II. Understanding the Concepts

CHAPTER FIVE

Data Transfer Rates: A Primer

You've probably seen them. Ks, Ms, and Gs. They're always used in computer ads: 56K, 6.4GB, 32MB. Sometimes they have other letters after them, like Kbps or MBps. But what do they mean?

Discussing network connectivity requires one to establish a basic vocabulary of data transfer speeds. Data transfer is the process of moving *computer data* from one point to another. The speed, or rate, of that movement is called the *data transfer rate*. There is a more common word used to describe this measurement also: *bandwidth*.

Data transfer is the process of moving computer data *from one point to another. The speed, or rate, of that movement is called the* data transfer rate.

Bandwidth

Bandwidth is a term borrowed from the world of wireless transmission, such as TV or radio broadcasting or ham radio. Bandwidth refers to the frequency width of a particular band of radio transmission. For example, the VHF television band extends from the 54 megahertz frequency to the 216 megahertz frequency. The width of that band is 216-54, or 162 megahertz.

Electrical signals are carried over network cables at different speeds depending on the frequencies used on specific wire types. So the term bandwidth is used in the computer networking world as well. In networking it is used to describe the maximum amount of data that can be transmitted across a medium in one second.

Other terms used commonly to describe this same measurement are line speed, throughput, and capacity. In this chapter I've used data transfer rate as a more descriptive phrase. These terms are used interchangeably in many

networking discussions although they have slightly different technical meanings.

The basic unit of storage in a computer system is the bit. A secondary unit is the byte. Bandwidth is normally measured in some form of bits-per-second (*bps*). Since the number of bits that can be transmitted through most media can be quite large, researchers and technicians use common abbreviations for large numbers. These are the Ks, Ms, and Gs we mentioned up front. Before we get to them, though, let's examine those two words I just threw at you: bits and bytes.

Bits and Bytes

Bandwidth is normally measured in some form of bits-per-second, abbreviated bps.

While computers can do some amazing things, they are fundamentally simple machines. In fact, they do just a few simple things: they recognize two states of electrical current (high and low); they recognize magnetic polarity (North and South); they "open" and "close" gates; they shift bits left and right. Out of these four basic operations come all the number crunching and visual operations we've come to expect and demand from them.

Since computers only recognize distinct states of electrical current and magnetic polarity, all data used by computers—letters, numbers, punctuation marks, pictures, and sounds—must be represented by using a series of two symbols. This type of system, where only two single values are possible, is known as a binary system. In mathematics, the binary (base 2) number system describes a binary system using two digits, 0 and 1. All counting is accomplished using just these two symbols.

(Obviously, this is not the counting system people use! We have ten fingers and ten toes, so our number system is based on having ten different counting symbols, or digits. This number system is called the *decimal* [base 10] number system.)

These symbols are called *binary digits*, or *bits* for short. They represent the smallest unit of storage on a computer. In order to program a computer to operate on textual data (letters, numerals, punctuation marks, and other special symbols), a binary code was necessary. Because storage space was very expensive in the early years of computers,

the code needed to provide enough symbols but not waste storage space. Eventually, a coding system using a sequence of eight bits was designed (eight bits provides up to 256 different text symbols). Because most computer data is textual in nature, the eight-bit sequence became a very common unit of storage. It is called a *byte*. Each letter in a document required one byte of storage. Oddly enough, because the byte became so prevalent in storage measurements, the sizes of even non-text objects like graphics and sounds are now expressed in bytes.

So, when measuring data transfer rates and storage sizes, different values are used. Bits are typically used in data transfer rates, and bytes are used to indicate storage space. A lowercase b is used to signify bits. An uppercase B is used to signify bytes. (In a few data transfer rate specifications—mainly for hard drives and tape drives—a byte value is used instead of bits. One can always see the difference in the symbol used, Bps instead of bps.)

If you'd like to see an example of how textual data is stored on microcomputers, read the sidebar "Encoding Text." Otherwise, let's get started on those Ks, Ms, and Gs.

Large Units

A 20-page word-processed document might take up 60,000 bytes or more of storage space. A small photograph on a web page might take up as many as 100,000 bytes. In most cases, measuring storage space or transfer rates requires large numbers. To make the notation of these measures easier, a series of unit abbreviations have been commonly used.

The letter K (for "kilo") is commonly used to indicate 1,000 units (e.g., kilograms). However, with computers such a number is not really a "round" number. The closest "round" number in the binary number system is 1,024. So, computer scientists have adopted the K designation as a substitute for 1,024 units. This symbol is combined with the proper computer unit used to create a complete measure: Kb for *kilobits* and KB for *kilobytes*.

Likewise, the letter M (for "mega") represents a million units. Once again, one million is not a "round" number in the binary number system, so the exact measure is a little

Encoding Text

Over two decades ago, the American Standard Code for Information Interchange (ASCII) was developed for microcomputers. This code uses numbers to represent letters, numerals, and punctuation marks. ASCII uses eight bits (binary digits) to provide up to 256 different characters. This unit of eight bits is called a *byte*. Each is numbered (in our decimal system) from 0 to 255. Here are a few examples, with their assigned decimal values and binary codes:

Char	Decimal Value	Binary Code
(space)	32	00100000
,	44	00101100
.	46	00101110
0 (zero)	48	00110000
A	65	01000001
Z	90	01011010
a	97	01100001
z	122	01111010

To see how unsuitable binary code can be for people, look at the word "computer" represented in binary:

01100011011011111011011010111000001110101
01110100011001010111001 0

This eight-letter word takes 8 bits per letter x 8 letters = 64 bits to represent in binary.

Common Abbreviations

Base units:

b = bits
B = bytes

Large units:

K = kilo (~thousand)
M = mega (~million)
G = giga (~billion)
T = tera (~trillion)

Rates:

bps = bits per second
Bps = bytes per second
Hz = cycles per second

Units of Storage:

KB = kilobytes
MB = megabytes
GB = gigabytes
TB = terabytes

Data Rates:

Kbps = kilobits per sec
Mbps = megabits per sec
Gbps = gigabits per sec

Radio Frequencies:

KHz = kilohertz
MHz = megahertz
GHz = gigahertz
THz = terahertz

more: 1,048,576 (1,024 x 1,024). Mb stands for *megabits*, and MB stands for *megabytes*.

In general discussions of storage requirements, we tend to use the round number we're familiar with: 1,000 and 1,000,000. For example, when an advertisement says a Zip disk holds 100MB of data, it really means about 100 million bytes, not 104,857,600 bytes (the technical value represented by 100MB). Data transfer rates are quoted using the same rounded numbers.

Over the past three years, even larger quantities of hard drive storage products have become common. And a new, very fast networking technology has emerged into high-end applications. These products have *gigabyte* and *gigabit* specifications, respectively. "Giga" indicates approximately a billion units. We use the letter G to represent this unit. For purists, a gigabit equals 1,024 x 1,024 x 1,024 = 1,073,741,824 bits. Wow!

Gigabit Ethernet networking is being used primarily where high-end graphics applications and huge data sets are used. Schools and libraries probably will not use this level of networking until real-time, high-quality desktop video is common. Such use would include distance learning, conferences, and others.

Now you know the basics for decoding all the data transfer rates you'll run across in reading computer magazines or books. But we have talked about these transfer rates in numbers that are basically meaningless. The addition of some perspective might be in order. What does 1Mbps really mean? How much *stuff* is it?

A Picturesque Perspective

It's time to put data throughput in terms we're familiar with. Let's start with some basic, common transfer rates and build mental pictures.

Most home computer users have a modem providing a data transfer rate of at least 28.8Kbps. Some have newer 56K modems. Some still have older 14.4Kbps modems. It turns out that the latter is a very convenient and meaningful number.

Remember when we used to type all our documents on a typewriter? An 8½ x 11 sheet of paper had a one-inch margin on the left and right sides, top and bottom. An extra half-inch at the top of the page was used for a page number and heading. Most typewriters we used had a Pica typeface, which put ten characters per inch across the page. Usually the lines were double-spaced. This provided about 26 typed lines per page, with about 65 characters per line—a total (26 x 65) of 1,690 characters per page. Do you remember how many bits it takes to represent a character? (If you said eight, give yourself a reward!) 1,690 x 8 equals 13,520 bits. Add a few hundred bits for the packaging required to send data across a network and you end up with a number very close to the per-second speed of a 14.4Kbps modem.

This gives us a nice mental picture. One normal, double-spaced page of text takes about one second to transfer with a 14.4Kbps modem. A 28.8Kbps modem can transfer about two pages per second. And the very latest technology, at 56Kbps, can transfer about four pages per second. Let's extend this picture to something else we can visualize.

One normal, double-spaced page of text takes about one second to transfer with a 14.4Kbps modem. A 28.8Kbps modem can transfer about two pages per second.

I read Tom Clancy novels. What about one of those two-inch-thick, hardback titles? Just for fun I estimated the number of characters contained in *Without Remorse*, one of Clancy's books that appears to be about "average" length. It has about 1,484,000 characters in it. Converting that to bits, we get 11,872,000 bits. So, how long will it take to transfer one Tom Clancy novel at 56Kbps? 11,872,000 bits / 56,000 bps = 212 seconds (or, 3.53 minutes).

In contrast, let's look at just *one* photograph the size of a common computer screen and stored in "real color" format. Just one requires 640 dots x 480 dots x 24 bits per dot = 7,372,800 bits to represent. Wow again! This photograph will take 132 seconds (2.2 minutes) to download at 56Kbps. So how long would the digital equivalent of a coffee table book of medieval art, with a hundred pages of photographs, take to download? Even with current technology that compresses photographs into smaller files, this would be a very intensive download. This shows why Gigabit Ethernet has become popular in certain fields relying heavily on graphics and motion video technologies.

Table 9 on the next page shows a comparison of the common data communication technologies. The "X" column shows how many times faster a specific technology is

compared to a 28.8Kbps modem (considered the benchmark for our purposes). Or, you can look at it as a statement of how many 28.8K modems are required to equal the performance of the specified technology. The download column indicates how long, in seconds, it takes to transfer our reference document, a Tom Clancy novel, using each technology.

Table 9. Comparison of Data Transfer Rates.

Speed	Description	X	Download Time*
300bps	Original PC Modem	$^1/_{96}$	39,573.33
9600bps	Fax Machine	$^1/_3$	1,236.66
14.4Kbps	Slow Modem	$^1/_2$	824.44
28.8Kbps	Regular Modem	1	412.22
56Kbps	Fast Modem	1.94	212.00
128Kbps	ISDN line	4.44	92.75
384Kbps	Fractional T-1 Data Circuit (Common)	13.33	30.92
1Mbps	Typical Wireless Network	34.72	11.87
1.54Mbps	Full T-1 Data Circuit	53.47	7.69
5Mbps	High-End Wireless Network	173.61	2.37
10Mbps	Ethernet Network	347.22	1.12
45Mbps	T-3 Data Circuit	1,562.50	0.26
100Mbps	Fast Ethernet Network	3,472.22	0.11
1Gbps	Gigabit Ethernet Network	33,472.2	0.01

* the theoretical time for the reference document at a given line speed; actual download times will be slightly longer

CHAPTER SIX

Building a Local Area Network

Before we can really begin talking about wireless data communications, let's take a step backward and discuss how computer networks work. At this point neither of us has time for a complete study of the subject—that's what college classes are for. So we'll run through just the basics here, one at a time.

Specifically, we'll review all the parts that make up a basic computer network, one that connects the computers in a single location (building or department). Such a network is called a *local area network*, commonly referred to by its acronym, *LAN*. When we finish, you should have the basic knowledge you need to be ready for your next discussion of computer networking.

The purpose in creating local area networks (LANs) is to allow multiple computers to share resources that would be too expensive or impossible to provide for every computer user.

How Computers Converse

The purpose in creating computer networks is to allow multiple computers to share a resource that would be too expensive to provide for every computer user. For example, instead of buying one printer for every computer, an agency might buy a single, high-speed, high-quality laser printer and install it on a computer network. Every computer connected to the network could potentially have access to the centralized printer (agency or departmental *network policy* determines who can use a centralized resource and a *network administrator* configures each computer in accordance with the policy). This generally saves money and allows the agency to purchase a higher quality product.

In order for several computers to share limited resources, there have to be rules in place for communication. It's like having a human conversation, except that most of our "rules" are taken for granted. Let's think about a

conversation for a moment and look at the rules in place governing our communication.

First, we have to agree on a language to use. In this book's context, we've chosen English. Secondly, we have to formulate rules of transmission "right of way." We recognize that the two people conversing can't both talk at the same time. (Not that we don't try to at times!) So some rules, usually unspoken but learned through experience, are in place. For example, if I'm impatient to make a point, I may begin to utter a sentence only to stop when I realize that the current speaker is not finished. Or perhaps another person might barge in before I can begin. The original speaker may take this as a sign to yield at an opportune moment and give me a chance to ask a question or make a point. In more formal situations we may be required to raise a hand to indicate we would like to interrupt to make a point.

In computer networking, the rules for the "language" used and for the process of starting, interrupting, and continuing communication are called network protocols.

In computer networking, the rules for the "language" used and for the process of starting, interrupting, and continuing communication are called *network protocols*, or just *protocols*. In order for a computer to participate in a network of computers, the same protocol software must be installed on each computer. Computers communicating over the Internet use a specific protocol called *TCP/IP*. The same computers can participate in a local area network using a different protocol, such as *IPX* or *NetBEUI*.

How the Signal is Transmitted

When we carry on a conversation, the words of our speech are carried over a *communications medium*—specifically through the air around us as sound waves. Our vocal cords and mouth form and transmit the sound waves, and our eardrums receive the sound. (This is, by the way, a very good demonstration of a *wireless* communication.) But the range of communication is limited, usually to several hundred yards. How loud we can yell (amplify the signal) determines how far the signal will travel as an identifiable sound before it degenerates into something unintelligible. The power of our lungs has a direct bearing on how much the signal is amplified.

On the other hand, let's say you want to speak to a friend in Milwaukee. You will have to use some form of wired connection—a telephone. The wired infrastructure inten-

sifies or amplifies your voice at various points along the wire so that your friend in Milwaukee hears your voice as if you were in the same room. If the sound is not transmitted very well, you can use an amplifier in your phone set to increase the "gain" of the signal, making the signal louder in your ear.

So whether close or far away when we carry on a conversation, we need several components in place to communicate with each other:

- lungs, vocal cords, tongue, teeth and lips to transmit a signal
- the air (or some other medium) to carry the sound vibrations (signal)
- ears, including the eardrum and the fine bones of the inner ear, to receive the signal.

Like humans, computers need the same type of components: a transmitter, a transmission medium, and a receiver. In the next section we discuss the various physical components required to create a computer network.

In order to get a computer connected to a network, a network interface card *must be used.*

General Network Equipment

Network Interface Cards

Which is the most basic component of a computer network: the interface card, the transmission medium, or the protocol drivers? It depends on one's philosophy. We'll tackle the interface card first.

In order to get a computer connected to a network, a *network interface card* (also called a *NIC* or *network card* for short) must be used. This is just another of the green electronic circuit boards you've grown used to seeing around computers. This particular circuit board has one or more port connectors attached to one end. The port extends to the outside of the computer case, on the rear panel.

The most common port looks just like a modular telephone jack, only a little larger. This connector is for an eight-wire cable (a regular telephone jack has only four). Technically it's known as a RJ-45 jack. Another common port looks like a silver barrel, not quite a half-inch in diameter. This con-

nector is called BNC port. The type of port your network card requires is determined by the cable type you use for your network. We'll discuss this in more detail in the next section.

The interface card has programming contained on it that provides several network functions, including transmission and reception of network signals. The interface card prepares the data and transmits it over a transmission medium. It also receives any network signals coming to the computer in which it is installed. It converts the signal to the data originally sent and makes it available for use on its host computer.

The network protocol software mentioned above and the computer's operating system software must work very closely with the network interface. This is accomplished by a third piece of software called a *driver*. A driver is software written specifically for a particular manufacturer's network interface card, allowing the network operating system to control (or "drive") it.

Common Cabling Types

Cabling doesn't really fit in the category of equipment, but it is one of the physical components required to create a network. The cable connects to the network interface card and, usually, to a centralized network device called a *hub*. We'll discuss the hub in the next section.

Coaxial. One of the oldest cable types for computer networks is thick coaxial cable, such as the type used in your cable TV connection. This cable is designated as 10Base-5 cable. While there are some good reasons to use regular coaxial cable, it has fallen out of general use in favor of fiber optic cable. We'll give it short shrift here.

Thin Coaxial. Sometimes called *thinnet cable*, thin coaxial cable gained great popularity is small, departmental LANs in the late 1980s. It is designated as 10Base-2 cable. Thinnet cable is more pliable and is much easier to install and maintain than regular coaxial cable. There are still many LANs partially or completely configured with thinnet.

The most serious drawback to thinnet is that it limits to 30 the number of computers that can be connected to a network without requiring additional, expensive equipment.

Once thirty computers are attached to the network, a repeater, costing several hundred dollars, is required to extend the LAN and attach additional computers. Also, it is difficult to move computers from location to another. No "open connections" are allowed along the network cable.

Because of these limitations, and the relatively higher cost of thin coaxial cable, another common type of cabling became popular in the early 1990s.

Twisted Pair. Twisted pair cable is the type you commonly see used for telephone cable. It comes in two flavors, shielded twisted pair (STP) or *unshielded twisted pair* (UTP). Shielded cabling adds a layer of protective "foil" inside to prevent many types of electromagnetic interference. The shielding makes it is much more expensive.

Unshielded twisted pair cabling is the most common type of cable in use today for computer networking. We will limit our discussion just to the levels of UTP cabling installed in many buildings. There are currently five levels, each of which differs in the number of twists per foot provided. More twists required more cable; therefore, as one goes up the levels, pricing gets higher, but so does signal quality. The more twists in a UTP cable, the more able it is to resist the effects of *crosstalk*, signal interference created by the other pairs of wires inside the cable. The five levels (or categories) are described below:

Unshielded twisted pair cabling is the most common type of cable in use today for computer networking.

- *Category 1*. Early unshielded twisted pair cable used for telephone systems. It is not capable of carrying data signals. If your twisted pair wiring was installed prior to 1983, it is probably traditional Category 1 phone cabling.

- *Category 2*. This level of UTP cabling is certified to carry data signals at acceptable networking levels. It uses four twisted pairs of copper wiring and provides bandwidth up to 4Mbps. It was used in some original LAN implementations.

- *Category 3*. As demand for higher bandwidth network connections developed, a higher-quality UTP cable was designed. It supports bandwidth of up to 10Mbps, the speed of standard Ethernet networks. Many early LAN implementations for Ethernet networks used Category 3 cable.

- *Category 4*. With some network architectures supporting speeds of 16Mbps, cable manufacturers increased the performance of their cable again, up to 16Mbps to match this standard. The minimum level of cabling that should be considered for current LANs is Category 4. However, *in all current or planned network installations*, the next level is recommended for installation simply because it costs almost the same as Category 4 and provides more versatility in future use.

- *Category 5*. Also called *Cat5* cable. The currently recommended level of UTP cable for new installations or upgrades. It is designed to provide bandwidth up to 100Mbps. All installations of Fast Ethernet should be cabled with certified Cat5 UTP cable.

- *Future Levels*. Enhancement of UTP cables is ongoing. Already some Cat5 cables are certified to deliver data at approximately 300Mbps. With gigabit Ethernet (1000Mbps) already appearing in the business and research sector, one can expect continued enhancement of UTP cabling.

Because it uses light, fiber optic cabling is immune to any electrical interference. It's also hard to tap by unauthorized users, so it is a very secure medium.

Fiber Optics. Fiber optic cabling is very different from any other cabling. It does not use copper at all, and the signals it carries are not electrical signals. Inside the cable jacket are very small glass tubes through which high energy light is transmitted. Because it uses light, fiber optic cabling is immune to any electrical interference. It's also hard to tap by unauthorized users, so it is a very secure medium.

It is primarily used where high-speed transmission or longer distance is required. Cable length can range from six-tenths of a mile to 6.4 miles, depending on the type of cable and network signaling used. Fiber optic cable is much more expensive than copper cables to purchase and install.

Radio Frequency Wireless. Obviously, *wireless* technology does not involve cables (wires). However, it does provide network connectivity in specialized local area situations. It is used in internal settings where it is not possible to run cabling effectively (such as older historical buildings which cannot be modified) or where mobile computing is required (such as factory or retail floors). Such internal wireless connections can be made over several hundred feet. Over such distances, the signal is strong enough to penetrate some types of walls and doors.

Network Devices

So far we have discussed network cards and cabling, the two basic building blocks for local area networks. A network card is installed in every computer to be networked. Cable is connected to each network card. The only remaining question is how to connect all the cables together.

Tranceivers. Older coaxial cabling used an Ethernet transceiver to connect the computer cable to the main network cable, referred to as the network *backbone*. Thin coaxial cable uses a small T-connector to connect the backbone cable directly to a transceiver on the network card. But newer network installations using UTP cable are configured quite differently. These networks use a device called a *hub*.

Hubs. When using UTP cabling, an Ethernet network is physically configured in an arrangement called a *star*. Cabling from each computer's network card runs directly to a centralized hub, named after the hub-and-spoke pattern produced when such a network is charted on paper.

The hub acts as a concentrator. It concentrates the signals from every computer attached and then distributes the signals back to all the computers. This is how basic communication occurs over the network. Each computer broadcasts a signal to all other computers on the network. The appropriate computer accepts the signal and sends an acknowledgment. All others ignore it.

Some hubs, generally the more expensive ones, contain electronic circuitry to clean up and regenerate the signals. This function is normally associated with another device called a repeater. (We don't cover repeaters here, because they are seldom used separately unless long runs of cable are required.) Therefore, some documentation refers to them as multi-port repeaters. Due to the popularity of the term hub, we will use it exclusively in this manual.

Each connector on a hub is called a *port*. So the plug from the cable of each computer on the network is plugged into a hub port. Hubs normally have 4, 8, 12, 16, or 24 ports. It is possible to connect one or more of these ports to another hub. This daisy-chaining of hubs allows the number of computers which can be connected to the network to grow.

Cabling from each computer's network card runs directly to a centralized hub. *The hub distributes a signal from one computer to all other computers connected to the hub.*

Network Operating Systems

Once the hardware is in place, a physical network exists. However, communication is still not possible. Next in the development process is the computer's operating system. A computer operating system simply provides basic control of the various components that make up a computer: the keyboard, mouse, monitor, hard drive, processor, etc. Software developers use the operating system to work with the various components of the computer.

The network operating system allows the computer to use shared resources on the network. Computers sold today with Windows 95/98, Windows NT, or Macintosh OS already include a network operating system.

In order for a computer to communicate on a network, a secondary operating system, called the *network operating system*, is required. This software allows the computer to operate the network card and use shared resources on the network. Most computers sold today have a network operating system embedded in the main operating system: Windows 95/98, Windows NT, Macintosh OS, OS/2, and, for high-end workstations, Unix. There are third-party software packages, such as LANtastic and NetWare, which also provide alternative network capabilities to DOS and Windows-based computers.

Some older Windows 3.1-based computers can be upgraded to Windows for Workgroups, which includes the network operating system components required to allow Windows 3.1 to communicate on a network.

Shared Services

The last, but most important, part of a local area network is the resources one wants to share among multiple computers. These include files, printers, and programs. Each of these requires a computer to act as a servant to the rest of the computer. These are called *servers*. The following paragraphs describe the most common network servers.

File Servers. Computers with large, fast hard drive systems can be used to provide access to central files for all computers on the network. These enhanced computers are called *file servers*. One of the primary uses of a file server is to provide access to centralized databases. Electronic library catalogs are one example of such databases. Another is the community non-profit agency database that some libraries maintain. Schools will use a file server to maintain records on their students.

Once an organization gets dedicated access to the Internet, there are a number of other servers the organization may need. To provide information on a web site, a web server is required. To provide e-mail capabilities to staff, an e-mail server is required. Schools may find servers necessary to provide in-house chat or videoconferencing services in support of curriculum.

A specialized form of a file server is used to provide networked access to software applications. These are, quite naturally, called *application servers*.

Shared Printers. Printers attached to a network server can be made available to any computer on the network. The computer to which such printers are attached is called a *print server*. Installing a network card in the expansion slot provided on some printers can make them available on a network without a computer. These are called *network printers*.

Sharing printers can allow an organization either to save money by reducing the number of printers required or to provide a higher quality printer than it normally could afford.

Shared CD-ROM Drives. In many library environments, both in schools and public libraries, many informational databases on CD-ROMs may be available. Some products specifically of interest to municipal and county offices are also available. It is possible to provide access to as many as 21 or more CD-ROM disks at the same time to any computer connected to the network by dedicating one computer to the task. Such computers are called *CD-ROM servers*. Obviously an organization must pay appropriate licensing fees for each product based on the number of users with access to it.

Electronic Messaging. Another common and beneficial use of networks is to provide electronic messaging capability, commonly called *electronic mail*, or *e-mail* for short. Depending on the network messaging software used, messages can be broadcast to all or any subset of the organization's staff. In the case of schools, it can also be used to provide student e-mail access for collaborating with students around the world or communication with teachers or other students.

File servers are *enhanced computers used to provide access to central files for all computers on the network.*

Summary

In this section we have provided a quick overview of the components in a local area network (LAN). We covered the following concepts:

- Protocols—the “language” and rules of communication chosen so that a group of computers can communicate.
- Network Equipment
  - Network cards—an adapter allowing a computer to send and receive data over the network.
  - Cabling—commonly Category 5 unshielded twisted pair, which provides a medium over which the data signals are carried.
  - Hubs—a network device that broadcasts the data signal from one computer to all other computers.
- Network Operating System—the software that controls the network card and allows software on one computer to send commands and responses to other computers, printers, or CD-ROM drives on another computer.
- Shared Resources
  - File servers—provide centralized access to organizational databases and other files.
  - Print servers and Network printers—provide shared access to high-end printers.
  - CD-ROM servers—provide centralized access to CD-ROM informational products.
  - E-mail servers—provide electronic communication capabilites to staff and users.

CHAPTER SEVEN

WANs, MANs, and the Internet

If there is a rule about computer networks, it is this: networks grow. Once an organization chooses to embrace technological solutions in its day-to-day operations, more and more jobs present themselves as viable tasks for technological solutions. So more technology is acquired. With various people needing access to information in computerized—electronic—format, networks of computers are created so that information can be transferred quickly and easily between computers. As we'll see below, these networks grow.

This section presents the basic terminology you will be confronted with in dealing with sharing information resources through a multi-entity, or community, computer network. This chapter also builds on the previous one, describing the basic components you will need to expand several local area networks into something larger. It's called a wide area network (WAN). Let's start with some definitions.

Types of Networks

LANs

In the previous chapter we introduced the concept of a basic network of computers, called a *local area network* or LAN. Remember that LANs are formed to provide a means of sharing information departmentally, or among a subset of computers. A local area network of computers might be formed for many purposes:

- to share a specific printer or printers
- to share databases on CD-ROMs or hard drives

- to enable computer users in a group to send electronic messages to each other
- as a central repository to store and retrieve files for multiple users
- to provide shared access to the Internet

WANs

As technology is used more to store information electronically and to promote effective staff communication, there is a more frequent need to share information among many or all departments in an organization. For county governments and other organizations with dispersed departmental operations—including county libraries with branches—the LANs in each department are joined together to create a network of computer networks. This broader type of network is called a *wide area network* or WAN.

The large network created when joining the LANs in each department of a dispersed organization—such as a county government or county library with branches—is called a wide area network *or WAN.*

The LANs being networked into a WAN are not directly wired in many cases. Some departmental sites will be connected to other sites using a leased data circuit from the local telephone company. Some sites with minimal access needs can be connected with just regular voice telephone lines. We'll discuss these options under "Communications Links" on page 76.

MANs

If all of the LANs being joined are located in the same community, the resulting large network is sometimes referred to as a *metropolitan area network* or MAN. Because there is no difference in how these networks are connected, many network specialists simply refer to LANs and WANs. In this manual we refer to all organization-wide networks as WANs.

Network Designations

Computer networks, both LANs and WANs, are created for various purposes. Some organizational networks are created only for use by organizational staff and managers. Depending on how they are used and who has access to them, these organizational networks have been given different designations. You will be familiar with some of these. Others may be new to you. Still others you may

never see outside the context of this discussion. They are included just to provide completeness.

Intranets

When an organization has information it shares only with staff and employees over an organizational network from a world wide web (or other traditional Internet) server using Internet protocols, the network is called an *intranet*. This means the network is only available inside the confines of the organization. This term has become popular with the advent of commercial access to the Internet. The web format has become so familiar that many companies are now formatting internal information the same way.

Internets

When two or more totally separate networks are joined so that information from each can be shared, the relationship is called an inter-network, or *internet* for short. A wide area network between a school and a public library, for instance, would be an internet.

Extranets

When a company or organization has internal information to which it allows access by a partner or collaborating organization, the network connection between the two is called an extranet (as opposed to an intranet).

The Internet

Obviously, the Internet (with a capital I) is the world's largest example of an internet. It spans the globe, linking computer networks of thousands of companies and organizations.

Creating a WAN

In order to create a wide area network linking two or more separate LANs, one needs three general components:

- a communications link
- a hardware device preparing data to be transmitted or received over the communications link

- a network device connecting a LAN to the communications link; these keep traffic destined for a local computer on the LAN and allow traffic destined for an external computer to pass through

Communications Links

While communication links "look" different, they all accomplish the same goal: they provide a "pipeline" allowing data signals to pass between networks. They look different because they use different *media*: copper wire, glass tubes, and airwaves. For our purposes, the only quantitative differences between the media will be the maximum amount of data that can travel through them in any one period of time and the cost—initial and ongoing—of using the media.

While communication links "look" different, for our purposes, the only quantitative differences between them is the maximum data transfer rate and the cost—initial and ongoing—of using them.

There are also qualitative differences between the various media. Chief among these is signal degradation. This is like sound waves moving through air. As sound travels through air, it spreads out with increasing distance so that it appears to diminish or grow fainter. Signal strength for all media diminishes, or attenuates, with distance, but the distance for each varies. However, when leasing data circuits or phone lines, attenuation is not a problem because the local telephone company is responsible for the quality of the signal, regenerating it when necessary.

The four most common methods of internetwork connectivity, listed in order of increasing data speeds, are analog (regular voice) telephone lines, digital telephone lines, leased data circuits, and private cable. Each of these is examined below.

Use of radio frequency wireless connectivity is increasing. As the main subject of this manual, it is described in great detail in the next chapter, "How RF Wireless Connections Work."

Analog Telephone Line

Unknown to many consultants and grant administrators, it is possible to use a plain old telephone line, also called a POTS line or an *analog* line, to connect an entity's local area network to some other external computer. This is true

whether the connection is to the Internet or to another network in another building. In many TIF grants, libraries have installed multiple phone lines and Internet accounts, one for each microcomputer connected to the Internet. Unfortunately, this results either in unnecessary expense or under-utilized performance.

If the computers were connected in a local area network, the whole network could then be connected to the Internet over a single phone line and Internet account using a network device called an *asynchronous router* (see next paragraph for more details). This would reduce the library's ongoing costs by half or more. If the ongoing expense is manageable, a second phone line and Internet account could be attached to the router as well. In this two-line scenario, the phones appear to be "bonded" so that each computer is capable of receiving web files at up to double the performance of a single line. A single-line LAN connection can support from two to four computers at generally acceptable levels of performance. A double-line connection will support five to ten computers, depending on how often all computers are actively engaged in Internet use.

Analog phone lines require that a modem be connected to the phone line to change the data signal from a digital signal the computer understands to a *range* of sounds (analog) which can be transmitted over the phone line. The modem performs the opposite function on an inbound signal. Multiple computers can share this single phone line, by attaching an *asynchronous router* to the modem. Then the router is connected to a network hub, which in turn is connected to the computers. The router acts like a traffic cop on the network, examining each piece of data and sending it to over the phone line if it is bound for the external network, or on to the appropriate computer if it is bound for the internal network.

Analog phone lines provide at best a *data transfer rate* of 56*Kbps*. In Chapter 5 we determined that this is equivalent to sending about four double-spaced typed pages per second. In actuality, the effective data transfer rate is much less. Analog phone lines commonly suffer from noise. Noise includes such phenomena as line crossover—when you can hear someone else's phone conversation in the background—and the crackling of lightning or static somewhere along the connection. When noise occurs, data is corrupted and must be retransmitted. These retries lower the average

data transfer of the line. In some communities, the greatest transfer rate possible over a regular phone line is 9600bps or less.

While very low, this level of bandwidth is acceptable for some applications, especially basic Internet connectivity. To learn more about how traffic travels over such a connection, and how you can connect more than one computer to the Internet using one phone line and Internet account, see the sidebar "Packets over POTS."

Digital Telephone Line

In some areas, usually metropolitan, another type of phone service is available which uses only digital signals. The bandwidth available through these lines is higher and more effective than that offered by analog phone lines. The most common type of digital line is called an ISDN (Integrated Services Digital Network) line. An ISDN line provides up to two *channels*, or data paths, for connectivity, each providing a maximum 64Kbps data transfer rate. Using both channels at the same time provides up to 128Kbps of bandwidth.

Digital lines are much cleaner lines than regular analog lines. They are less affected by "noise," so their effective data transfer rates are much better than analog lines. While the maximum bandwidth of an ISDN line is almost two-and-a-half times as great as an analog line, its effective bandwidth is commonly three-and-a-half to four times as great.

Another type of digital line is called an ADSL (Asynchronous Digital Subscriber Line) line. ADSL technology provides various combinations of data transfer rates. When equalizing transmit/receive data rates, it is common to achieve bandwidth in excess of 600Kbps. Unfortunately, it is not yet available in most markets. If your local phone company is willing to provide a "dry line," or alarm line, to the two ends of a network connection, at least one vendor sells the equipment needed to create one's own ADSL connection. However, most phone companies are reluctant to do so for competitive purposes.

Packets Over POTS

When data is transmitted over a network, it doesn't have a continuous nature like a radio channel or phone conversation. Instead, it operates in a piece-meal fashion. In fact, a highway analogy works well in visualizing the process.

A data file is split into pieces. Each piece is encoded with information like the sending and destination computers' identifications. A sequence number is also included, indicating how to reassemble the pieces at the receiving end. All of this is enclosed in a unit we call a *packet*.

Data packets are like cars on a highway. They are sent up the onramp (network card) to the highway (data cable) where they merge with other cars (packets). A one-lane highway is not limited to just one car. Many cars can be on the highway at the same time. The network operating system makes sure that each packet takes the correct exit. On the other end, the packets are reassembled into the original file and displayed or stored on the remote computer.

This works over phone lines, too. When *three to five* computers are connected to a hub, and the hub is connected to a router, and the router is connected to the Internet through a modem and phone line, the packets from the several computers can all go out over the single line. A phone line is like a country road, though. More than five computers may create a traffic jam!

Leased Data Circuit

Data circuits provide a wall outlet that looks like a regular phone line connection. Nevertheless, they are not phone lines because they are not switched; that is, one cannot dial multiple places. In fact, one does not dial at all. A data circuit is a digital connection (normally) between two distinct entities, often called point-to-point service. The line becomes active when the network equipment on each end is connected and begins the communications process. Data circuits are "on" 24 hours a day. They are priced on a flat monthly rate. However, the rate is distance sensitive. The greater the distance between the two entities being connected, the higher the cost.

Four common terms are used to describe data circuits: 56K line, T-1 line, fractional T-1 line, and T-3 line. Due to recent state legislation lowering the cost of T-1 lines for public libraries, schools, and telemedicine centers in Southwestern Bell and many GTE-served communities, 56K lines are falling out of favor due to their limited bandwidth.

T-1 lines are data circuits with a maximum bandwidth of 1.544Mbps. These circuits are capable of being divided into 24 distinct channels, which can carry different streams of data, and, in fact, different types of data. Each channel, effectively represents 64Kbps of bandwidth.

Some T-1 circuits are ordered only using a portion of the channels available. These circuits are called *fractional* T-1 lines. Common increments of bandwidth in a fractional T-1 line are 384K, 512K, and 768K.

T-3 circuits are similar to T-1 lines in that they can be channelized or used "full pipe." Each of the 28 channels in a T-3 line equates to a T-1 line, or 1.544Mbps of bandwidth. When non-channelized, a T-3 circuit is capable of providing 45Mbps bandwidth. And, like T-1 circuits, fractional T-3 circuits can be ordered.

At this point in application development, T-1 circuits suffice for most community networks. However, when motion video transmission is more prevalent, perhaps in two-to-five years, the bandwidth limitation of a T-1 circuit will be a constraint on service.

Private Data Cable

The most common alternative to leased phone lines or data circuits is privately installed fiber optic cable. Especially for school districts where campuses are located “next door” to each other, laying fiber optic cable between campuses is the most cost-effective method of creating linking networks in separate buildings. But for those cases where a highway, private property, or physical barrier such as a lake must be crossed, the initial cost of laying fiber optic cable can be considerable. Costs can easily be in the tens of thousands of dollars in small communities and the hundreds of thousands of dollars in larger cities. Plus, right-of-way fees may be incurred for crossing private property or using utility poles to hang the cable.

The most common alternative to leased phone lines or data circuits is privately installed fiber optic cable.

Radio Waves

The use of commercial wireless technologies to create municipal and wide area network links is a very recent development. It is ideal in situations where physical barriers or right-of-way fees prevent fiber optic installation. We cover wireless connectivity in greater detail in the next chapter.

WAN Equipment

Any discussion of network equipment can quickly become very technical. In this introduction to the concepts we purposely simplify the description of components. Our purpose is to acquaint you with the component parts and what they do, not necessarily teach you how they do it.

For each of the connectivity options listed above, certain hardware is required to connect the local area network to the transmission medium. In most cases, two separate pieces of hardware are required. The first translates network data into signals that can be carried over a particular medium. These include modems, channel service unit/digital service units (CSU/DSUs), radio transceivers, and others. The second is a network device that determines whether data can come into the network or go out across the WAN connection. These include bridges, routers, and switches.

A third component, a combination of computer hardware and software, is used in many cases to protect an internal, private LAN from abuse by outside users. These devices are called *firewalls*. We discuss each of these in more detail below.

Modems and CSU/DSUs

Modems. In order to get a packet of data from one computer network to another over a phone line, a *modem* is used. (Modem is an acronym for modulator/demodulator.) A modem translates a data signal that works on a computer network into a signal that works over a phone line. Another modem performs the reverse function on the other end. It's all magic, of course!

A modem translates a data signal that works on a computer network into a signal that works over a phone line. Another modem performs the reverse function on the other end.

Other types of modems are also used to connect networks to other types of phone lines, such as ISDN or ADSL lines. While they work a bit differently, these modems accomplish the same purpose. Note that in many cases modems for these digital lines are housed inside another network device called a router. We'll discuss routers in the next section.

CSU/DSUs. Once you move up the scale of connectivity options to a leased data circuit, another type of hardware is needed. A Channel Service Unit/Data Service Unit (CSU/DSU, also called a DSU/CSU) provides an interface between a network device like a bridge or router and the leased data circuit.

Not only does the CSU/DSU prepare network data packets for transport over a data circuit, it also maintains "channels" over the data circuit. When a data circuit is channelized, its bandwidth is segmented for different purposes. For example, one channel may carry voice traffic while other channels carry data traffic.

CSU/DSUs may be purchased as independent units. However, when acquiring a CSU/DSU and the associated router or bridge from the same manufacturer, it is usually less expensive to purchase the CSU/DSU as a module which slides into the router/bridge chassis.

Bridges and Routers

Whenever two networks are joined, there must be a traffic cop to determine where every packet goes. Any data

broadcast over one of the networks might be destined for a computer on its local network or the remote network. Instead of having every packet traverse *both* networks, a network device is positioned at the connecting point and examines every data packet. Those addressed to a computer on the local network are ignored. Those addressed to a computer on the other network are sent over the connecting link. This maximizes the efficiency of the link and keeps unnecessary traffic off the LANs.

Bridges. One common type of network device used in connecting multiple networks is a *bridge*. A bridge is used for two different purposes: to break a large LAN into smaller segments so that traffic is more efficiently distributed, and to create a WAN link to another computer network. When used to segment a LAN into smaller components, only one bridge is required. The separate segments are connected to separate ports on the bridge. When used to connect two LANs into a WAN, two bridges are required, one for each side of the WAN link. Each monitors the traffic on its own LAN.

Bridges are the simplest, quickest traffic cops. But they're not as intelligent as other types. Bridges examine the packets on one network and then perform one of three actions:

- dropping, or ignoring, the packet because it is destined to another computer on the same network
- forwarding the packet to the appropriate external network link (there can be more than one other link) because it recognizes the destination computer address
- broadcasting the packet to all other links because it does not recognize the destination computer address

While quick, this does not provide the most efficient means of linking the networks. The broadcasting of packets can clog the networks involved or saturate the communications link. For better efficiency, a router is required.

Routers. Routers are configured into a network of networks the same way bridges are. However, they operate slightly differently. They actually "open" packets to read more information. Then they send the packet to appropriate network segment. Broadcasts to other segments are eliminated, increasing the effectiveness of all connections.

In an environment where there are multiple routers, the router can determine if there are multiple "paths" to the destination computer. They can also determine which of the possible paths is the most efficient. In this way, severe congestion over one popular path is avoided, increasing apparent throughput in the network connections. Almost all connections involving disparate networks now employ routers.

Wireless Bridges. In wireless network connections, a network device called a wireless bridge is used. Wireless bridges have two components included: a radio transceiver which enables the wireless connection and a network bridge which routes network traffic across the radio connection as needed.

Wireless bridges have two components included: a radio transceiver which enables the wireless connection and a network bridge which routes network traffic across the radio connection.

The radio transceiver and associated circuitry performs a function similar to a CSU/DSU or modem. It prepares data packets for transmission across a medium with a different signaling structure than a network cable. It also receives radio signals and turns them back into data packets the bridge can forward to the network. See the section "Radio Transceivers" on page 98 for more information about how data is transmitted over radio waves.

The bridge portion performs standard bridging functions. However, because of the improved routing available in a router, some bridges now have software performing routing functions. Some of them are referred to as wireless bridge/routers, or brouters.

Because of their specialized nature—that is, preparing network data to be transmitted over radio waves—wireless bridges must operate together seamlessly. This requires bridges on both sides of a radio connection to be made by the same company. When a large radio WAN is created, all of the bridges connecting the WAN must be made by the same company. (A new networking standard for wireless bridge and brouter products has emerged over the last year, so interoperability is a future possibility.) Because of this, product quality and manufacturer support are very important.

Firewalls/Proxy Servers

The last component we'll mention in relation to WANs is the *firewall*. Like the firewall between a car's engine and the

passenger compartment—literally designed to keep fire in a car's engine compartment away from the passengers—network firewalls keep *outside* threats away from sensitive data available inside the network.

Whenever the networks from two different organizations are joined together, there is always a threat that someone from one organization (or someone breaking into that organization's network) will break into the other organization's network. Such break-ins may result in private data being stolen and distributed, valuable data being altered or destroyed, or entire hard drives being erased. In network terms these risks are called *security risks*. Add an Internet connection to this equation, and a whole class of dark threats, real or imagined, can be foreseen.

The primary purpose of creating many community networks is to share a high-speed Internet connection, providing better throughput at lower total costs.

Firewalls are used as a means of preventing or minimizing the security risks inherent in connecting to other networks. Some routers have firewall capabilities and are called *firewall routers*. When they exist outside the router, firewalls normally take the form of a computer dedicated for this one purpose, with appropriate security software installed.

It is important that any organization connecting to others or to the Internet take security precautions. The topic of security is addressed in more detail in Chapter 9.

Linking to the Internet

The primary purpose of creating many community networks is to share a high-speed Internet connection among two or more organizations, rather than having these organizations pay higher total costs for separate, and sometimes lower-speed, service. With more commercial services being offered over the Internet, such connectivity enables the cooperating group of entities to negotiate lower fees for the service than the aggregate cost of having each entity contract for the same service separately.

We know it's an economically viable thing to do. The question is, how does this Internet connection work? The following two sections discuss briefly the two cost components of an Internet connection: a telecommunications link for the Internet connection and access charges for getting data traffic to and from the Internet.

Making the Link

We've discussed the components required to create a wide-area network: communication links and bridges or routers to route data traffic over the links. Sometimes showing is better than telling. See Figure 1 on page 43 for a diagram of a very simple WAN connecting the LANs of a school and public library and providing a link to the Internet.

The communication link between two or more LANs has a defining characteristic: you either pay a monthly fee or you pay to have a private connection implemented so that there is no ongoing cost. (Both require maintenance of the equipment, however.) Regular telephones, ISDN lines, and 56K and T-1 lines all require regular monthly payments to your local phone company. In some cases when entities install a private fiber optic cable, there may be recurring monthly or yearly fees, such as a payment to the electrical utility for the right to hang the fiber on utility poles. In other cases, the fiber link will be free of recurring charges. Wireless links involve no recurring fee.

The communication link between two or more LANs has a defining characteristic: you either pay a monthly fee or you pay to have a private connection implemented so that there is no ongoing cost.

The cost of voice-grade lines will range from $25-$40 per month. ISDN lines in most locations in Texas will cost $50-$60 per month with no per-minute charges. In some locations which are provided an extended ISDN link from a metropolitan area, the monthly cost will be about $90-$140. Data circuit costs rise sharply from there. Regular business costs of a T-1 line, which are related to the distance between the two points being connected, range from $200-$1,000 per month or more. Public schools and libraries qualify for reductions in these rates. But there is some question whether municipal and county data traffic can then be carried over them.

While the link between the two LANs can be created with wireless technology, to incorporate Internet access a separate communication link to the Internet is required. The Internet link will almost always take the form of a leased data circuit between the WAN's central site and an *Internet Service Provider* (ISP)—a company acting as a conduit between your network and the Internet. Few ISPs currently offer wireless connections to their networks. The leased circuit incurs the costs mentioned above. But communicating over the Internet involves a second cost as well: the cost of Internet access.

Paying for the Traffic

In addition to the communications link costs quoted in the previous section, a link to the Internet also requires payment to the ISP. High-speed access to the Internet is expensive. While dial-up accounts to the Internet cost around $20 per month, full-time, high-speed access to the Internet is much more expensive.

Commercial ISPs charge as much as $2,500 to $3,500 per month for *guaranteed* T-1 access to the Internet. Guaranteed access means the full bandwidth of a T-1 line is available to the Internet whether the customer uses it or not. ISPs also provide *shared* T-1 access to the Internet. Shared T-1 access means two or more T-1 lines are connected to a router which provides just T-1 access to the Internet. At any moment, only T-1 access is available. If one entity is using 25% of the total capacity, another entity will have only 75% of the capacity available.

Normally, shared access comes with some guaranteed level of service, such as 128Kbps or 384Kbps (1/12th and 1/4th the full capacity of a T-1 line). Since a high-speed connection to the Internet is seldom fully loaded, paying for shared access is more cost effective. Such connections range in price from $1,000 to $2,500 per month through a commercial ISP. Municipal and county governmental entities in Texas can get shared access to the Internet from $300 to $1,000 per month.

With the cost of T-1 Internet connectivity ranging from about $300 on the low end to $3,500 on the high end, sharing the cost of the Internet link is a primary benefit to creating a wide area network for public entities. Given the fact that one entity very rarely uses the entire capacity of its link, this sharing seldom results in degradation of service. These concepts are described in more detail in Chapter 1, “The Need for Community Networks.”

Summary

In this section we looked at the basic components used in a wide area network. We covered the following concepts:

- Communication Links—the various types of telephone lines and data circuits used to transport data from one network to another. These include:
  - Voice-grade telephone lines
  - Digital telephone lines
  - Point-to-point leased data circuits
  - Private fiber optic cables
  - Airwaves (wireless connections)
- Network Equipment
  - "Modem"—any of a variety of devices that allow a computer or network to transmit data over telephone lines and other links
  - CSU/DSU—hardware unit used to terminate and channelize a leased data circuit
  - Bridge or Router—hardware used to control the flow of data traffic over two or more linked networks
  - Wireless Bridge—a combination of a radio transceiver and a network bridge, linking two or more networks
  - Firewall—hardware and software unit securing a network against unwanted external threats
- Linking to the Internet
  - Network link—usually a leased high-speed data circuit, connecting a LAN or WAN to the Internet
  - Access costs—the charges payed to an Internet Service Provider for tranferring and receiving data over the Internet

CHAPTER EIGHT

How RF Wireless Connections Work

RF is commonly used in the wireless communications industry to describe equipment using *radio frequency waves* to transmit sounds and data from one point to another. In computer networking, RF is used to describe network devices (hubs, bridges, etc.) that transmit data signals using radio waves instead of data cables or telephone lines. What is required to enable this wireless network is described in this chapter.

I'm going to assume you have a basic understanding of the concepts related to creating a wide area or municipal network (these concepts are presented in the previous chapter, "WANs, MANs, and the Internet"). So if you're not sure, review those concepts before proceeding. Once you're ready, read on and plunge into the world of wireless networking.

What are Wireless Technologies?

"Wireless" products, from remote control cars to cellular telephones, use a form of energy known as electromagnetic radiation to carry signals. The signals can be the pattern of vibrations commonly experienced as sound by the human ear. Or they can be the abrupt changes of frequency or intensity used to encode data signals. Whichever, electro-magnetic radiation carries them through free space. We will get into this in detail in a moment. First, let's describe the four most common forms of wireless technologies: satellite, microwave, infrared, and radio communications.

Satellite Communications

Normally, satellite communications are unavailable to small entities for network connectivity. The cost of leasing a

Note: Microwaves

Designations of the various parts of the electromagnetic spectrum (radio, microwave, infrared, visible light, ultraviolet, x-ray, gamma ray) are man-made. Therefore, the boundaries of each may be quoted differently in various sources. The *microwave* spectrum generally includes frequencies above 1.0GHz to about 30GHz. In this manual, however, microwave refers to the portion of the spectrum higher than 6.0GHz.

Communication devices operating at these higher frequencies require a license from the FCC. Devices that operate in the Scientific and Medical bands (2.4Ghz and 5.3Ghz), while technically operating in the microwave band, are non-licensed and referred to herein as radio frequency devices to reduce confusion.

transponder is prohibitive. However, one viable exception is the use of satellites to connect end-users to the Internet. A couple of companies currently offer high-speed Internet access to home and business customers through the installation of a small parabolic antenna (*satellite dish*).

While this type of connectivity provides over 400Kbps download speeds, it is strictly a one-way medium. In order to make use of these services, end users must also maintain a land-based, physical connection (lower speed) to the Internet. In this scenario, requests are sent to web sites over the land-based connection and are received through the satellite connection. This provides quick response times from the Internet but is unsuitable for community network connectivity.

On the other hand, new satellite technology is being explored. Low-Earth-orbiting (LEO) satellites are being deployed as this manual is being written. With hundreds of these satellites available in the next few years, the cost of transmit-and-receive capability through satellite technology may drop. Projects such as *Iridium* (http://www.iridium.com/) and *Teledesic* (http://www.teledesic.com) bear watching over the next few years. Iridium is being deployed as a wireless phone service alternative. Teledesic, with the moniker "Internet-in-the-Sky," is set to provide wireless Internet service to businesses, schools, and end users.

Microwave Communications

The complete electromagnetic spectrum includes many types of wavelengths we've become very familiar with, at least in name. First among these is visible light. Two other types of wavelengths, just at either end of the visible spectrum, are infrared and ultraviolet light. These are the wavelengths that bring us "night vision" technology and tanning booths, respectively. Another portion of the electromagnetic spectrum we're becoming familiar with are frequencies called *microwaves*. These exist below infrared frequencies, but above normal radio frequencies.

transponder—the portion of a satellite which transmits and receives radio signals in a prescribed frequency range from ground stations (transmitter/responder).

Many of the data communications services offered by major telecommunications companies are supported by microwave technology. While it is a viable alternative even in private communications, it has two drawbacks. First, microwave communication requires FCC licensing. Second, the cost of implementing microwave technology (tower/dish

infrastructure) is higher than other options. On the other hand, microwave communication is extremely resistant to interference. But, because of its cost, it will not be an adequate alternative for many rural community networks.

Infrared Communications

Computer technology that uses the infrared spectrum is becoming common. For example, wireless keyboards and receivers are commonly distributed with computers that serve as a base for home entertainment systems. A receiver is attached to the keyboard connector on the back of a computer case. An infrared transmitter operating at a proprietary frequency (each wireless keyboard manufacturer typically uses a different frequency) translates the keystroke coding into an infrared signal and sends it to the receiver. Also, some computers now come with an infrared port which allows information from a hand-held or pocket computer to be transmitted to the desktop computer.

There are also network bridges/routers that use the infrared frequencies to transmit data. (For this manual, infrared communications includes laser technology used for data communications.) Like microwave technology, infrared provides high-speed connectivity. But infrared communication solutions are expensive to implement.

In most cases of community infrastructure, radio and microwave equipment will offer the most effective form of wireless communications. Because of licensing and cost issues, we have chosen to focus on radio frequency wireless. In the remainder of this chapter we'll discuss in plain English the core aspects of using radio frequencies to transmit computer data.

Because of licensing and cost issues, we have chosen to focus on radio frequency wireless.

Common RF Uses

Even though the phrase "RF wireless networking" might seem mysterious, the underlying technology is very common. It uses radio waves, the same type of energy used to transmit radio and television broadcasts. Two-way radios and walkie-talkies also use this technology.

The space program utilizes radio waves to control computers onboard space capsules and probes, and receive signals from other devices. Remember the video broadcasts

from the surface of the moon? The color photographs of the surface of Mars? All of these were translated into radio waves and transmitted to Earth using radio technology.

Thinking about radio and TV, you can probably already identify some of the components needed to make RF wireless networking work: a radio transmitter, a radio receiver, an antenna, and a cable from the antenna to the receiver or transmitter. Add a couple of other components to protect the equipment—such as lightning arrestors and noise filters—and you've pretty much listed what you need.

Thinking about radio and TV, you can identify some of the components needed for RF wireless networking: a radio transmitter, a radio receiver, an antenna, and a cable from the antenna to the receiver or transmitter.

You thought this was going to be complicated, didn't you? In the next few sections we'll describe what is involved in transmitting data over a radio frequency and how a wireless network connection can reliably be established.

Radio Waves

When radio waves are described as the technology used to broadcast radio and TV programs, some people assume radio waves are a little like sound waves. Thus the term "airwaves." A sound is made when something causes the air to vibrate. This vibration is transferred to our eardrums when the sound wave arrives. The vibration is then translated into a signal transmitted to our brains, where we perceive the sound. But radio stations broadcast their signals through the air, so why don't we hear them without a radio receiver?

This is a trick question. Radio waves are really not at all like sound waves. They do not create vibrations in our ears. They do not rely on vibrations in the air; in fact, they do not need air for transmission. Instead of being a vibration, they are a form of energy. They are part of what is called the *electromagnetic spectrum*. This energy spectrum includes the full range of radiation created by the interaction of electrons and magnetic fields. As we mentioned in the sidebar "Airwaves" on page 22, these types of radiation include radio waves, microwaves, infrared light, visible light, ultraviolet light, and x-rays.

Okay, we won't delve into physical science too much. Let's just say that radio waves are akin to light waves. They're also akin to microwaves and X-rays. All are forms of radiation, created by the properties of electromagnetic

fields. For example, radio waves are created when electrons are passed through a conductor, like an electrical wire. The current creates a magnetic field. Fluctuations in the current produce changes in the magnetic field, creating *waves* of electromagnetic energy or radiation. Other forms of electromagnetic radiation are produced through other atomic processes (we'll definitely skip the course on atomic physics!).

These changes in the magnetic field are called waves because the energy *oscillates*—rises in intensity to a peak, fades to a minimum, and then rises to its peak level again. The distance between two successive peaks or troughs is called the energy's *wavelength*.

All of these forms of energy travel at the same speed—the speed of light. The only difference between them is their wavelengths. Radio waves are the longest. Gamma rays are the shortest. Because gamma rays are shorter, and they travel the same speed as radio waves, more of them can pass a specified point in a single second. The number of waves passing a point in one second is called the energy's *frequency*. Gamma rays have much, much higher frequencies than radio waves.

Radio waves are created when electrons are passed through a conductor, like an electrical wire.

Frequency is measured in a unit called a *hertz*, after Heinrich Hertz, one of the early experimenters with radio waves (originally, radio waves were called Hertzian waves). The *hertz* is usually defined as one cycle per second, or one wave per second. So, the spectrum of electromagnetic waves is described in hertz, normally abbreviated *Hz*.

Like data transfer rates, frequencies can be very large, so the standard large units are used to note them: kilo (K), mega (M), and giga (G). Radio waves have frequencies from about 150kHz (kilohertz) through 300GHz (gigahertz). In contrast, light waves are much shorter and have much higher frequencies. Light wave frequencies are in the area of about 100 trillion hertz, or 100THz (terahertz).

Radio Bands

In order to keep people in the United States from interfering with each other's use of radio signals, the Federal Communications Commission (FCC) is in charge of assigning small sections of the radio frequencies to specific

uses. These are called *licensed frequencies*. In order to broadcast radio signals at these frequencies you must apply to the FCC for a license.

However, to allow use of some of the radio spectrum for small applications that would not require a license, the FCC has allocated three separate bands of radio frequencies as *public* bands. No license is required to use equipment transmitting at these frequencies. These are called the *ISM bands*, short for Industrial, Scientific, and Medical bands. Table 10 shows the frequencies reserved for these bands.

Table 10. ISM radio frequency bands.

Frequency Range	Band Description	Bandwidth Available
902-928MHz	Industrial Band	26.0MHz
2.40-2.4835GHz	Scientific Band	83.5MHz
5.725-5.850GHz	Medical Band	125.0MHz

Notice that the bandwidth available increases in the higher frequency ranges. These higher frequencies will support higher data transfer rates. Therefore, many wireless bridge products being sold today operate in the 2.4GHz and 5.7GHz frequencies. As throughput increases, computer networking becomes more of a real possibility. And, with more companies producing RF wireless networking products, prices are continuing to fall, making wireless networking a viable alternative to land-based lines in many local areas.

On the other hand, whenever unlicensed technology becomes available, there eventually comes a time when one user interferes with another's ability to use the same technology. Remember the CB radio craze of the 1970s? CBs also operated on public radio frequencies. Since they were not licensed or regulated, and were very inexpensive, many people tried to use them. Even when 40-channel radios became available, there were still too many people trying to use too few communications channels. Their popularity waned.

What keeps the unlicensed ISM bands from becoming equally overused? There are two primary differences in how RF wireless networking is implemented that minimize interference and contention for use of the bandwidth

available. The first relates to the method used in transmitting a data signal over radio waves. The second relates to the type of antennas used to radiate and receive the radio signals. Let's examine the transmission technology first.

Spread Spectrum Technology

Most communication technologies we are familiar with—radio, television, two-way radios—use what is called *narrowband* communications. Each station or channel operates over a very thin slice of the radio spectrum. Because the station is assigned that particular band, and the FCC ensures that no other broadcasters in the local area use that same band through licensing, there is no interference. The range of each station is limited, so the same frequency can be re-used a great distance away without interference.

Radio, television, and two-way radio technology uses narrowband *communications. New techniques spread the radio signal over a wide "spectrum" of radio frequencies, minimizing interference. This is called* spread spectrum technology.

Because many devices might use the ISM bands in a local area, additional technology is required to keep the various signals from interfering with each other. Fortunately, a technology has been developed over the past fifty years which permits such bandwidth "sharing." This technology provides a way to spread the radio signal over a wide "spectrum" of radio frequencies, minimizing the impact of narrowband interference. In most cases, only small parts of the transmission are corrupted by any interference, and coding techniques allow that data to be recaptured. This technology is now generally known as *spread spectrum*.

There are currently two different spreading techniques used. Both use a coded pattern of communication. A receiving unit is synchronized to use the same pattern and successfully receive the transmission. Any other radio unit hears the signal as noise because it is not programmed with the appropriate coding. The two techniques are called *frequency hopping spread spectrum* and *direct sequence spread spectrum*. I'll discuss each in detail, but I want to begin with frequency hopping. It was the first conceived, and it has a wonderful story behind it.

Frequency Hopping Spread Spectrum (FHSS). The United States military developed a radio technology called *spread spectrum* during the 1950s and 1960s. Obviously, the first concern was ensuring that radio transmissions were not

intercepted. The second concern was to ensure that guided missile communications were not jammed by enemy radio transmissions.

Though developed and implemented by the U.S. military, the problem was first addressed by Hedy Lamarr, a famous actress of Austrian descent in the 1930s and 1940s. She and a music composer, George Antheil, patented the idea in 1940. She was so far ahead of her time in conceptualizing the idea that she never received any monetary rewards for her patent. The patent license expired before government and commercial implementation of the concepts occurred. You can read the story in more detail by visiting the "secret communications technique" web site, at the following address.

http://www.nache.com/chris/pat2/index.html

Here's how the idea works. A communications signal (voice or data) is split into separate parts. Instead of transmitting a signal continuously over one narrow frequency band, the several parts are transmitted separately over a wide spectrum of radio frequencies. A defined, but random-appearing pattern of non-sequential bands is used, with successive parts being transmitted over the next frequency band in the pattern. On the other end, a receiver is configured to receive the signals in the same pattern. The radio receiver then reassembles the pieces into the original signal. Since many distinct patterns can be developed, it is possible to have multiple radios transmitting at the same time, but never at the same frequency at the same time.

The process of jumping quickly from one frequency to another is called *frequency hopping*. And, therefore, the technique is called *frequency hopping spread spectrum*.

Frequency hopping has two benefits. Electrical *noise*—random electromagnetic signals which are not part of any communications signal—will only affect a small part of the signal. Also, the effects of any other forms of radio communications operating in narrow bands of the spectrum will be minimized. Any such interference that occurs will result in only a slightly reduced quality of voice transmission, or a small loss of data. Since data networks acknowledge successful receipt of data, any missing pieces will trigger a request to transmit the lost data.

Direct Sequence Spread Spectrum (DSSS). Direct sequence spreading is very different from frequency hopping. Instead of splitting a data signal into pieces, direct sequencing encodes each data bit into a longer bit string, called a *chip*. Usually, 11 to 20 bits are used for the chip, depending on the application. Because the military requires a much higher degree of security, it generally uses much longer chips—even a long as 1,000 to 10,000 bits! An eleven-bit chip is illustrated below.

0=10010010110
1=01101101001

Notice that the binary string encoding a 0 has the opposite form as the string encoding a 1—where a "1" is used in one chip, a "0" is used in the other.

The chip is then used to modulate (change) the signal generated by the radio transmitter, spreading the signal out over a wide band of frequencies. The receiver uses the same code and so listens for the unique signature across the frequency spectrum. It then decodes the signal back to the original data.

This is a simplified explanation of a very technical subject, but hopefully it gives you an idea of how spread spectrum works. The gist is that spread spectrum technology allows multiple radio signals to operate in an open, unlicensed band with a minimum of interference. It also provides security for the transmission.

Spread spectrum technology allows multiple radio signals to operate in an open, unlicensed band with a minimum of interference.

Radio Signals as a Data Transmission Medium

Now that you've become a little more familiar with what radio signals are and how they can be used in a public band of frequencies without creating general chaos, let's take a look at how those radio signals are used to create a network transmission medium.

Computer networks use variations in electrical current to transmit data from one computer to another. While each type of cable (coaxial, thin coaxial, and unshielded twisted pair) has its own electrical properties, there is a commonality in how the electrical signals are transmitted from one network card to another using these media. Using a telephone "line," whether analog or digital, adds a little

complexity to the process, but not a lot. However, when using fiber optic cable, which uses light waves as a medium, and radio signals, which use radio waves as a medium, the process is a bit more complex. (Fiber optic transmission deserves its own work, so I'll skip it here.)

To see how electrical signals get changed into radio signals, let's look at the two radio components of a wireless data connection: the radio transceiver and the antenna.

Radio Transceivers

To create a computer network connection over radio waves, two puzzle pieces are needed. First, a network device such as a bridge or a router is needed. The network bridge/router handles the data traffic. It routes the appropriate data signals bound from the computer network in one building to the network at the other end of the radio connection. Second, a radio transmitter and receiver, commonly called a *transceiver*, is required. The radio transceiver handles the radio signal communications between locations.

The interesting part of this marriage of technologies is that radios have always dealt with electrical signals. The radio transmitter *modulates*, or changes, an electrical signal so that its frequency is raised to one appropriate to radio communications. Then the signal is passed on to a radio antenna. We'll discuss the work of antennas more in the section "How the Antennas Work," on the next page.

At the other end of the transmission, the receiving portion of the radio transceiver takes the radio signal and de-modulates it back to its normal frequency. Then the resulting electrical signal is passed to the bridge/router side for processing by the network. While the actual process of modulation/demodulation is technical, the concept of radio transmission is very simple.

Likewise, when a response is sent back to the originating site, the radio transceiver "flips" from reception mode to transmission mode. The radio transceivers at each end have this characteristic. Transmit-receive, transmit-receive. They change modes as many as thousands of times per second. This characteristic leads to a delay in communications called *latency*. It is idiosyncratic to radio communications

and negatively affects data throughput. See "Throughput vs. Data Rates" on page 102 for more information.

How the Antennas Work

In the middle of the radio transmission/reception process sit two antennas, one at the building from which the signal is transmitted and one at the building receiving the signal. Of course, it is possible to have one central location and several remote locations connected to the network. For discussion's sake, though, let's think of the communication process as a straight line, from one antenna to the other.

In order to transmit the modulated radio signal, an electrical current passes through the antenna, inducing a magnetic field, which oscillates at the given frequency. The variations in the current create slight variations in the radio frequency. These radio waves radiate outward from the antenna in a "beam" according to the antenna's design.

On the other end, when the radio is in receive mode, the antenna is passive. The electromagnetic radiation from the originating antenna passes across the receiving antenna. This creates a magnetic field, which, in turn, induces an electrical current through the antenna. The current passes through the radio receiver and is demodulated back into an electrical signal with the same form as the original electrical signal from the first network bridge/router. This electrical signal passes to the bridge/router portion of the receiving unit as a normal data signal.

As if by magic, a data signal is transferred from one network bridge/router to another without the necessity or expense of an interconnecting wire. More information about the various antennas used in wireless networking is presented in the next section.

An electrical current passes through the antenna, inducing a magnetic field, which oscillates at the given frequency. The variations in the current create slight variations in the radio frequency, which radiate outward from the antenna in a "beam."

Types of Antennas

Because the radio equipment used in wireless networking must by law be very low-powered to minimize interference with other devices, the antennas required are much more focused than those used in radio or television applications. The amount of focus they use in transmitting a signal, and their corresponding ability to "pick out" specific radio

signals, is called *gain*. The gain is measured in *decibels*, abbreviated *dB*.

There are two major categories of antennas: directional and omni-directional. Directional antennas focus their energy in tight, narrow beams. When receiving signals, directional antennas do not "see" any signals coming from outside the "beam" on which they are focused. This eliminates a great deal of potential interference from other radio sources and contributes to the ability of multiple wireless communications systems to coexist with a minimum of interference.

Omni-directional antennas transmit their energy in a full circle. Spreading the radio signal over such a large area reduces the energy in the signal. This severely restricts the distance the signal can be transmitted and received effectively. Therefore, transmissions via an omni-directional antenna do not travel as far before being degraded as do those from directional antennas. (However, amplifiers are available for both types of antennas to lengthen the transmit distance.)

These characteristics make each type of antenna optimal in different situations. For those networks involving more than two buildings, called *multi-point connections*, an omni-directional antenna at the central site will be most cost-effective. A directional antenna is installed at each remote site, aimed back at the central site omni-directional antenna. Since the omni-directional antenna transmits in all directions, every remote antenna can pick up its signal and transmit back to it.

On the other hand, some network connections involve only two distinct buildings. These are called *point-to-point connections*. In these situations, a directional antenna is used at each site, each aimed at the other.

Both types of antennas are available with various levels of gain. Table 4 on page 40 shows some common antenna types, their gain, the maximum distance over which they are effective, and their approximate cost.

Other Components of Wireless Connections

In addition to the wireless bridge and antenna, there are a few more items required to make a functional wireless

network connection. In the course of specifying a system, some are easy to overlook.

Feature Sets. Some manufacturers sell their wireless bridges in separate units. In such instances, the physical radio/bridge unit has a base cost. Software features, such as individual protocol routing and encryption, are sold as a separate unit. However, these may be required in your implementation. Be sure to define your needs completely to the reseller/integrator/installer who installs your wireless connection.

External Cables. For all wireless installations there must be a cable which connects the antenna to the radio in the wireless bridge. Because it runs to the outside of the building, this is called an external cable. When purchasing all the components as part of a kit, an external cable is included. Depending on where the wireless bridge is located inside your building, and where the antenna is mounted, an additional length of cable may be required.

In order to keep the wireless system within specifications, it is important to minimize the length of the cable. If necessary, it is possible to locate the wireless bridge at one location in your building and run a network cable from it to your network connection at an alternate location in the building. Be sure to physically secure the bridge if it is located in a public area.

Lightning Arrestor. Since external antennas are involved, the threat of a lightning strike can be very real. Make sure that proper measures are implemented to minimize the risk of lightning strikes. Most manufacturers of wireless bridges sell an optional device called a lightning arrestor. It is normally installed between the antenna and the bridge. Also make sure the antenna is properly grounded.

Emissions Filter. Some manufacturers provide another optional component known generally as an emissions filter. It reduces the level of extraneous noise that might interfere with the electrical signal on its way from the antenna to the wireless bridge. It also is installed inline between the antenna and bridge.

Mast or Tower. When it is not possible to obtain a clear line-of-sight between the two antennas involved in a wireless connection, a mast or radio tower may provide additional

height for the antenna, clearing obstacles such as trees or buildings which lie in the path of the radio signal. (For more information about line-of-sight issues, see page 34.) Masts are generally mounted on the roof and may be 10-50 feet in height. If a mast is used in your implementation, be sure it is tied down properly to minimize the risk of wind damage.

Radio towers are generally independent structures erected to raise antennas when extended distances are desired. They may also be required when tall buildings (larger than three stories) or topographical features lie directly in the path of the radio signal between two antennas. Towers can be erected at heights of 50 feet and higher. Obviously, depending on the application, the cost of erecting tall towers can be prohibitive.

Radio towers are generally independent structures erected to raise antennas when extended distances are desired. They may also be required to achieve radio line-of-sight.

Data Cable. A network data cable is required to connect the wireless bridge to your internal network (to a hub, switch, or repeater). This cable is generally the responsibility of the individual entity. If the wireless bridge is a significant distance from the network equipment, installation of this cable may require a cable installer. In this case, be sure to discuss the cable run with your wireless installer when the system is being specified.

Throughput vs. Data Rates

A last word regarding wireless connectivity is appropriate. In Table 9 on page 62, I listed the theoretical download times of a Tom Clancy novel using various connection types. These are theoretical because real network transmission involves some “overhead,” or additional information sent to aid in delivery of the actual data.

On a network, data is divided into pieces and packaged for transmission over the network. Called *packets*, these pieces all have additional information attached to them. Think of the attached information as an “address label” for the packet. At minimum, the “label” has the address of its destination on the network and that of its sending computer. It also has a sequence number so that the pieces can be reassembled in proper order. (There are other items included as well, but these will do for our purposes.)

Because of this added information, the data transfer rate associated with any medium refers to the maximum

amount of total data transmitted per second, including address labels. The actual data content transmitted is less.

In wireless networking, there is even more overhead than encountered in cabled connectivity. Because a radio is used, a small slice of time is used to switch from transmit to receive mode. Other internal functions required to receive data signals from the bridge and alter them to work over a radio connection consume more slices of time. Since time lost equals data throughput lost, a radio connection generally is not as efficient as a direct-cabled connection.

Two specifications are normally provided for wireless bridges. The term *data rate* is normally used to specify the theoretical bit transfer rate of a particular implementation of radio frequency transmission. Throughput specifies the maximum amount of data that can be pushed across the link. Some spreading technologies are more effective than others, so the throughput will vary.

As a rule of thumb, you can take the data rate and divide it in half to obtain an estimate of actual throughput. In my estimates of throughput in Table 2 on page 26, I included a range of throughputs for each performance level of wireless bridge: the low end is the one-half-data-rate rule, and the high end is the average of vendor claims for throughput.

Summary

In this chapter we have discussed the technical aspects of radio frequency wireless network connectivity. Here are some of the points we made:

- Radio waves are like light waves—they are electro-magnetic energy traveling at the speed of light.
- *Frequency* equals the number of waves that pass a specific point in one second. The measure of frequency is *hertz*.

- There are three license-free radio frequency bands used in radio frequency wireless networking. These are called the *ISM bands* (Industrial, Scientific, and Medical).

- *Spread spectrum* transmission enables multiple wireless transmissions over the same frequency bands without interference.
- The two spread spectrum techniques are called *frequency hopping spread spectrum* and *direct sequence spread spectrum*.
- There are several components required to implement an RF wireless network link:
  - Wireless bridges
  - Optional software feature sets
  - Antennas, directional and omni-directional (for multi-point connections)
  - External cables
  - Lightning arrestors
  - Masts or Towers
  - Data cable (from bridge to network hub)

CHAPTER NINE

Sharing Without Sacrificing: Securing Wireless Networks

One misconception I've seen in print sources about wireless network communications is that they are prone to being intercepted. The reasoning is as follows: data signals are transmitted across the open airwaves, so anyone with an antenna can pick them up, somewhat like eavesdropping on a wireless phone conversation. It's an unfortunate misconception, especially if it keeps managers and decision-makers from considering the merits of wireless networking.

Because of the confusion, it seems appropriate to include a brief discussion of the security of wireless connections. To complement the foundational components of LANs, WANs, and MANs included in Chapters 6 and 7, I have included additional security topics as well. Hopefully, these will be helpful when a library or school administrator submits budget requests involving security equipment and the professional services required to secure the network.

Security in a Wireless Environment

First, let's tackle the concept of security as it applies to wireless networking.

When we discuss the "interceptibility" of wireless data communications, there are a couple of things to keep in mind. First, the communications are data communications, not voice communications. It's not something that can be listened to. So the reception is going to take more than a simple antenna. In fact, it will also take a wireless bridge

from the same manufacturer as the one used in the transmission. So casual eavesdropping is ruled out.

Secondly, remember from our discussion of antennas in the previous chapter (see page 99) that the antennas, at least in a point-to-point connection, have to be well aligned to receive the signal. So now our eavesdropper not only has to have a few thousand dollars to acquire a wireless bridge, but must also erect his or her receiving antenna roughly in line with the two antennas in the wireless connection.

Wireless links are no more insecure than regular local area network links. It is much easier to try to tap the emanations from the wiring in your local network where it runs along an outside wall.

Third, in our discussion of spread spectrum transmission, we mentioned that a hopping code or spreading code is used to spread the signal across a wide band of radio frequencies. Both the transmitting and receiving units must use the same code in order for the receiving unit to correctly receive the signal. Now the eavesdropper has to reconfigure the unit repeatedly to gain the correct spreading code.

Last of all is a topic we haven't mentioned. Many wireless bridge manufacturers include encryption technology in their bridges. And encryption software is available for purchase separately to secure all network communications. With DES (Data Encryption Standard) encryption, approved by the U.S. government, trying to steal the signal becomes far more trouble than its worth in most cases.

Wireless links, therefore, are no more insecure than regular local area network links. If a thief is bent on intercepting your network communications, it will be much easier to try to tap the emanations from the wiring in your local network where it runs along an outside wall. And it will be even easier to try to break through your Internet connection to your internal network. This last option is also much cheaper!

The moral? Buy the encryption module if it isn't already included in the base cost. Encrypt the wireless link, then worry about your more pressing vulnerability: your Internet connection.

"Hackers" and "Crackers"

So who are these dangerous people I've called eavesdroppers and thieves? In network jargon, they are called

crackers. Most of us haven't seen their work directly, but we've heard about them. *Crackers* are computer users who break into computers in order to read, copy, or delete data files and perhaps use one computer as a jumping off point to break into other computers. They also break into telecommunications systems. Some are just joyriders: they just want to see which systems they can break into. Others are thieves: they want to find sensitive information and steal, use, or destroy it.

Crackers are unlike hackers. *Hackers* are characterized as having an intense curiosity about how computers work and sometimes create software to work around the limitations of operating systems. This curiosity and sense of independence have both good and bad sides. As an example of a good end, hackers have generally made it possible to do things with a computer that the original operating system designers never considered. On the other hand, cracking seems to have only negative consequences. (However, crackers have been hired by reputable companies to test system security. The crackers report on their activities and their ability to break into the systems. The vendor then uses this information to strengthen its defenses.)

Crackers have gained attention over the past few years due to the wild implementation of Internet access by various companies around the world. And as crackers learn to break into systems, another group of security experts learns how to sew up the holes. Which leads us to our second security topic.

Perimeter Defenses

Tom Sheldon, in his book *Windows NT Security Handbook*, offers the best security analogy I've read. It compares crackers trying to break into a network to an enemy horde trying to breach the defenses of a castle. Castles, with their high walls and battlements were very effective in repelling attacks in their day. But as added defenses, nobles had a moat built around the castle. The moat slowed enemies down enough that defense was even easier. Some castles had a series of moats, making the attack even more difficult. Sheldon suggested that adding circles of razor wire and land mines would set up a warning system so castle defenders would know when intruders were approaching.

All these layers are typically called *perimeter defenses* or *perimeter security*. They extend all the way from these outside warning devices to the castle walls. In network-speak, the device required to perform these functions is a firewall. A *firewall* is a computer with specialized software that examines all the data that tries to cross from one network to another. The firewall encompasses a set of rules, determined by the organization, defining which data can come into the organization's network and to which specific resources it can be transmitted. It may also provide rules defining which computers on the organization's network may connect to an external resource—the Internet, for example.

The firewall encompasses a set of rules, determined by the organization, defining which data can come into the organization's network and to which specific resources it can be transmitted.

With a firewall, a network administrator can set "traps," or alerts, when certain types of network requests are made. These correspond to the razor wire and land mines, warning of a possible intruder. Being forewarned, an astute network administrator can then monitor the cracker's behavior and possibly learn how to further secure his or her network. Along with the denial-of-entry capability of a firewall, logs of user activity and traps assist the administrator in reasonably securing the network against intruders.

Firewalls need to be standard equipment when multiple entities create common network infrastructure. They go a long way in helping prevent unauthorized entry. In a municipal network connecting the local networks of the school, public library, and other public agencies, a separate firewall should be installed for each entity's network. Usually, the firewall will be located between the entity's primary network hub and the router, bridge, or switch used to connect its local network to the shared network.

In addition to a firewall, many entities install a computer called a proxy server. (To make things really confusing, some proxy servers have firewall capabilities. These are sometimes called *firewalling proxy servers*.) A proxy server enhances a site's security by hiding the identity of every computer on the internal network. When local users request access to resources located outside the local network, the requests are first forwarded to the proxy server. The proxy server then substitutes its own computer identification for the internal user's computer. When responses are received, the proxy server determines which local computer is the recipient and forwards the response to it. Any

crackers who monitor network traffic see only the identification for the proxy server.

Brute force denial-of-entry and hidden identities make a network much less susceptible to penetration by outside threats. By installing these devices and diligently monitoring access attempts, an organization will repel most attempts to break into its network.

Keeping Crackers Out (From the Inside)

However, preventing unauthorized access to network resources from the outside solves only half of the problem. Unauthorized access can occur from inside the organization's walls as well. And most anecdotal evidence indicates that threats of electronic theft or sabotage are greater from employees and individuals inside the organization than from persons outside. Disgruntled employees are a common source of unauthorized access.

The first defense against undesired access to data resources is the implementation of user authentication.

The first defense against undesired access to data resources is the implementation of user authentication. Authentication techniques get more sophisticated as the computer industry matures. Here are some of the means employed to make sure users are who they say they are.

- User login—user name and password required
- Security tokens—requires a key, computer-generated "token," or encoded data card (smart card) to identify the user
- Biometric devices—fingerprint readers, retina scanners, and other devices which uniquely identify a user

All of these systems have good points and bad points. From a cost and maintenance standpoint, typical user login procedures are the only truly viable means of authentication for many public entities. They are the simplest to implement and the easiest to maintain. On the other hand, they are also the easiest to crack. Users can share their user names and passwords. If not managed well, passwords can to be very easy to "crack."

General Network Suggestions

- Implement an environment where users are required to log on to use computer resources. This provides a foundation from which suspicious activity can be traced.
- Install software to analyze user activities and system activity logs. Doing so enables the organization to detect suspicious activity before a full-blown break-in occurs.
- Provide sufficient training to end-users. Especially be sure that users are aware of the dangers of not logging off their computers. Such dangers include the ability of a third-party to sit at an "open" computer and assume the user's identity. The unauthorized person has all the rights and privileges of the logged in user. Any suspicious activity will be traced back to the user's login, not to the unauthorized person.
- In a Windows NT environment, don't log in as the network "Administrator" from end-user computers. Windows NT stores the user name and password for all logins on the local hard drive, which the end-user or an unauthorized user may later be able to crack. If an unauthorized user learns the Administrator password, the entire network is open to attack.
- Be very careful in allowing staff to dial in to their work computer from home. Any cracker equipped with automatic dialing software can discover the modem. To access the network, all a cracker needs to do is "guess" a user name and password.
- Public libraries and some schools have "public" computers anyone can use. In order to minimize the threat of unauthorized access to network resources, install these computers on a "public" network segment, or "demilitarized zone." This can be done with many firewall products.

These are some very basic suggestions. The subject of network security is a large one. Many good books are available for those interested in a fuller treatment of the subject. Two are listed in Appendix C, "Other Resources."