basic of the ATM services. It delivers precisely what its name implies: a "raw pipe" transport mechanism for cell-based data. As such, it does not provide any ATM bells and whistles, such as QoS discrimination. Nevertheless, it is the most commonly implemented ATM offering because of its lack of implementation complexity.

CES gives service providers the capability to offer a selection of bandwidth levels by varying both the number of cells transmitted per second and the number of bytes contained in each cell.

VTOA is a service that has yet to be clearly defined. The capability to transport voice calls across an ATM network is a nonissue, given the availability of Class A service. What is not clearly defined, however, are corollary services such as 800/888 calls, 900 service, 911 call-handling,

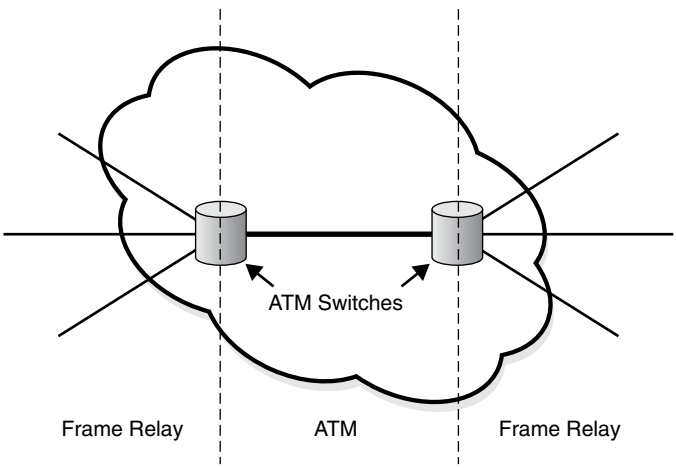
enhanced services billing, SS7 signal interconnection, and so on. Until these issues are clearly resolved, ATM-based, feature-rich telephony will not become a mainstream service, but will instead be limited to simple voice, and there *is* a difference.

FRBS refers to the capability of ATM to interwork with Frame Relay. Conceptually, the service implies that an interface standard enables an ATM switch to exchange data with a Frame Relay switch, thus allowing for interoperability between frame and cell-based services. Many manufacturers are taking a slightly different tack, however; they build switches with soft, chewy cell technology at the core and surround the core with hard, crunchy interface cards to suit the needs of the customer.

For example, an ATM switch might have ATM cards on one side to interface with other ATM devices on the network, but it might have Frame Relay cards on the other side to enable it to communicate with other Frame Relay switches, as shown in Figure 6-11. Thus, a single piece of hardware can logically serve as both a cell and Frame Relay switch. This design is becoming more and more common, because it helps to avoid a future rich with forklift upgrades.

LANE enables an ATM network to move traffic transparently between two similar LANs, but it also enables ATM to transparently slip into the LAN arena. For example, two Ethernet LANs could communicate across the fabric of an ATM network, as could two Token Ring LANs. In effect, LANE enables ATM to provide a bridging function between similar LAN environments. In LANE implementations the ATM net-

Figure 6-11
FRBS in ATM.



work does not handle MAC functions such as collision detection, token passing, or beaconing; it merely provides the connectivity between the two communicating endpoints. The MAC frames are simply transported inside AAL5 cells.

One clear concern about LANE is that LANs are connectionless, while ATM is a virtual circuit-based, connection-oriented technology. LANs routinely broadcast messages to all stations, while ATM enables point-to-point or multipoint circuits only. Thus, ATM must look like a LAN if it is to behave like one. To make this happen, LANE uses a collection of specialized LAN emulation clients and servers to provide the connectionless behavior expected from the ATM network.

On the other hand, MPOA provides the ATM equivalent of routing in LAN environments. In MPOA installations, routers are referred to as MPOA servers. When one station wants to transmit to another station, it queries its local MPOA server for the remote station's ATM address. The local server then queries its neighbor devices for information about the remote station's location. When a server finally responds, the originating station uses the information to establish a connection with the remote station, whereas the other servers cache the information for further use.

MPOA promises a great deal, but it is complex to implement and requires other ATM components, such as the Private NNI capability to work properly. Furthermore, it's being challenged by at least one alternative technology, known as IP switching.

IP switching is far less overhead-intensive than MPOA. Furthermore, it takes advantage of a known (but often ignored) reality in the LAN interconnection world: most routers today use IP as their core protocol, and the great majority of LANs are still Ethernet. This means that a great deal of simplification can be done by crafting networks to operate around these two technological bases. And in fact, this is precisely what IP switching does. By using existing, low-overhead protocols, the IP switching software creates new ATM connections dynamically and quickly, updating switch tables on the fly.

In IP switching environments, IP resides on top of ATM within a device, as shown in Figure 6-12, providing the best of both protocols. If two communicating devices want to exchange information and they have done so before, an ATM mapping already exists and no layer three involvement (IP) is required. The ATM switch portion of the service simply creates the connection at high speed. If an address lookup is required, then the "call" is handed up to IP, which takes whatever steps are required to perform the lookup (a DNS request, for example). Once it has

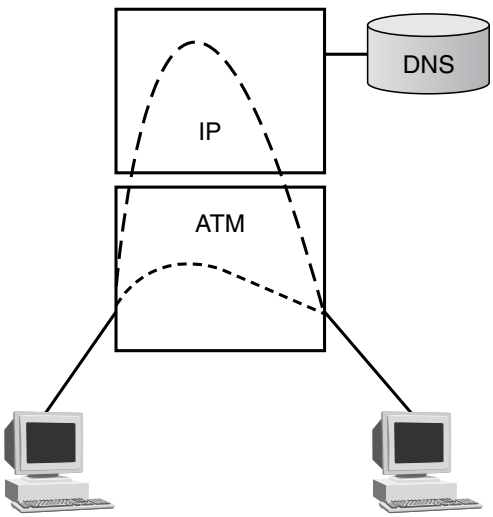


Figure 6-12
IP switching.

the information, it hands it down to ATM, which proceeds to set up the call. The next time the two need to communicate, ATM will be able to handle the connection.

Other services in which ATM plays a key role are looming on the horizon, including wireless ATM and video on demand for the delivery of interactive content such as videoconferencing and television. This leads to what I often refer to as "the great triumvirate": ATM, SONET or SDH, and broadband services. By combining the powerful switching and multiplexing fabric of ATM with the limitless transport capabilities of SONET or SDH, true broadband services can be achieved, and the idea of creating a network that can be all things to all services can finally be realized.

Optical Networking

Optical networking is often viewed as a point-to-point technology. It has achieved such a position of prominence in the last two years, however, that it qualifies as a transport option in its own right. Furthermore, optical switching is fast becoming real and optical routing is not far behind. In this next section, we discuss the development of optical networking, the various technologies that it employs, and the direction it seems to be going in this fast-paced market.

Early Optical Technology Breakthroughs

In 1878, two years after perfecting his speaking telegraph (which became the telephone), Alexander Graham Bell created a device that transmitted the human voice through the air for distances of up to 200 meters. The device, which he called the Photophone, used carefully angled mirrors to reflect sunlight onto a diaphragm that was attached to a mouthpiece, as shown in Figure 6-13.

At the receiving end (see Figure 6-14), the light was concentrated by a parabolic mirror onto a selenium resistor, which was connected to a battery and speaker. The diaphragm vibrated when struck by the human voice, which in turn caused the intensity of the light striking the resistor to vary. The selenium resistor, in turn, caused the current flow to vary in concert with the varying sunlight, which caused the received sound to come out of the speaker with remarkable fidelity. This represented the birth of optical transmission.

Optical transmission in its early days was limited in terms of what it was capable of doing. Consider the following analogy. If you look through a two-foot-square pane of window glass, it appears clear. If the glass is clean, it is virtually invisible. However, if you turn the pane on edge and look through it from edge to edge, the glass appears to be dark green. Very little light passes from one edge to the other. In this example, you are looking through two feet of glass. Imagine trying to pass a high-bandwidth optical signal through 40 or more kilometers of that glass!

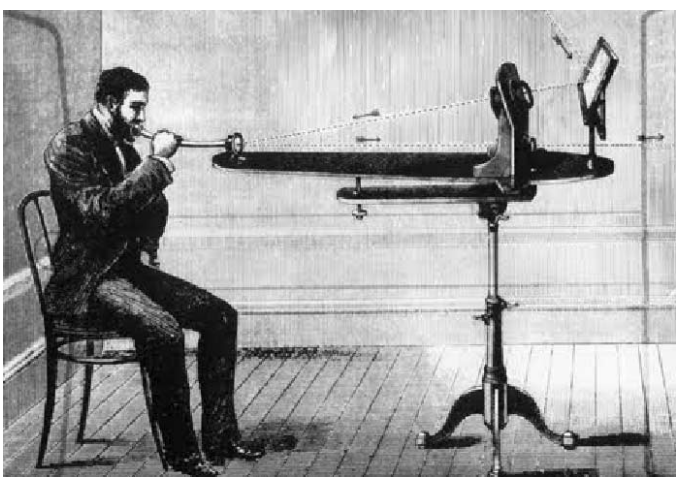


Figure 6-13 Bell Photophone transmitter.

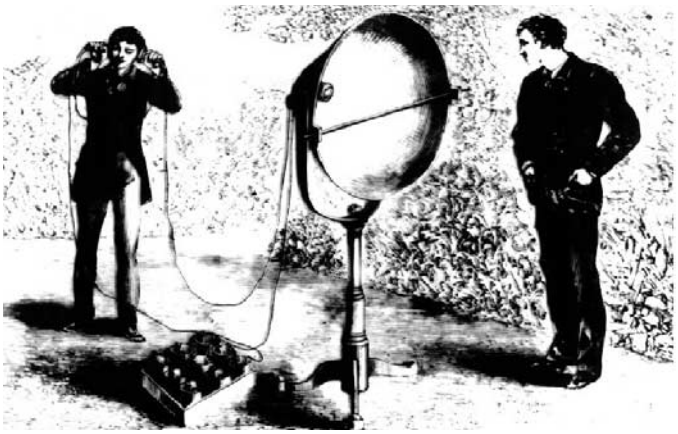


Figure 6-14
Bell Photophone receiver.

In 1966, Charles Kao and Charles Hockham at the United Kingdom's Standard Telecommunication Laboratory (now part of Nortel Networks) published their seminal work, demonstrating that optical fiber could be used to carry information, provided its end-to-end signal loss could be kept below 20 dB per kilometer. Keeping in mind that the decibel scale is logarithmic, 20 dB of loss means that 99 percent of the light would be lost over each kilometer of distance. Only 1 percent would actually reach the receiver, and that's a one-kilometer run. Imagine the loss over today's fiber cables that are hundreds of kilometers long if 20 dB was the modern performance criterion!

Kao and Hockham proved that metallic impurities in the glass such as chromium, vanadium, iron, and copper were the primary cause for such high levels of loss. In response, glass manufacturers rose to the challenge and began to research the creation of ultra-pure products.

In 1970, Peter Schultz, Robert Maurer, and Donald Keck of Corning Glass Works (now Corning Corporation) announced the development of a glass fiber that offered better attenuation than the recognized 20-dB threshold. Today, fiber manufacturers offer fiber so incredibly pure that 10 percent of the light arrives at a receiver placed 50 kilometers away. Put another way, a fiber with 0.2 dB of measured loss delivers more than 60 percent of the transmitted light over a distance of 10 kilometers. Remember the windowpane example? Imagine glass so pure that you could see clearly through a window 10 kilometers thick.

Fundamentals of Optical Networking

At their most basic level, optical networks require three fundamental components, as shown in Figure 6-15: a source of light, a medium over which to transport it, and a receiver for the light. Additionally, regenerators, optical amplifiers, and other pieces of equipment may be used in the circuit. We will examine each of these generic components in turn.

Optical Sources

Today the most common sources of light for optical systems are either *light-emitting diodes* (LEDs) or laser diodes. Both are commonly used, although laser diodes have become more common for high-speed data applications because of their coherent signal. Although lasers have gone through several iterations over the years, including ruby rod and helium-neon, semiconductor lasers became the norm shortly after their introduction in the early 1960s because of their low cost and high stability.

Light-Emitting Diodes (LEDs) LEDs come in two varieties: *surface-emitting LEDs* and *edge-emitting LEDs*. Surface-emitting LEDs give off light at a wide angle and therefore do not lend themselves to the more coherent requirements of optical data systems because of the difficulty involved in focusing their emitted light into the core of the receiving fiber. Instead, they are often used as indicators and signaling devices. They are, however, quite inexpensive and are therefore commonly found.

An alternative to the surface-emitting LED is the edge-emitting device. Edge emitters produce light at significantly narrower angles and have a smaller emitting area, which means that more of their emitted light can be focused into the core. They are typically faster devices than surface emitters, but do have a downside: they are temperature-sensitive

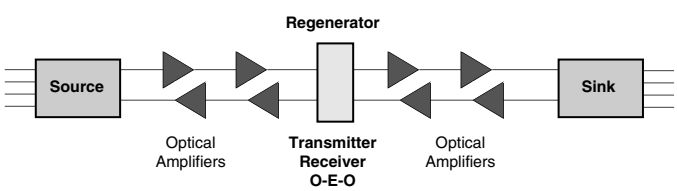


Figure 6-15 Components of a typical optical network.

and must therefore be installed in environmentally controlled devices to ensure the stability of the transmitted signal.

Laser Diodes Laser diodes represent the alternative to LEDs. A laser diode has a very small emitting surface, usually no larger than a few microns in diameter, which means that a great deal of the emitted light can be directed into the fiber. Because they represent a coherent source, the emission angle of a laser diode is extremely narrow. It is the fastest of the three devices.

Optical Fiber

When Peter Schultz, Donald Keck, and Robert Maurer began their work at Corning to create a low-loss optical fiber, they did so using a newly crafted process called *inside vapor deposition* (IVD). Whereas most glass is manufactured by melting and reshaping silica, IVD deposits various combinations of carefully selected compounds on the inside surface of a silica tube. The tube becomes the cladding of the fiber; the vapor-deposited compounds become the core. The compounds are typically *silicon chloride* ($SiCl_4$) and *oxygen* (O_2), which are reacted under heat to form a soft, sooty deposit of *silicon dioxide* (SiO_2), as shown in Figure 6-16. In some cases, impurities such as germanium are added at this time to cause various effects in the finished product.

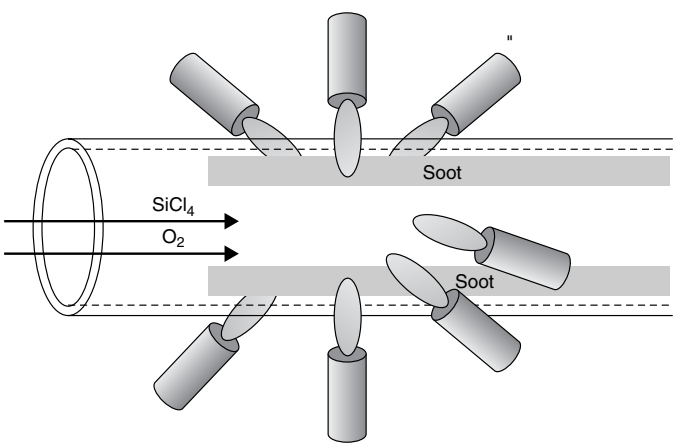


Figure 6-16
Creating a multilayer preform.

In practice, the $SiCl_4$ and O_2 are pumped into the fused silica tube as gases. The tube is heated in a high-temperature lathe, causing the sooty deposit to collect on the inside surface of the tube. The continued heating of the tube causes the soot to fuse into a glass-like substance.

This process can be repeated as many times as required to create a graded refractive index, if required. Ultimately, once the deposits are complete, the entire assembly is heated fiercely, which causes the tube to collapse, creating what is known in the optical fiber industry as a *preform*. An example of a preform is shown in Figure 6-17.

An alternative manufacturing process is called *outside vapor deposition* (OVD). In the OVD process, the soot is deposited on the surface of a rotating ceramic cylinder in two layers. The first layer is the soot that will become the core; the second layer becomes the cladding. Ultimately, the rod and soot are sintered to create a preform. The ceramic is then removed, leaving behind the fused silica that will become the fiber.

A number of other techniques can be used to create the preforms that are used to create fiber, but these are the principal techniques in use today. The next step is to convert the preform into optical fiber.

Drawing the Fiber

To make fiber from a preform, the preform is mounted in a furnace at the top of a tall building called a *drawing tower*. The bottom of the preform is heated until it has the consistency of taffy, at which time the soft glass is drawn down to form a thin fiber. When it strikes the cooler air outside

Figure 6-17 Preforms, ready to be drawn.

the furnace, the fiber solidifies. Needless to say, the process is carefully managed to ensure that the thickness of the fiber is precise; microscopes are used to verify the geometry of the fiber.

Other stages in the manufacturing process include monitoring processes to check the integrity of the product, a coating process that applies a protective layer, and a take-up stage where the fiber is wound onto reels for later assembly into cables of various types.

Optical Transmission

Dozens of different types of fiber exist. Some of them are holdovers from previous generations of optical technology that are still in use and represented the best efforts of technology available at the time. Others represent improvements on the general theme or specialized solutions to specific optical transmission challenges.

Generally speaking, two major types of fiber exist: *multimode,* which is the earliest form of optical fiber and is characterized by a large diameter central core, short distance capabilities, and low bandwidth; and *single mode,* which has a narrow core and is capable of greater distances and higher bandwidth. Varieties of each will be discussed in detail, later in the book.

To understand the reason for and philosophy behind the various forms of fiber, it is first necessary to understand the issues that confront transmission engineers who design optical networks.

Optical fiber has a number of advantages over copper. It is lightweight, has enormous bandwidth potential, has significantly higher tensile strength, can support many simultaneous channels, and is immune to electromagnetic interference. It does, however, suffer from several disruptive problems that cannot be discounted. The first of these is *loss* or *attenuation,* the inevitable weakening of the transmitted signal over distance that has a direct analog in the copper world. Attenuation is typically the result of two subproperties, *scattering* and *absorption,* both of which have cumulative effects. The second is *dispersion*, which is the spreading of the transmitted signal and is analogous to noise.

Scattering

Scattering occurs because of impurities or irregularities in the physical makeup of the fiber itself. The best known form of scattering is called

Rayleigh scattering. It is caused by metal ions in the silica matrix and results in light rays being scattered in various directions.

Rayleigh scattering occurs most commonly around wavelengths of 1000 nm and is responsible for as much as 90 percent of the total attenuation that occurs in modern optical systems. It occurs when the wavelengths of the light being transmitted are roughly the same size as the physical molecular structures within the silica matrix. Thus, short wavelengths are affected by Rayleigh scattering effects far more than long wavelengths. In fact, it is because of Rayleigh scattering that the sky appears to be blue. The shorter (blue) wavelengths of light are scattered more than the longer wavelengths of light.

Absorption

Absorption results from three factors: hydroxyl (OH^-; water) ions in the silica, impurities in the silica, and incompletely diminished residue from the manufacturing process. These impurities tend to absorb the energy of the transmitted signal and convert it to heat, resulting in an overall weakening of the optical signal. Hydroxyl absorption occurs at 1.25 and 1.39 μm. At 1.7 μm, the silica itself starts to absorb energy because of the natural resonance of silicon dioxide.

Dispersion

As mentioned earlier, dispersion is the optical term for the spreading of the transmitted light pulse as it transits the fiber. It is a bandwidth-limiting phenomenon and comes in two forms: *multimode dispersion* and *chromatic dispersion*. Chromatic dispersion is further subdivided into *material dispersion* and *waveguide dispersion.*

Multimode Dispersion To understand multimode dispersion, it is first important to understand the concept of a *mode.* Figure 6-18 shows a fiber with a relatively wide core. Because of the width of the core, it enables light rays arriving from the source at a variety of angles (three in this case) to enter the fiber and be transmitted to the receiver. Because of the different paths that each ray, or mode, will take, they will arrive at the receiver at different times, resulting in a dispersed signal.

Now consider the system shown in Figure 6-19. The core is much narrower and only enables a single ray, or mode, to be sent down the fiber.

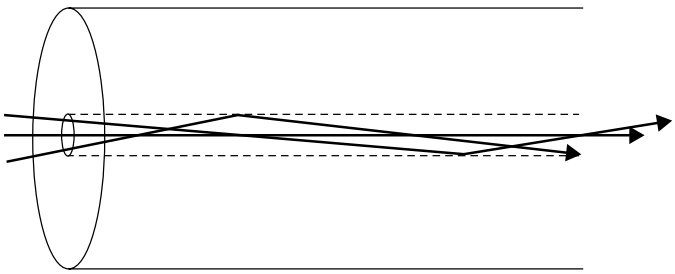


Figure 6-18
Multimode fiber. Note wide core diameter.

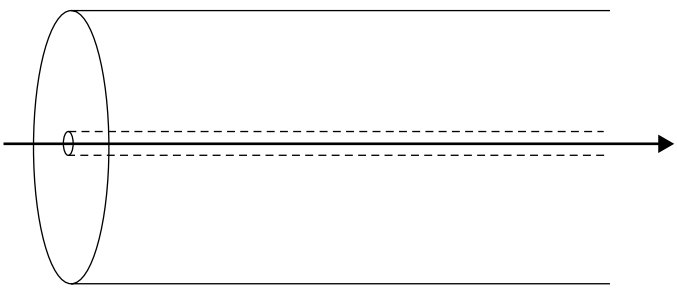


Figure 6-19
Single mode fiber. Note narrow core diameter.

This results in less end-to-end energy loss and avoids the dispersion problem that occurs in multimode installations.

Chromatic Dispersion The speed at which an optical signal travels down a fiber is absolutely dependent upon its wavelength. If the signal comprises multiple wavelengths, then the different wavelengths will travel at different speeds, resulting in an overall spreading or smearing of the signal. As discussed earlier, chromatic dispersion comprises two subcategories: material dispersion and waveguide dispersion.

Material Dispersion Simply put, material dispersion occurs because different wavelengths of light travel at different speeds through an optical fiber. To minimize this particular dispersion phenomenon, two factors must be managed. The first of these is the number of wavelengths that make up the transmitted signal. An LED, for example, emits a rather broad range of wavelengths between 30 and 180 nm, whereas a laser emits a much narrower spectrum, typically less than 5 nm. Thus, a laser's output is far less prone to be seriously affected by material dispersion than the signal from an LED.

The second factor that affects the degree of material dispersion is a characteristic called the *center operating wavelength of the source signal.* In the vicinity of 850 nm, red, longer wavelengths travel faster than their shorter blue counterparts, but at 1550 nm, the situation is the opposite: blue wavelengths travel faster. Of course, the two meet at a point and share a common minimum dispersion level; it is in the range of 1310 nm, often referred to as the *zero-dispersion wavelength*. Clearly, this is an ideal place to transmit data signals, since dispersion effects are minimized here. As we will see later, however, other factors crop up that make this a less desirable transmission window than it appears. Material dispersion is a particularly vexing problem in single-mode fibers.

Waveguide Dispersion Because the core and the cladding of a fiber have slightly different indices of refraction, the light that travels in the core moves slightly slower than the light that escapes into and travels in the cladding. This results in a dispersion effect that can be corrected by transmitting at specific wavelengths where material and waveguide dispersion actually occur at a minimum.

Putting It All Together

So what does all of this have to do with the high-speed transmission of voice, video, and data? A lot, as it turns out. Understanding where attenuation and dispersion problems occur helps optical design engineers determine the best wavelengths at which to transmit information, taking into account distance, the type of fiber, and other factors that can potentially affect the integrity of the transmitted signal.

Consider the graph shown in Figure 6-20. It depicts the optical transmission domain as well as the areas where problems arise. Attenuation (dB/km) is shown on the Y axis; Wavelength (nm) is shown on the X axis.

First of all, note that four *transmission windows* are in the figure. The first one is at approximately 850 nm, the second at 1,310 nm, a third at 1,550 nm, and a fourth at 1,625 nm, the last two labeled C and L band, respectively. The 850-nm band is the first to be used because of its adherence to the wavelength at which the original LED technology operated. The second window at 1,310 nm enjoys low dispersion; this is where dispersion effects are minimized. 1,550 nm, the so-called C band, has emerged as the ideal wavelength at which to operate long-haul systems and systems upon which *Dense Wavelength Division Multiplexing* (DWDM) has

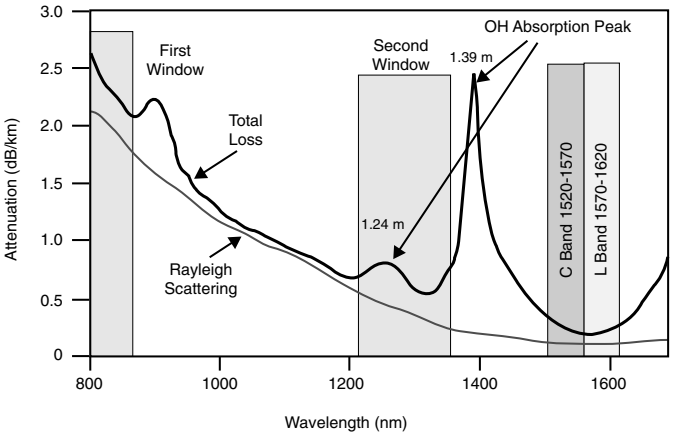


Figure 6-20
The optical transmission domain.

been deployed because (1) loss is minimized in this region, and (2) dispersion minimums can be shifted here. The relatively new L band has enjoyed some early success as the next effective operating window.

Notice also that Rayleigh scattering is shown to occur at or around 1,000 nm, while hydroxyl absorption by water occurs at 1,240 and 1,390 nm. Needless to say, network designers would be well served to avoid transmitting at any of the points on the graph where Rayleigh scattering, high degrees of loss, or hydroxyl absorption have the greatest degree of impact.

Note also that dispersion, shown by the lower line, is at a minimum point in the second window, while loss, shown by the upper line, drops to a minimum point in the third window. In fact, dispersion is minimized in traditional single-mode fiber at 1,310 nm, whereas loss is at minimums at 1,550 nm. So, the obvious question becomes this: which one do you want to minimize: loss or dispersion?

Luckily, this choice no longer has to be made. Today, *dispersion-shifted fibers* (DSF) have become common. By modifying the manufacturing process, engineers can shift the point at which minimum dispersion occurs from 1,310 nm to 1,550 nm, causing it to coincide with the minimum loss point such that loss and dispersion occur at the same wavelength.

Unfortunately, although this fixes one problem, it creates a new and potentially serious alternative problem. DWDM has become a mainstay technology for multiplying the available bandwidth in optical systems. When DWDM is deployed over dispersion-shifted fiber, serious non-

linearities occur at the zero dispersion point, which effectively destroy the DWDM signal. Think about it: DWDM relies on the capability to channelize the available bandwidth of the optical infrastructure and maintain some degree of separation between the channels. If dispersion is minimized in the 1,559-nm window, then the channels will effectively overlay each other in DWDM systems. Specifically, a problem called *four-wave mixing* (FWM) creates "sidebands" that interfere with the DWDM channels, destroying their integrity. In response, fiber manufacturers have created *non-zero dispersion-shifted fiber* (NZDSF) that lowers the dispersion point to *near zero*, making it occur just outside of the 1,550-nm window. This eliminates the nonlinear FWM problem.

Fiber Nonlinearities

A classic business quote, imminently applicable to the optical networking world, observes "in its success lie the seeds of its own destruction." As the marketplace clamors for longer transmission distances with minimal amplification, more wavelengths per fiber, higher bit rates, and increased signal power, a rather ugly collection of transmission impairments, known as *fiber nonlinearities,* rises to challenge attempts to make them happen. These impairments go far beyond the simple concerns brought about by loss and dispersion; they represent a significant performance barrier.

The "special relationship" that exists between transmission power and the refractive index of the medium gives rise to four service-affecting optical nonlinearities: *self-phase modulation* (SPM), *cross-phase modulation* (XPM), FWM, and *intermodulation.*

Self-Phase Modulation (SPM)

When SPM occurs, chromatic dispersion kicks in to create something of a technological double-whammy. As the light pulse moves down the fiber, its leading edge increases the refractive index of the core, which causes a shift toward the longer-wavelength, blue end of the spectrum. The trailing edge, on the other hand, decreases the refractive index of the core, causing a shift toward the shorter-wavelength, red end of the spectrum. This causes an overall spreading or smearing of the transmitted signal, a phenomenon known as *chirp.* It occurs in fiber systems that transmit a single pulse down the fiber and is proportional to the amount of

chromatic dispersion in the fiber; the more chromatic dispersion, the more SPM. It is counteracted with the use of large effective area fibers.

Cross-Phase Modulation (XPM)

When multiple optical signals travel down the same fiber core, they both change the refractive index in direct proportion to their individual power levels. If the signals happen to cross, they will distort each other. Although XPM is similar to SPM, one significant difference exists: self-phase modulation is directly affected by chromatic dispersion, yet cross-phase modulation is only minimally affected by it. Large effective area fibers can reduce the impact of XPM.

Four-Wave Mixing (FWM)

FWM is the most serious of the power/refractive index-induced non-linearities today because it has a catastrophic effect on DWDM-enhanced systems. Because the refractive index of fiber is nonlinear, and because multiple optical signals travel down the fiber in DWDM systems, a phenomenon known as *third-order distortion* can occur that seriously affects multichannel transmission systems. Third-order distortion causes harmonics to be created in large numbers that have the annoying habit of occurring where the actual signals are, resulting in their obliteration.

FWM is directly related to DWDM. In DWDM fiber systems, multiple simultaneous optical signals are transmitted across an optical span. They are separated on an ITU-blessed standard transmission grid by as much as 100 GHz (although most manufacturers today have reduced that to 50 GHz or better). This separation ensures that they do not interfere with each other.

Consider now the effect of dispersion-shifted fiber on DWDM systems. In DSF, signal transmission is moved to the 1,550-nm band to ensure that dispersion and loss are both minimized within the same window. However, minimal dispersion has a rather severe unintended consequence when it occurs in concert with DWDM. Because it reduces dispersion to near zero, it also prevents multichannel systems from existing because it does not enable proper channel spacing. FWM then becomes a serious problem.

Several things can reduce the impact of FWM. As the dispersion in the fiber drops, the degree of FWM increases dramatically. In fact, it is *worst*

at the zero-dispersion point. Thus, the intentional inclusion of a small amount of chromatic dispersion actually helps to reduce the effects of FWM. For this reason, fiber manufacturers sell NZDSF, which moves the dispersion point to a point *near* the zero point, thus ensuring that a small amount of dispersion creeps in to protect against FWM problems.

Another factor that can minimize the impact of FWM is to widen the spacing between DWDM channels. This, of course, reduces the efficiency of the fiber by reducing the total number of available channels and is therefore not a popular solution, particularly because the trend in the industry is to move toward narrower channel spacing as a way to increase the total number of available channels. Already several vendors have announced spacing as narrow as 5 GHz. Finally, large effective area fibers tend to suffer less from the effects of FWM.

Intermodulation Effects

In the same way that cross-phase modulation results from interference between multiple simultaneous signals, intermodulation causes secondary frequencies to be created that are cross-products of the original signals being transmitted. Large effective area fibers can alleviate the symptoms of intermodulation.

Scattering Problems

Scattering within the silica matrix causes the second major impairment phenomenon. Two significant nonlinearities result: *Stimulated Brillouin Scattering* (SBS) and *Stimulated Raman Scattering* (SRS).

Stimulated Brillouin Scattering (SBS) SBS is a power-related phenomenon. As long as the power level of a transmitted optical signal remains below a certain threshold, usually on the order of three milliwatts, SBS is not a problem. The threshold is directly proportional to the fiber's effective area, and because DSF typically have smaller effective areas, they have lower thresholds. The threshold is also proportional to the width of the originating laser pulse; as the pulse gets wider, the threshold goes up. Thus, steps are often taken through a variety of techniques to artificially broaden the laser pulse. This can raise the threshold significantly, to as high as 40 milliwatts.

SBS is caused by the interaction of the optical signal moving down the fiber with the acoustic vibration of the silica matrix that makes up the fiber. As the silica matrix resonates, it causes some of the signal to be reflected back toward the source of the signal, resulting in noise, signal degradation, and a reduction of overall bit rate in the system. As the power of the signal increases beyond the threshold, more of the signal is reflected, resulting in a multiplication of the initial problem.

It is interesting to note that two forms of Brillouin Scattering exist. When electric fields that oscillate in time within an optical fiber interact with the natural acoustic resonance of the fiber material itself (sorry, a little more physics), the result is a tendency to backscatter light as it passes through the material, which is called simply Brillouin scattering. If, however, the electric fields are caused by the optical signal itself, the signal is seen to cause the phenomenon. This is called SBS.

To summarize: because of backscattering, SBS reduces the amount of light that actually reaches the receiver and causes noise impairments. The problem increases quickly above the threshold and has a more deleterious impact on longer wavelengths of light. One additional fact: in-line optical amplifiers such as *erbium-doped fiber amplifiers* (EDFAs) add to the problem significantly. If four optical amplifiers are located along an optical span, the threshold will drop by a factor of four. Solutions to SBS include the use of wider-pulse lasers and larger effective area fibers.

Stimulated Raman Scattering (SRS) SRS is something of a power-based crosstalk problem. In SRS, high-power, short-wavelength channels tend to bleed power into longer wavelength, lower-power channels. It occurs when a light pulse moving down the fiber interacts with the crystalline matrix of the silica, causing the light to (1) be back-scattered, and (2) shift the wavelength of the pulse slightly. Whereas SBS is a backward-scattering phenomenon, SRS is a two-way phenomenon, causing both back-scattering and a wavelength shift. The result is crosstalk between adjacent channels.

The good news is that SRS occurs at a much higher power level, close to a watt. Furthermore, it can be effectively reduced through the use of large effective area fibers.

Optical Amplification

As long as we are on the subject of Raman scattering, we should introduce the concept of optical amplification. This may seem like a bit of a

non-sequitur, but it really isn't. True optical amplification actually uses a form of Raman scattering to amplify the transmitted signal.

Traditional Amplification and Regeneration Techniques

In a traditional metallic analog environment, transmitted signals tend to weaken over distance. To overcome this problem, amplifiers are placed in the circuit periodically to raise the power level of the signal. This technique itself has a problem, however. In addition to amplifying the signal, amplifiers also amplify whatever cumulative noise has been picked up by the signal during its trip across the network. Over time, it becomes difficult for a receiver to discriminate between the actual signal and the noise embedded in the signal. Extraordinarily complex recovery mechanisms are required to discriminate between optical wheat and noise chaff.

In digital systems, *regenerators* are used to not only amplify the signal, but to also remove any extraneous noise that has been picked up along the way. Thus, digital regeneration is a far more effective signal recovery methodology than simple amplification.

Even though signals propagate significantly farther in optical fiber than they do in copper facilities, they are still eventually attenuated to the point that they must be regenerated. In a traditional installation, the optical signal is received by a receiver circuit, converted to its electrical analog, regenerated, converted back to an optical signal, and transmitted onward over the next fiber segment. This optical-to-electrical-to-optical conversion process is costly, complex, and time-consuming. However, it is proving to be far less necessary as an amplification technique than it used to be because of true optical amplification that has recently become commercially feasible. Please note that optical amplifiers *do not* regenerate signals; they merely amplify. Regenerators are still required, albeit far less frequently.

Optical amplifiers represent one of the technological leading edges of data networking. Instead of the O-E-O process, optical amplifiers receive the optical signal, amplify it as an optical signal, and then retransmit it as an optical signal; no electrical conversion is required. Like their electrical counterparts, however, they also amplify the noise; at some point, signal regeneration is required.

Optical Amplifiers: How They Work

It was only a matter of time before all-optical amplifiers became a reality. It makes intuitively clear sense that a solution that eliminates the electrical portion of the O-E-O process would be a good one. Optical amplification is that solution.

You will recall that SRS is a fiber nonlinearity that is characterized by high-energy channels pumping power into low-energy channels. What if that phenomenon could be harnessed as a way to amplify optical signals that have weakened over distance?

Optical amplifiers are actually rather simple devices that, as a result, tend to be extremely reliable. The optical amplifier comprises the following: an input fiber carrying the weakened signal that is to be amplified, a pair of optical isolators, a coil of doped fiber, a pump laser, and the output fiber that now carries the amplified signal. A functional diagram of an optical amplifier is shown in Figure 6-21.

The coil of doped fiber lies at the heart of the optical amplifier's functionality. Doping is simply the process of embedding some kind of functional impurity in the silica matrix of the fiber when it is manufactured. In optical amplifiers, this impurity is more often than not an element called *erbium*. Its role will become clear in just a moment.

The pump laser shown in the upper-left corner of Figure 6-21 generates a light signal at a particular frequency, often 980 nm, in the *opposite direction* than the actual transmitted signal flows. As it turns out, erbium becomes atomically excited when it is struck by light at that wavelength. When an atom is excited by pumped energy, it jumps to a higher energy level (those of you who are recovering physicists will remember classroom discussions about orbital levels: $1S^1$, $1S^2$, $2S^1$, $2S^2$, $2P^6$, and so on) and then

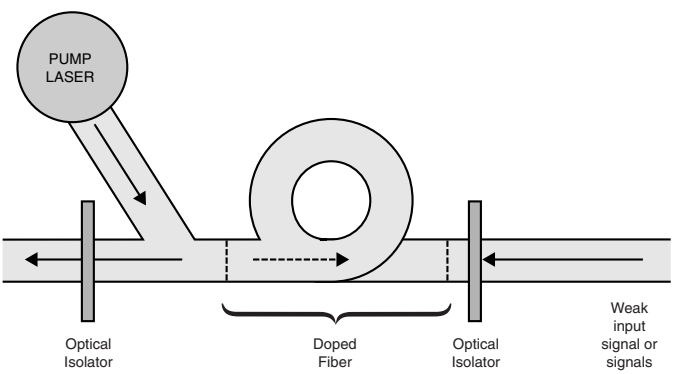


Figure 6-21
EDFA.

falls back down, giving off a photon at a certain wavelength. When erbium is excited by light at 980 nm, it emits photons within the 1,550 nm region, coincidentally the wavelength at which multichannel optical systems operate. So, when the weak, transmitted signal reaches the coil of erbium-doped fiber, the erbium atoms, now excited by the energy from the pump laser, bleed power into the weak signal at precisely the right wavelength, causing a generalized amplification of the transmitted signal. The optical isolators serve to prevent errant light from backscattering into the system, creating noise.

EDFAs are highly proletariat in nature. They amplify anything, including the noise that the signal may have picked up. Therefore, a need will still exist at some point along the path of long-haul systems for regeneration, although far less frequently than in traditional copper systems. Most manufacturers of optical systems publish recommended span engineering specifications that help service providers and network designers take such concerns into account as they design each transmission facility.

Other Amplification Options

At least two other amplification techniques in addition to EDFAs have recently come into favor. The first of these is called Raman amplification, which is similar to EDFA in the sense that it relies on Raman effects to do its task, but is different for other rather substantial reasons. In Raman amplification, the signal beam travels down the fiber alongside a rather powerful pump beam, which excites atoms in the silica matrix that in turn emit photons that amplify the signal. The advantage of Raman amplification is that it requires no special doping; erbium is not necessary. Instead, the silica itself gives off the necessary amplification. In this case, the fiber itself becomes the amplifier.

Raman amplifiers require a significantly high-power pump beam (about one watt, although some systems have been able to reduce the required power to 750 mw or less) and even at high levels the power gain is relatively low. Their advantage, however, is that their induced gain is distributed across the entire optical span. Furthermore, it will operate within a relatively wide range of wavelengths, including 1,310 and 1,550 nm, currently the two most popular and effective transmission windows.

Semiconductor lasers have also been deployed as optical amplification devices in some installations. In semiconductor optical amplifiers, the

weakened optical signal is pumped into the ingress edge of a semiconductor optical amplifier. The active layer of the semiconductor substrate amplifies the signal and regenerates it on the other side.

The primary downside to these devices is their size. They are small, and their light-collecting capabilities are therefore somewhat limited. A typical single-mode fiber generates an intense spot of light that is roughly 10 microns in diameter. The point upon which that light impinges upon the semiconductor amplifier is less than a micron in diameter, meaning that a lot of the light is lost. Other problems also crop up, including polarization issues, reflection, and variable gain. As a result, these devices are not in widespread use; EDFAs and Raman amplification techniques are far more common.

Optical Receivers

So far, we have discussed the sources of light, including LEDs and laser diodes. We have briefly described the various flavors of optical fiber and the problems they encounter as transmission media. Now we turn our attention to the devices that receive the transmitted signal.

The receive devices used in optical networks have a single responsibility: to capture the transmitted optical signal and convert it into an electrical signal that can then be processed by the end equipment. Various stages of amplification may be used to ensure that the signal is strong enough to be acted upon, and demodulation circuitry may be used to recreate the originally transmitted electronic signal.

Photodetector Types

Although many different types of photosensitive devices exist, two are used most commonly as photodetectors in modern networks: *positive-intrinsic-negative* (PIN) photodiodes and *avalanche photodiodes* (APDs).

Positive-Intrinsic-Negative (PIN) Photodiodes PIN photodiodes are similar to the device described previously in the general discussion of photosensitive semiconductors. Reverse biasing the junction region of the device prevents a current flow until light at a specific wavelength strikes the substance, creating electron-hole pairs and enabling the current to flow across the three-layer interface in proportion to the intensity

of the incident light. Although they are not the most sensitive devices available for the purpose of photodetection, they are perfectly adequate for the requirements of most optical systems. In cases where they are not considered sensitive enough for high-performance systems, they can be coupled with a preamplifier to increase the overall sensitivity.

Avalanche Photodiodes (APDs) APDs work as optical signal amplifiers. They use a strong electric field to perform what is known as *avalanche multiplication.* In an APD, the electric field causes current accelerations such that the atoms in the semiconductor matrix get excited and create, in effect, an "avalanche" of current to occur. The good news is that the amplification effect can be as much as 30 to 100 times the original signal; the bad news is that the effect is not altogether linear and can create noise. APDs are sensitive to temperature and require a significant voltage to operate them, 30 to 300 volts depending on the device. However, they are popular for broadband systems and work well in the gigabit range.

We have now discussed transmitters, fiber media, and receivers. In the next section, we examine the fibers themselves and how they have been carefully designed to serve as solutions for a wide variety of networking challenges and to forestall the impact of the nonlinearities described in this section.

Optical Fiber

As mentioned briefly in a prior section, fiber has evolved over the years in a variety of ways to accommodate both the changing requirements of the customer community and the technological challenges that emerged as the demand for bandwidth climbed precipitously. These changes came in various forms of fiber that presented different behavior characteristics to the market.

Modes: An Analogy

The concept of modes is sometimes difficult to understand, so let me pass along an analogy that will help. Imagine a shopping mall that has a wide, open central area that all the shops open onto. An announcement comes over the PA system informing people that "the mall is now closed;

please make your way to the exit." Shoppers begin to make their way to the doors, but some wander from store to store, window-shopping along the way, whereas others take a relatively straight route to the exit. The result is that some shoppers take longer than others to exit the mall because there are different modes.

Now consider a mall that has a single, very narrow corridor that is only as wide as a person's shoulders. Now when the announcement comes, everyone heads for the exit, but they must form a single-file line and head out in an orderly fashion. If you understand the difference between these two examples, you understand *single-* versus *multimode fiber*. The first example represents multimode; the second represents single mode.

Multimode Fiber

The first of these is multimode fiber, which arrived in a variety of different forms. Multimode fiber bears that name because it enables more than a single mode or ray of light to be carried through the fiber simultaneously because of the relatively wide core diameter that characterizes the fiber.

Although the dispersion that potentially results from this phenomenon can be a problem, multimode fiber has its advantages. For one thing, it is far easier to couple the relatively wide and forgiving end of a multimode fiber to a light source than that of the much narrower single-mode fiber. It is also significantly less expensive to manufacture (and purchase) and relies on LEDs and inexpensive receivers rather than the more expensive laser diodes and ultra-sensitive receiver devices. However, advancements in technology have caused the use of multimode fiber to fall out of favor; single-mode is far more commonly used today.

Multimode fiber is manufactured in two forms: *step-index fiber* and *graded-index fiber*. We will examine each in turn.

Multimode Step-Index Fiber In step-index fiber, the index of refraction of the core is slightly higher than the index of refraction of the cladding. Remember that the higher the refractive index, the slower the signal travels through the medium. Thus, in step-index fiber, any light that escapes into the cladding because it enters the core at too oblique an angle will actually travel slightly faster in the cladding (assuming it does not escape altogether) than it would if it traveled in the core. Of course, any rays that are reflected repeatedly as they traverse the core

also take longer to reach the receiver, resulting in a dispersed signal that causes problems for the receiver at the other end. Clearly, this phenomenon is undesirable; for that reason, graded-index fiber was developed.

Multimode Graded-Index Fiber Because of the dispersion that is inherent in the use of step-index fiber, optical engineers created graded index fiber as a way to overcome the signal degradation that occurred.

In graded-index fiber, the refractive index of the core actually decreases from the center of the fiber outward. In other words, the refractive index at the center of the core is higher than the refractive index at the edge of the core. The result of this rather clever design is that as light enters the core at multiple angles and travels from the center of the core outward, it is actually accelerated at the edge and slowed down near the center, causing most of the light to arrive at roughly the same time. Thus, graded-index fiber helps to overcome the dispersion problems associated with step-index multimode fiber. Light that enters this type of fiber does not travel in a straight line, but rather follows a parabolic path, with all rays arriving at the receiver at more or less the same time.

Graded-index fiber typically has a core diameter of 50 to 62.5 microns, with a cladding diameter of 125 microns. Some variations exist; at least one form of multimode graded-index has a core diameter of 85 microns, somewhat larger than those described. Furthermore, the actual thickness of the cladding is important. If it is thinner than 20 microns, light begins to seep out, causing additional problems for signal propagation.

Graded-index fiber was commonly used in telecommunications applications until the late 1980s. Even though graded-index fiber is significantly better than step-index fiber, it is still multimode fiber and does not eliminate the problems inherent in being multimode. Thus was born the next generation of optical fiber: single-mode.

Single-Mode Fiber

An interesting mental conundrum crops up with the introduction of single-mode fiber. The core of single-mode fiber is significantly narrower than the core of multimode fiber. Because it is narrower, it would seem that its capability to carry information would be reduced due to its limited light-gathering capability. This, of course, is not the case. As its name implies, it enables a single mode or ray of light to propagate down the fiber core, thus eliminating the intermodal dispersion problems that plague multimode fibers.

In reality, single-mode fiber is a stepped-index design, because the core's refractive index is slightly higher than that of the cladding. It has become the de facto standard for optical transmission systems and takes on many forms depending on the specific application within which it will be used.

Most single-mode fiber has an extremely narrow core diameter on the order of seven to nine microns, and a cladding diameter of 125 microns. The advantage of this design is that it only enables a single mode to propagate. The downside, however, is the difficulty involved in working with it. The core must be coupled directly to the light source and the receiver in order to make the system as effective as possible. Given that the core is approximately one-sixth the diameter of a human hair, the mechanical process through which this coupling takes place becomes Herculean.

Single-Mode Fiber Designs

The reader will recall that we spent a considerable amount of time discussing the many different forms of transmission impairments (nonlinearities) that challenge optical systems. Loss and dispersion are the key contributing factors in most cases and do, in fact, cause serious problems in high-speed systems. The good news is that optical engineers have done yeoman's work creating a wide variety of single-mode fibers that address most of the nonlinearities.

Since its introduction in the early 1980s, single-mode fiber has undergone a series of evolutionary phases in concert with the changing demands of the bandwidth marketplace. The first variety of single-mode fiber to enter the market was called *non-dispersion-shifted fiber* (NDSF). Designed to operate in the 1,310-nm second window, dispersion in these fibers was close to zero at that wavelength. As a result, it offered high bandwidth and low dispersion. Unfortunately, it was soon the victim of its own success.

As demand for high-bandwidth transport grew, a third window was created at 1,550 nm for single-mode fiber transmission. It provided attenuation levels that were less than half those measured at 1,310 nm, but unfortunately was plagued with significant dispersion. Since the bulk of all installed fiber was NDSF, the only solution available to transmission designers was to narrow the linewidth of the lasers employed in these systems and make them more powerful. Unfortunately, increasing the power and reducing the laser linewidth is expensive, so another solution emerged.

Dispersion-Shifted Fiber (DSF)

One solution that emerged was DSF. With DSF, the minimum dispersion point is mechanically shifted from 1,310 nm to 1,550 nm by modifying the design of the actual fiber so that waveguide dispersion is increased. The reader will recall that waveguide dispersion is a form of chromatic dispersion that occurs because the light travels at different speeds in the core and cladding.

One technique for building DSF (sometimes called *zero dispersion-shifted fiber*) is to actually build a fiber of multiple layers. In this design, the core has the highest index of refraction and changes gradually from the center outward until it equals the refractive index of the outer cladding. The inner core is surrounded by an inner cladding layer, which is in turn surrounded by an outer core. This design works well for single-wavelength systems, but experiences serious signal degradation when multiple wavelengths are transmitted, such as when used with DWDM systems. FWM, described earlier, becomes a serious impediment to clean transmissions in these systems. Given that multiple-wavelength systems are fast becoming the norm today, the single-wavelength limit is a show-stopper. The result was a relatively simple and elegant set of solutions.

The second technique is to eliminate or at least substantially reduce the absorption peaks in the fiber performance graph so that the second and third transmission windows merge into a single, larger window, thus enabling the creation of the fourth window described previously that operates between 1,565 and 1,625 nm, the so-called L-band.

Finally, the third solution came with the development of NZDSF. NZDSF shifts the minimum dispersion point so that it is *close* to the zero point, but not actually *at* it. This prevents the nonlinear problems that occur at the zero point to be avoided because it introduces a small amount of chromatic dispersion.

Why Does It Matter?

It is always good to go back and review why we care about such things as dispersion-shifting and absorption issues. Remember that the key to keeping the cost of a network down is to reduce maintenance and the need to add hardware or additional fiber when bandwidth gets tight. DWDM, discussed in detail later, offers an elegant and relatively simple solution to the problem of the cost of bandwidth. However, its use is not

without cost. Multiwavelength systems will not operate effectively over DSF because of dramatic nonlinearities, so if DWDM is to be used, NZDSF must be deployed.

Dense Wavelength Division Multiplexing (DWDM)

When high-speed transport systems such as SONET and SDH were first introduced, the bandwidth that they made possible was unheard of. The early systems that operated at OC-3/STM-1 levels (155.52 Mbps) provided volumes of bandwidth that were almost unimaginable. As the technology advanced to higher levels, the market followed Say's Law, creating demand for the ever-more available volumes of bandwidth.

There were limits, however. Today OC-48/STM-16 (2.5 Gbps) is extremely popular, but OC-192/STM-64 (10 Gbps) represents the practical upper limit of SONET's and SDH's transmission capabilities, given the limitations of existing *time division multiplexing* (TDM) technology. The alternative is to simply multiply the channel count, and that's where WDM comes into play.

WDM is really nothing more than *frequency division multiplexing* (FDM), albeit at very high frequencies. The ITU has standardized a channel separation grid that centers around 193.1 THz, ranging from 191.1 THz to 196.5 THz. Channels on the grid are technically separated by 100 GHz, but many industry players today are using 50-GHz separation.

The majority of WDM systems operate in the C-band (third window, 1,550 nm), which enables the close placement of channels and the reliance on EDFAs to improve signal strength. Older systems, which spaced the channels 200 GHz (1.6 nm) apart, were referred to simply as WDM systems, while the newer systems are referred to as *Dense* WDM systems because of their tighter channel spacing. Modern systems routinely pack 40- to 10-Gbps channels across a single fiber for an aggregate bit rate of 400 Gbps.

How DWDM Works

As Figure 6-22 illustrates, a WDM system consists of multiple input lasers, an ingress multiplexer, a transport fiber, an egress multiplexer, and, of course, customer receiving devices. If the system has eight

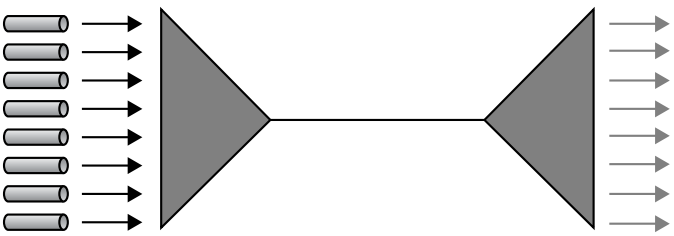


Figure 6-22 DWDM channel separation.

channels, such as the one shown in the figure, it has eight lasers and eight receivers. The channels are separated by 100 GHz to avoid fiber nonlinearities or they are closer if the system supports the 50-GHz spacing. Each channel, sometimes referred to as a lambda (l, the Greek letter and universal symbol used to represent wavelength), is individually modulated, and ideally the signal strengths of the channels should be close to one another. Generally speaking, this is not a problem, because in DWDM systems the channels are closely spaced and therefore do not experience significant attenuation variation from channel to channel.

Operators of DWDM-equipped networks face a significant maintenance issue. Consider a 16-channel DWDM system. This system has 16 lasers, 1 for each channel, which means that the service provider must maintain 16 spare lasers in case of a laser failure. The latest effort underway is the deployment of tunable lasers, which enable the laser to be tuned to any output wavelength, thus reducing the volume of spares that must be maintained and, by extension, the cost.

So, what do we find in a typical WDM system? A variety of components that include the following:

- **Multiplexers** Combine multiple optical signals for transport across a single fiber
- **Demultiplexers** Disassemble the aggregate signal so that each signal component can be delivered to the appropriate optical receiver (PIN or APD)
- **Active or passive switches or routers** Direct each signal component in a variety of directions
- **Filters** Serve to provide wavelength selection
- **Optical add-drop multiplexers** Give the service provider the ability to pick up and drop off individual wavelength components at intermediate locations throughout the network

Together these components make up the heart of the typical high-bandwidth optical network. And why is DWDM so important? Because of the cost differential that exists between a DWDM-enhanced network and a traditional network. To expand network capacity today by putting more fiber in the ground costs, on average, about $70K per mile. To add the same bandwidth using DWDM by changing out the endpoint electronics costs roughly one-sixth that amount. There is clearly a financial incentive to go with the WDM solution.

Optical Switching and Routing

DWDM facilitates the transport of massive volumes of data from a source to a destination. Once the data arrives at the destination, however, it must be terminated and redirected to its final destination on a lambda-by-lambda basis. This is done with switching and routing technologies.

Switching versus Routing: What's the Difference?

A review of these two fundamental technologies is probably in order. The two terms are often used interchangeably, and a never-ending argument is underway about the differences between the two.

The answer lies in the lower layers of the now-famous OSI Protocol Model. You will recall that OSI is a conceptual model used to study the step-by-step process of transmitting data through a network. It comprises seven layers, the lower three of which define the domain of the typical service provider. These layers, starting with the lowest in the seven-layer stack, are the Physical layer (layer one), the Data Link layer (layer two), and the Network layer (layer three). Layer one is responsible for defining the standards and protocols that govern the physical transmission of bits across a medium. SONET and SDH are both Physical-layer standards.

Switching, which lies at layer 2 (the Data Link layer) of OSI, is usually responsible for establishing connectivity within a single network. It is a

relatively low-intelligence function and is therefore accomplished quite quickly. Such technologies as ATM; Frame Relay; wireless access technologies such as FDMA, TDMA, and CDMA; and LAN access control protocols (*Carrier Sense Multiple Access with Collision Detection* [CSMA/CD] and token passing) are found at this layer.

Routing, on the other hand, is a layer 3 (Network layer) function. It operates at a higher, more complex level of functionality and is therefore more complex. Routing concerns itself with the movement of traffic between subnetworks and therefore complements the efforts of the switching layer. ATM, Frame Relay, LAN protocols, and the *Public Switched Telephone Network* (PSTN) are switching protocols. The *Routing Internet Protocol* (RIP), *Open Shortest Path First* (OSPF), and *Internetwork Packet Exchange* (IPX) are routing protocols.

Switching in the Optical Domain

The principal form of optical switching is really nothing more than a sophisticated digital cross-connect system. In the early days of data networking, dedicated facilities were created by manually patching the end points of a circuit at a patch panel, thus creating a complete four-wire circuit. Beginning in the 1980s, digital cross-connect devices such as AT&T's *Digital Access and Cross-Connect* (DACS) became common, replacing the time-consuming, expensive, and error-prone manual process. The digital cross-connect is really a simple switch, designed to establish long-term temporary circuits quickly, accurately and inexpensively.

Enter the world of optical networking. Traditional cross-connect systems worked fine in the optical domain, provided no problems were happening in the O-E-O conversion process. This, however, was one of the aspects of optical networking that network designers wanted to eradicate from their functional requirements. Thus was born the optical cross-connect switch.

The first of these to arrive on the scene was Lucent Technologies' LambdaRouter. Based on a switching technology called the *Micro-Electrical Mechanical System* (MEMS), the LambdaRouter was the world's first all-optical cross-connect device.

MEMS relies on micro-mirrors, an array of which is shown in Figure 6-23. The mirrors can be configured at various angles to ensure that

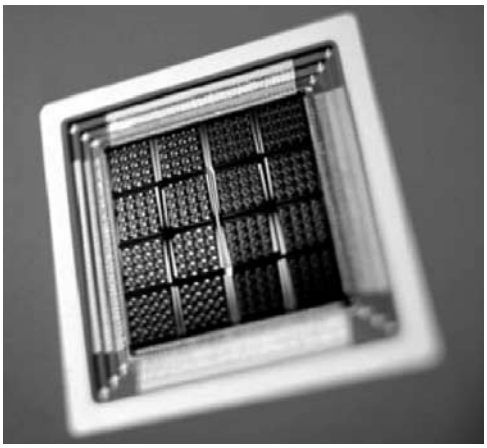


Figure 6-23
MEMS mirror array (Courtesy Lucent Technologies).

an incoming lambda strikes one mirror, reflects off a fixed mirrored surface, strikes another movable mirror, and is then reflected out an egress fiber. The LambdaRouter and other devices like it are now commercially deployed and offer speed, a relatively small footprint, bit rate and protocol transparency, nonblocking architecture, and highly developed database management. Fundamentally, these devices are very high-speed, high-capacity switches or cross-connect devices. They are not routers, because they do not perform layer-three functions. They will, however; all major manufacturers have announced plans to incorporate a layer-three routing function in their devices.

Thus, optical networking is a major component of the modern transport network. Together with switching technologies like Frame Relay and ATM, and Physical-layer standards like SONET, SDH, and copper-based transport technologies, the current network can handle the transport requirements of *any* traffic type while overlaying QoS at the same time.

CHAPTER 7

Final Thoughts

This is Paseo de la Castellana, a wide thoroughfare that runs through the center of Madrid's upscale business district. On both sides are ultra-modern buildings with gold-mirrored windows, designer shopping on the ground floors, and multinational tenants in the upper floors. There is money here.

The Castellana could be in any major European or Latin American city. It is more than 100 blocks long, very wide, and has three traffic lanes in each direction in the center divided by a wide island. The street used to be called Generalísimo after General Francisco Franco, but most references to him have long since been erased. On either side of the center lanes are express bus lanes, and outside the bus lanes are local traffic lanes. All of these are separated by landscaped traffic islands. The islands are 30 feet wide, heavily treed, and surrounded by low stylish wrought-iron fences. They give the street a European feel; it almost looks like a park with cars.

One 12-block segment is different, however. Among the shady trees and tall, full bushes, carefully enclosed by wrought-iron fencing, is a massive tent city (see Figures 7-1 and 7-2). Two thousand people live here, and they are all telecommunications professionals. The tent city is divided into regions named for the provinces of Spain, and each region is inhabited by people from that province. It contains sleeping quarters, washing areas, a swimming pool, meeting rooms, and even a computer room.

I came across this tent city during an early morning walk. To say I was intrigued is a bit of an understatement. The buildings, such as they are, are built from plywood with roofs made of plastic tarpaulins. Parked along the street are telephone repair trucks that have been converted into campers. The walls are covered with posters and graffiti that refer to Telefónica, the national telephone company, as a group of assassins and that blame Telefónica for the existence of this island of discontent.

Spotting a group of men sitting under a canopy drinking coffee, I walked over and asked them to explain to me the reason for their living conditions. They were immediately suspicious. I was an American, after all, but because I spoke Spanish and clearly knew something about their industry, they finally agreed to talk with me. Several times they left me to discuss what they were willing to say. Finally, they asked me this question: "are you neutral?"

"Yes," I replied; "I don't take sides." This seemed to satisfy them. Grabbing a piece of paper, one of the men (whom I later learned was in charge of the tent city) told me the story.

"Everyone here used to work for a telecommunications company called Sintel. We have been on strike for 250 days. Since January, we

Figure 7-1
The Sintel tent city.

have been camped out here, in front of the Ministry of Science and Technology and that of Economy and Finance. We are doing this since January 29th of 2001 to attract the attention of the public and denounce what we believe was the fraudulent sale of Sintel five years ago by Telefónica.

We call our community here the 'Camp of Hope.' It is more than a kilometer long and consists of 400 tents and shacks that we have built ourselves. Our message is simple: we want the back pay that is owed us, we want our company to be profitable again, and we want the government and Telefónica investigated because we believe that the company was sold fraudulently."

Later I went back to the hotel room and logged on to the tent city's Web site (Of course, they have one that tells the story; **http://galeon.com/comitesintel/En_Lucha.htm**). After browsing the material there

Figure 7-2
Another view of the tent city along the Paseo de la Castellana.

as well as information at Telefónica's site, I learned the following. Sintel came into being in May of 1975. It was the most important wholly owned subsidiary of Telefónica with 4,000 employees and annual sales of 62 billion pesetas (about $300 million). The company had contracts in Libya, Argentina, Chile, Venezuela, and a variety of other countries around the world, and a staff of 400 qualified engineers to do the work. The company was basically a wholly owned plant-engineering firm.

In March of 1996, Telefónica sold its shares in Sintel to the Mastec Company, a Miami-based corporation with strong ties to the anti-Castro movement in the United States and a strong financial supporter of Spain's current leadership, headed by José María Aznar.

My host now continued his story with greater fervor: "the sale of our company was done under complete cover. No prior notice was given to the union. Both Telefónica and Sintel were financed with public money, so the sale was the responsibility of the government. They should have been obligated to tell us of their intentions. The company was sold for 4.9 billion pesetas ($25 million), a steal at that price. Mastec had to pay for the sale over a three-year period, which they have not done. Furthermore, Telefónica retained ownership of all the Sintel offices and warehouses, leaving the company undercapitalized and without tangible assets.

Since 1996, Telefónica has strangled Sintel. Even though the company still does business with Telefónica, it has reduced the prices it pays for jobs and employees have been laid off in 30 provinces. Furthermore, the company refuses to pay for work that has already been done, and we're

talking about more than 6 billion Pesetas. What we want is simple: we want the unions, Telefónica, and the government to sit down together around a table so that we can reach an agreement to save Sintel from the serious plight it is in and figure out a way to pay these people the nine months of wages that are owed to them. It's only fair."

These people are trapped between the jaws of a vise made up of government, union, philosophical, political, economic, and historical forces. Until five years ago, Spain was led by the *Partido Socialista Obrero de España* (PSOE), the Spanish Socialist Labor Party. In keeping with its political leanings, the party was pro-labor and union, anti-growth, and anti-big business. As Spain marched inexorably toward membership, and potentially a leadership role, in the *European Union* (EU), the need for growth and political change became real, and in 1996 the center-right Popular Government Party was elected to lead the country. The left was out; the center-right was in. The new government is more business and growth-oriented and encourages less government intervention. This represents a major change in the philosophical leanings of the country's leadership and is hard for companies accustomed to life under a left-leaning government to accept.

NOTE: *In early August 2001, as we went to press with this book, the Castellana tent city was in the process of being dismantled. The Spanish government, Telefónica, and the Sintel unions came to an agreement to pay some of the back wages, arrange for early retirement for a portion of the affected employees, and seek alternative employment for others.*

What a fascinating world this is. On the one hand, seriously disadvantaged people in Brazil make the most of their situation by using the Internet to overcome the challenges of looking for work in an economically and socially stratified country, never losing sight of their desire to get out of the slum they live in. Meanwhile, telecommunications professionals in Spain advertise their plight, caused by a business deal gone bad, by creating a tent city in the middle of the financial district of Madrid and decorating it with inflammatory posters and graffiti. All over the world the Internet has taken center stage as a primary driver for social change. Those who can't get it at home can always go to an Internet café like the one in Madrid shown in Figure 7-3, or those owned and operated by my taxi driver from the Ivory Coast.

Figure 7-3
An Internet café in Madrid near the royal palace.

There was a time when telecommunications was invisible. It manifested itself as telephony, and telephony was taken for granted; it was just there. No one ever stopped to think about life without it, *because it was always there.* Colleges and universities offered courses and degrees in computer science, but few if any of them offered courses (much less entire degree programs!) in telecommunications. That was the domain of the telephone company.

All that has changed, of course. Today telecommunications is the fastest growing and most dynamic professional field on Earth (yes, even in spite of the telecom meltdown of 2000) and is the degree program in greatest demand among technical majors. It's real. It's happening. It's the place to be.

And why? The answer is actually rather simple. As I observed in the introduction of this book, *I defy you to find me an industry that is not inextricably dependent upon telecommunications technologies for its very livelihood.* Don't try, because you won't succeed. And if by chance you *do* find one, I'll show you a business that is either on the verge of failure or so economically and geographically isolated that its success or failure is, to put it bluntly, immaterial.

When William wrote his message to me from Kenya, thanking me (and the Internet) for helping his business to succeed, I realized something important. The global telecommunications network is evolving to provide universal connectivity for every country on Earth, and every business and person in those countries. It is no longer a technological extravagance, available only to the rich; it is a global economic impera-

tive. Countries, companies, and individuals that want to play a part in the world's economy *must* be connected or they can't play. It really is that simple—and complex. Connectivity will bring about massive social change, economic tectonics, and a profound and utter redefinition of the way countries view each other. States seen today as third-rate backwaters may well become innovative powerhouses in the same way that Cisco, AOL, and Siebel came out of nowhere to become guiding forces in their own industry, helping to shape and direct it.

Many believe that telecom infrastructure development cannot succeed without sophisticated governments running the countries in which it is deployed. There is an element of truth to this, of course; far more important, however, is the opposite: *governments cannot succeed without sophisticated telecommunications infrastructures in place.* Furthermore, oppressive governments are often driven to failure because of the overwhelming force of telecommunications-based communications applications.

Not all that long ago, some of the more extreme Middle-Eastern countries referred to the United States as the evil empire. Today they have shifted that name to CNN because of its unique ability to communicate to their oppressed populace news of the rest of the world, and most importantly, hope: hope brought about by an understanding that there are places where people are free to live without fear of reprisal for the simple act of speaking out against abuses of human rights. Satellite dishes in some Middle Eastern countries have been banned because of their ability to freely expose people to other people, cultures to other cultures. When the Tiananmen Square crisis occurred in 1989, guards were placed at public telephones and fax machines to prevent word getting out about what was happening.

Some military analysts are concerned about the rising military power of Russia and China. They express fear that these countries could mount a serious military or economic threat given their size and power. I disagree: I believe that these countries may Balkanize long before they become major economic or military powers, simply because they have no telecommunications fabric of any consequence to hold the country together. Without effective communications, there really cannot be a single, cohesive, organized country with a sense of self or purpose.

In July of 1919, a young army captain named Dwight David Eisenhower joined other members of the army on an overland trip from Washington D.C. to San Francisco. Because of poor roads, the caravan averaged five miles per hour and took 62 days to cross the country.

At the end of World War II, Eisenhower, now a General, found himself impressed by Germany's Autobahn. A single bomb might destroy a train route, but Germany's highways could often be used soon after being bombed because it was difficult to destroy such a wide area of concrete or asphalt and because numerous alternate routes existed that could be used.

Within a year of becoming President in 1953, Eisenhower began to push for a system of interstate highways that would crisscross the United States. Although federal highways already covered many areas of the country, they were old and often narrow. The interstate highway plan would create an additional 42,000 miles of modern highways.

Eisenhower worked for two years to gain Congress's approval of the largest public works project ever conceived. On June 29, 1956 the Federal Aid Highway Act was signed and the interstates began to appear. The standards for the highways were carefully designed and highly regulated. Lanes were required to be 12 feet wide, shoulders had to be 10 feet wide, bridges required a minimum of 14 feet of clearance, grades had to be less than 3 percent, and the highway had to be designed for travel at 70 miles per hour. The plan for the Interstate Highway system was to complete all 42,000 miles within 16 years. In reality, it took 27 years to complete the system. The last link, Interstate 105 in Los Angeles, was not completed until 1993.

Similarly, when President Roosevelt signed into law the Communications Act of 1934, he did so with the following stated goal:

> For the purpose of regulating interstate and foreign commerce in communication by wire and radio so as to make available, so far as possible, to all the people of the United States a rapid, efficient, nation-wide, and world-wide wire and radio communication service with adequate facilities at reasonable charges, for the purpose of the national defense, and for the purpose of securing a more effective execution of this policy by centralizing authority heretofore granted by law to several agencies and by granting additional authority with respect to interstate and foreign commerce in wire and radio communication, there is hereby created a commission to be known as the "Federal Communications Commission," which shall be constituted as hereinafter provided, and which shall execute and enforce the provisions of this Act.

All commerce depends on transportation, whether for the physical movement of goods or the logical movement of information. In *Being Digital*, author Nicholas Negroponte observes that we are rapidly evolving to a world where more and more, we make money not by shipping

atoms around, but by shipping *bits* around. He's right, of course. Online commerce, Internet banking, and other examples of electronic trade are legion, and growing. We still have to ship lettuce and squash out of California's great Central Valley by truck, but more and more of those lettuce and squash crops are being sold online to Asia, Europe, South America, and the Middle East. Why? Because they can be. And as the business evolves, so too evolve the players in the business.

The Telecom Players: Where Are They Going?

The telecommunications industry was so *simple* in 1984 when divestiture struck. There were seven *Regional Bell Operating Companies* (RBOCs), *three long-distance companies* (*Interexchange Carriers* [IXCs]), and customers. Today there are at least three IXCs, three-and-a-half *Incumbent Local Exchange Carriers* (ILECs) (formerly RBOCs; the half is USWest, acquired by Qwest), a host of *Competitive Local Exchange Carriers* (CLECs), and a plethora of *Internet Service Providers* (ISPs), cable providers, *Data Local Exchange Carriers* (DLECs), *Building Local Exhange Carriers* (BLECs), *Application Service Providers* (ASPs), and more manufacturers than can be counted. Also, specialized carriers have been around like Rhythms NetConnections and Covad, both of which gambled on technology (DSL) as their principal deliverable and found that the market wasn't there.

Hardware manufacturers have also learned a painful lesson: customers as a general rule are not in the market for whiz-bang technology. They are in the market for communications solutions that make them and their companies more competitive. The heady days when customers could be wowed by bit rates and chip speeds are over. Today those customers are looking for performance and reliability. Remember the days when the process of buying a car always included the obligatory look under the hood? Not anymore. How many cylinders does your car's engine have? Is it carbureted or fuel injected? Disk brakes or drums? For the most part, those details are no longer important. What matters is that the car is reliable and has the functional features the driver wants.

Telecom has evolved to the same place in its evolution. It doesn't really matter anymore how it works; what matters is that it *does*. Period.

A Look at the Crystal Ball

You have now reached the end of this book, so I'd like to offer a summary of sorts that will put everything we've covered into perspective.

This industry is in a state of great change at the moment. Consider the graph in Figure 7-4, which plots price against features. This relationship provides a valuable tool to assess the relative success of players in the telecom industry, because it uses two very important characteristics: feature offerings, which are most important to the customer, and price, which is most important to the provider of those features.

Let's examine the long-distance providers as examples of how to use this chart. For the most part, the long-distance providers are squarely housed in the lower-right quadrant of the graph where prices are high and features are nonexistent, yet the providers are moving to the lower-left quadrant where feature-richness is still lacking, but the price is dropping. Little movement upward exists, however. For the most part, they have not enhanced their service offerings much beyond transport. As circuit switching in the long-distance space inexorably gives way to packet-based transport, prices for transport services will plummet. Without a basket of value-added services, the long-distance players will be relegated to being participants in a game of who's-got-the-cheapest-prices, a game none of them are particularly excited to enter.

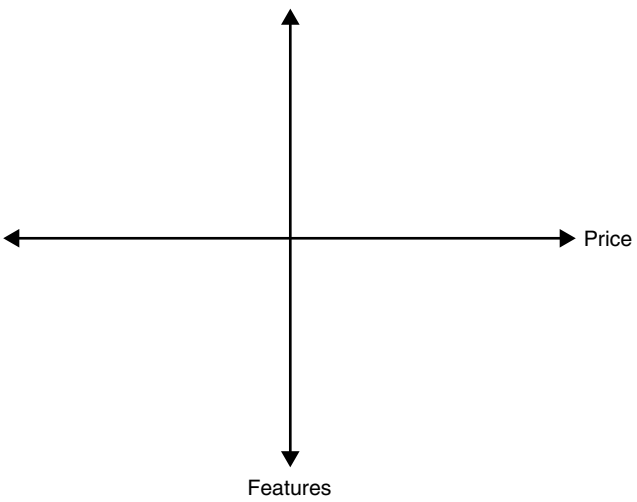


Figure 7-4 Graphing features against price as a way to assess performance.

What about wireless? In the last few years, they have made the same move from right to left and are just now beginning to toy with the idea of also moving into the upper-right quadrant by adding services.

Customers are rather elastic in terms of what they are willing to pay for telecom services. As long as they perceive value, they will pay more. I often tell people the following statement: "I am going to offer you a new service. The service isn't as good as the service you've become accustomed to over the years, but it does have one advantage: it costs more." I then ask how many would be willing to buy the service. Of course, no one raises their hand. I then observe, "So, none of you has a cell phone, eh?" After all, cellular service for the most part costs considerably more than wireline service, and the quality is *absolutely* inferior. Yet people buy it by the thousands of minutes per month. Why? Because there is tangible, perceptible value in the convenience of mobility, and subscribers are willing to pay more for that added value while at the same time accepting the tradeoff of quality for the convenience of mobility.

The secret to success is this: quality and value must be measured from the perspective of the consumer of the service, not from that of the provider of it. For many years, the monopoly telecommunications industry *told* customers what they wanted and defined the *quality of service* (QoS) for them. And the customers, because they had no choice, listened, smiled, and liked the service—because they were told to. It was a case of the Emperor's New Clothes that brought things crashing down. With divestiture came competition, and with competition came innovation, and with innovation came reduced prices for services. Now that they had freedom of choice, customers could make their own decisions and issue their own dictates about the characteristics of quality, reliability, and reasonable cost. The service providers clamored for a long time following divestiture for open, aggressively competitive markets, and now that they have them, they are realizing the pain that comes from the old adage, "be careful what you wish for—you might get it."

This industry is in its early adolescence. The players are strong, full of energy, and laden with ego and possibility. The customers, who in many ways are playing the role of the responsible adult, are watching carefully to see where they're being led. They're willing to give the industry players plenty of leash because they know that good things inevitably come from all that energy.

I often hear people say that "the telecom industry is bust; the boom is over." What in the world are they talking about? Are we through communicating? Is it time to move on to something else now? For crying out loud, we have been building telecommunications infrastructure

unceasingly since the end of the nineteenth century. This latest little burble is exactly that, a hiccup that resulted from too much money, not enough return on investment, and accelerated timeline expectations. "Underpromise, overdeliver" somehow got inverted, and the result was a financial backlash. The forward movement is far from over, however. The telecom industry is just now building up a head of steam, and corporations and countries the world over are beginning to realize the potential of telecommunications infrastructure within their future plans.

So what *is* coming down the road ahead? Here are a few of my own predictions. I read a lot of market tea leaves, so these predictions are based on a considerable amount of market awareness. However, in the words of Dennis Miller, "it's just my opinion—I could be wrong."

The Internet's influence is far from over. In these times of cost-cutting and economic stringency, the Internet will play a key role. Business-to-business and business-to-consumer sales via the Internet already enable cost reductions in the neighborhood of 5 percent. Furthermore, the belief that primacy rules supreme with regard to the Internet is spurious. Those companies that took their time and proceeded slowly and carefully have prospered, while those that went in with little heed are largely gone today. Those companies that tried to become pure-play Internet companies have largely failed for the simple reason that they failed to understand what consumers were looking for: solutions and advantages.

Broadband access will continue to be important. Both DSL and cable modem connections will continue to enjoy sales for the near term, but over time, fixed wireless will overshadow both of them because of its lower infrastructure cost and soon-to-be-available high-bandwidth, two-way symmetric service.

In spite of the hype, 3G doesn't cut it. Third-generation (3G) wireless is a nice idea, but it is a technology looking for a problem to solve. All the bandwidth in the world doesn't do much for the consumer if no applications are available to take advantage of it. The mini-browsers that accompany many digital cell phones today are cute but frankly worthless for the most part: advertised as "the wireless Internet," they're not even close. According to various studies, the average number of screens a user has to go through on a minibrowser to reach the site they're looking for is 22. Calling *that* the wireless Internet is a major marketing blunder; the Internet connotes speed, a large screen, color, and universal access. Until applications emerge that are specifically built around the concept of high bandwidth to the cell phone and the known limitations of a mobile device, 3G will flounder.

Final Thoughts

Recently, while teaching in Europe, I asked a group of 50 people what they wanted from their mobile 3G services provider. The answers were voiced almost in *a capella* harmony: low cost, secure communications, universal access, reasonably good signal quality, and instant messaging. No fancy Internet access, no color graphics, just solid communications capability. Europe already has this, you see. It's called *Global System for Mobile Communications* (GSM). Perhaps the North American service providers should pay attention.

Hand-in-hand with the evolution of wireless will be a concomitant evolution in the design, deployment, and use of mobile appliances that are actually useful. They will incorporate wireless connectivity, but will be designed *not* to replace the PC or laptop, but rather to provide spontaneous, just-in-time connectivity to online databases. Coupled with ubiquitous connectivity and adequate bandwidth, these devices will herald the arrival of a new wave of mobility. And they will be built around the functionality that the customer wants to use, not what the technologists want to deliver.

The players in the game will continue to evolve in terms of who they are and what they do. As the adolescent companies in the telecom industry grow up and become young adults, they will set aside childish things and focus on serious business. They will narrow down their business activities and focus on those that they do well and which make money. They will recognize that they will only make money if they satisfy the demands of the customer, and they will satisfy the demands of the customer if and only if they pay attention to that customer. The herd will be further culled; the numbers will drop. Those that remain will be those that have the wherewithal to change their business practices on the fly to match changing customer requirements.

Consider the following quote from Tom Peters' *In Search of Excellence:*

> Probably the most important management fundamental that is being ignored today is staying close to the customer to satisfy his needs and anticipate his wants. In too many companies, the customer has become a bloody nuisance whose unpredictable behavior damages carefully made strategic plans, whose activities mess up computer operations, and who stubbornly insists that purchased products should work.

Convergence is real and it's only just begun. The move to a single-network fabric for the transport of multiple service types is underway and *will happen.* However, the imminent demise of the circuit switch is exaggerated. In the local market, these devices will be around for some time

to come. In the long-distance business, where packet transport over high-bandwidth optical facilities simply makes sense, the displacement process will occur much faster. Furthermore, the convergence of companies continues apace as they jostle each other for the pole position in the services and solutions provisioning game.

The functional migration from the edge of the network to the core is underway. A redesign of the network is in progress as intelligence migrates from the core to the edge. The closer network resources are to the customer, the more those resources can be customized to meet their dynamic demands. As long as resources are concentrated in the core, customers tend to be treated like commodities. In this age of service focus, that philosophy is deadly.

A new regulatory environment is needed and will happen. Darwin was right: only the fittest members of a species survive, thus enabling hybrid vigor. Darwinian evolution is alive and well in the telecommunications business and only the fittest will survive. Fittest, of course, is a measure of the degree to which a company meets customer demand through the proper and judicious deployment of new technologies as a way to offer competitive advantage. Although there will always be a need for protection against predatory, anti-competitive behavior, an open marketplace with minimal regulation is wise and necessary. Contrived competition and protectionism are bad things and do nothing to prepare companies for a truly competitive environment. Thus, regulators will become guidance agencies, tasked with the responsibility to work themselves out of a job as the industry becomes more and more independent.

The metro environment will become a central marketplace in the next three to five years. Metropolitan networking is undergoing a huge growth spurt in response to changing customer business models. Long-haul networks are largely complete and offer massive overcapacitization of bandwidth. In the metro space, however, bandwidth is in short supply and, where available, is inflexible. New technologies deployed by metro-focused companies such as Yipes! And Telseon will change the metro space and expand it as a viable and lucrative market for service providers and manufacturers alike.

Globalization is real, painful, and necessary. According to a recent article in *The Economist,* globalization today is largely dependent upon falling telecommunications costs. As the costs of optical transmission, Internet and telephone connectivity, satellite deployment, switching centers, and semiconductors plummet, the degree to which these technologies can be used to weave a tighter and more cohesive global communications fabric becomes greater and greater. Low-cost communi-

cations means that emerging countries can play in the information services game for a comparatively small investment.

Is there a downside to globalization? Absolutely—change is painful and must be monitored closely to eliminate abuses during the change process. More good than bad will take place, however, and because the process is inevitable, a prudent, informed acceptance is safer than ignorance and avoidance.

So what is the message of this book? There are several, really. First, telecommunications is the interstitial tissue, the systemic fabric that more and more weaves the world together. Second, it does so because it can. Yes, there's a downside to the homogenization that occurs with globalization (which is in turn accelerated by the proliferation of telecommunications technologies) and the potential for the loss of some degree of national identity.

However, as I said a moment ago, a powerful upside outweighs the downside. I am writing this on the balcony of a small apartment in the pueblo of Majadahonda, just west of Madrid. When I lived near here 20 years ago, the road below me was not paved, and my brothers and I used to run with the bulls down this road during bullfight season. The stores were small, dark establishments that sold a few things, typically whatever they were able to get that day.

Now I look out across the same street, now paved, and see a Gap, a Tony Roma's, a Toys 'R' Us, a United Colors of Benetton, and a sign for Burger King somewhere down there around the corner. But about the time I start to get that deep-seated sense of loss, I look across the street, and there, sitting in a loosely cobbled together collection of ancient plastic chairs, are four old men playing cards, just like they did when I lived here. Above their heads is a satellite dish and sitting at the table adjacent to them are two college students with laptops, one of them accessing the Internet via a wireless modem and both drinking lattés.

So, although things have changed here and in Africa, Asia, Latin America, and the Middle East, the important things have not. Technology has helped create opportunity, wealth, an end to poverty, and hope. And although it may be difficult to see the old culture buried beneath all the glitz of technological globalization, it's still there, and it doesn't take the Web to find it.