PART I

Overview of Cabling Technology

CHAPTER 1

Types of Cable and Hardware

As the demand for high-speed telecommunications increases across the globe, copper, fiber optic, and wireless systems are being deployed to fulfill the needs of telephone companies, cable TV companies, and businesses with high-speed LANs. The battle for supremacy between copper, fiber, and wireless systems in telecommunications and data communications continues to increase in complexity rather than becoming more clear. This has put serious pressure on the copper wire and cable industry, which has seen its market share decline steadily over the past decade as fiber and wireless systems take hold. A number of major copper cable suppliers have either pulled out of the copper cable business and embraced fiber optics or redesigned their organizations around adding value to traditional copper wire and cable products. This has provided market opportunities for some nimble market-oriented firms with lower manufacturing costs to enter niche markets.

The copper-based network equipment manufacturers continue to fight back, using recent developments in digital signal processing technology to extend the bandwidth and usefulness of copper cabling, in order to preserve both the embedded base of copper cabling and to retain market share for present and future installations. In the telephone network, asymmetric digital subscriber line (ADSL), high-bit-rate digital subscriber line (HDSL), and very-high-data-rate digital subscriber line (VDSL) technologies are delivering megabit speeds over the local loop, allowing for the delivery of high-speed Internet access, telecommuting, and eventually video services. For premises networks,100 Mbps (megabits per second) Ethernet equipment has quickly eclipsed fiber distributed data interface (FDDI) technology, and standards are underway for gigabit Ethernet and copper-based asynchronous transfer mode (ATM) LANs.

This chapter provides detailed assessments of competing cable types and hardware technologies and discusses cabling solutions for telecommunications and data networks with an emphasis on Network+ (N+) certification, which sets the stage for the rest of this book. Network+ is a new testing program from the Computing Technology Industry Association (CompTIA) [1]. Attaining Network+ certification indicates that the individual knows how to configure and install the TCP/IP client. In other words, N+ is substantially more than how to configure and install the TCP/IP client, it covers network topologies, technology, cable section, WANs, and so on.

Network+ is a new testing program intended to certify networking technicians with 18 to 24 months of experience. This certification is the logical next step for those who have already attained A+ certification. The point here is that this book is not an A+ or N+ specific certification study guide, but it does target N+ students and graduates. For further information on A+ and N+ certification, see the Introduction.

This chapter also describes the global copper cable market and briefly analyzes the effect of sweeping regulatory reforms standards. Finally, this chapter also provides major players in the fiber optics, copper cable, and wireless industry (copper wire manufacturers, copper wire companies seeking joint ventures or acquisitions, copper producers, telecommunications suppliers, telecommunications systems vendors, fiber optics manufacturers, networking equipment vendors, investors, consultants, long-range planners, strategic planners, and executives like presidents and CEOs) with a brief look at the range of strategies that can be pursued in order for them to remain competitive in this changing marketplace.

COPPER, FIBER, OR WIRELESS MEDIA: CHOOSE ONE

Perhaps your company thrives on copper cabling. Perhaps you're considering fiber optic alternatives. Or maybe you have problems that only a wireless LAN can solve.

Private network providers are often involved with providing systems to support future applications, while at the same time they're confronted with the seemingly contradictory objectives of lowering costs. Today, network providers are often faced with the question of whether to install an unshielded twisted pair (UTP) copper or multimode fiber cabling system or a wireless local area network (LAN) when searching for an answer to these objectives.

Unfortunately, this question does not have a clearly defined answer. In order to create the most cost-effective networks for voice, video, and data, most private networks require a mixture of all three media. UTP is unquestionably the right choice for traditional telephone and fax services. However, the answer is not as clear for data services. With rates from 100 to 155 Mbps, high performance Category 5 UTP provides the lowest initial cost for LANs. Nevertheless, recurring operational costs can be reduced by fiber-based networks. Furthermore, with wireless systems, you can bring 21st-century technology to older buildings without disturbing a single historic brick, go mobile for on-the-spot presentations, and even create instant extensions to an existing LAN anywhere in the building. These savings can, over time, far exceed the higher initial costs.

By definition, cable is the medium through which information usually moves from one network device to another. As previously mentioned, there are several types of cable media that are commonly used with LANs. In some cases, other networks will use a variety of cable media, while a network will utilize only one type of cable media. The type of cable media chosen for a network is related to the network's size, topology, and protocol. Therefore, what is necessary for the development of a successful network is an understanding of the characteristics of different types of cable media and how they relate to other aspects of a network.

The choice of media depends largely on the customer's present and future applications and business situations. A selection made without considering these fundamentals has little chance of providing the best solution. That is why it is important to understand not only the capabilities of each media, but also specific customer needs.

Overall, this chapter briefly examines the situation surrounding each of the cable media today and when and how to use them. The following sections discuss the types of cable media and hardware used in networks and other related topics.

COPPER MEDIA

If cost concerns are more critical than high bandwidth, you should consider a copper media cabling solution. There are two main reasons for the broad acceptance and rapid growth of copper media: low initial cost and the ability to deliver high data rate LAN services.

Copper media encompasses basically two major types of cable: unshielded twisted pair (UTP) and shielded twisted pair (STP). There is also a third type, coaxial cabling, which will also be discussed.

Unshielded Twisted Pair Cabling

Twisted pair cabling comes in two varieties: unshielded and shielded. Unshielded twisted pair (UTP) is the most popular and is generally the best option for school networks, as shown in Figure 1–1 [2].

UTP can support telephone, 4- and 16-megabyte per second (Mbps) token ring, Ethernet, 100 Mbps Ethernet, copper fiber distributed data interface (CFDDI), 155 Mbps asynchronous transfer mode (ATM), and is generally deployed as the cable of choice for many installations. UTP cable is rated by the Electronic Industry Association/Telecommunication Industry Association (EIA/TIA) standards into categories, which are shown in Table 1–1.

Currently the best value on pricing is Category 3 and Category 5. Category 3 is the low price choice for today's cable plant, and there are plans to support 100 Mbps over Category 3 cable by using all 4 pair (100BASE-T4, for example). The price gap between Category 4 and Category 5 is so small that most people are going right to Category 5.

You may hear of Level 5 cable. Underwriters Laboratories (UL) rates cable from Levels 1 to 5. Levels 3–5 correspond to Categories 3–5. UL Levels 1 and 2 are voice grade cable, not normally deployed with data transmission requirements.

UTP cable is generally wired in a star topology, with the troubleshooting advantages associated with stars. Although most of the topologies require only 2 pair (4 wires), the specific 2 pair used varies by network type (see Chapter 6, " Network Design Issues," for more information on topologies). Telephone requires only 1 pair for a single-line phone. Normal data network deployments are done with 4 pair cabling so that it will support any possible combination without requiring you to put new connectors or reterminate each connection if you change network types.

UTP quality may also vary from extremely high-speed cable to telephone-grade wire. Four pairs of cable wires exist inside the jacket. In order to help eliminate interference from adjacent pairs and other electrical devices,

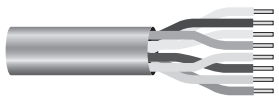

Figure 1–1 Unshielded twisted pair.

each pair is twisted with a different number of twists per inch. As previously stated, the Electronic Industry Association/Telecommunication Industry Association (EIA/TIA) has also established standards of UTP and rated five categories of wire, as shown in Table 1–1. For further information on these UTP standards, see Chapter 3, "Standards."

Table 1–1 Categories of Unshielded Twisted Pair

Category	*Use*
1	Alarm systems, voice only (telephone wire), characteristics specified up to 0 (MHz) and other noncritical applications.
2	Voice, EIA-232, data to 4 Mbps (LocalTalk), characteristics specified up to 0 (MHz) and other low speed data.
3	10BaseT Ethernet, 4-Mbits/s token ring, 100BaseT4, 100VG-AnyLAN, basic rate ISDN, data to 10 Mbps (suitable for Ethernet) and characteristics specified (rated) up to 16 (MHz). Generally the minimum standard for new installations.
4	16-Mbits/s token ring. Not widely used, data to 20 Mbps (16 Mbps suitable for token ring) and characteristics specified up to 20 (MHz).
5	TP-PMD, SONet, OC-3 (ATM), 100BaseTX. The most popular for new data installations, data to 100 Mbps (suitable for Fast Ethernet) and characteristics specified up to 100 (MHz) and ATM (155 Mbps).

The tightness of the twisting of the copper pairs is one difference among the different categories of UTP shown in Table 1–1. The higher the supported transmission rate and greater cost per foot, the tighter the twisting. Buy the best cable you can afford. Most schools purchase Category 5 or Category 3. Category 5 cable comes highly recommended.

Remember, the Category 5 cable will provide more room to grow as transmission technologies increase—especially if you are designing a 10 Mbps Ethernet network and are considering the cost savings of buying Category 3 wire instead of Category 5. A maximum segment length of 100 meters exists in both Category 3 and Category 5 UTP. In most schools, Category 5 cable is required for retrofit grants. Also, the specifications for unshielded twisted pair cable (Category 3, 4, or 5) carrying Ethernet signals is referred to as 10BaseT, as shown in Table 1–2.

Unshielded Twisted Pair Connector

An RJ45 connector is the standard connector for unshielded twisted pair cabling. This is a large, plastic, telephone-style connector (Figure 1–2) [3]. The placement of a slot allows the RJ45 connector to be inserted only one way. RJ stands for registered jack. The implication here is that the connector follows a

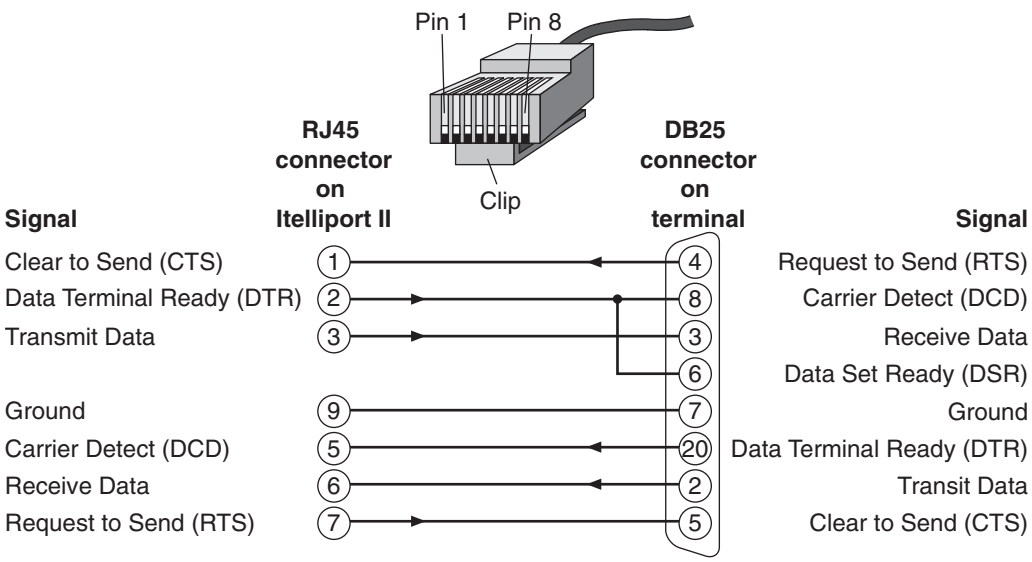

Figure 1–2 RJ45 connector.

standard borrowed from the telephone industry. Thus, which wire goes with each pin inside the connector is designated by this borrowed standard.

Shielded Twisted Pair

STP has come to mean two entirely different types of cable. The original STP cabling was proposed by IBM and was used for token ring networks. It sported a universal data connector (UDC), which was large and neither male nor female (the connectors could always plug into each other). The cable was bulky, and had a shield around each pair, plus a shield around all of the pairs. It was rated to 16 MHz. IBM called this Type 1 cable.

Type 1 STP cable really doesn't have much of a future except in IBM's token-ring shops, due to its low speed, bulkiness, connector size, and one-network support.

Recently, a new version of STP cable has been introduced. Instead of shielding around each pair, it has only one shield around the entire cable. This type of STP cabling uses an RJ45 connector with some metal on it so that the system can be grounded. It's not bulky, and it's easy to work with and terminate.

The jury is still out on whether or not this shielding is needed, but proponents say it will become critical as 155 Mbps signals are transmitted for ATM usage. Electromagnetic interference (EMI) tests show that STP cable radiates less signal than UTP cable. Overall, though, the new STP has all the advantages of UTP, and perhaps better signal carrying capability. While most technicians choose UTP for their installation, STP warrants a close watch.

In other words, a disadvantage of UTP is that it may be susceptible to radio and electrical frequency interference. Shielded twisted pair (STP), on the other hand, is suitable for environments with electrical interference. However, the extra shielding can make the cables quite bulky. Shielded twisted pair is often used on networks using token ring topology, the industry standard (Project 802.5 of the IEEE) that specifies protocols for connection and transmission in local area networks. As a media access method, it operates at layers 1 and 2 in the OSI (Open System Interconnection) model. Token ring transmits at 4 or 16 Mb/s.

A Comparison: STP Versus UTP

This section continues the debate of UTP versus STP, presenting an indepth comparison of the advantages and disadvantages of how and when to use cables and systems.

A debate has recently arisen on the advantages and disadvantages of unshielded twisted-pair (UTP) cable and shielded twisted-pair (STP) cable. Without adequately presenting both sides of the story, advocates of STP cable (a category that includes screened twisted-pair cable and foil twisted-pair cable) have attempted to claim that their product is superior to UTP cable. In order to provide reliable connectivity of electronic equipment, STP and UTP's purpose should still be the same, even though it is true that they are inherently different in design and manufacture. The true test comes when you look at the performance of each of these cable types within its respective end-to-end system, although, in theory, both types of cable should perform this task successfully.

In order to form a twisted pair, two copper wires, each encased in its own color-coded insulation, are twisted together. But, to form twisted-pair cable, multiple twisted pairs are packaged in an outer sheath, or jacket. The possibility of interference between pairs in the same cable sheath can be minimized by varying the length of the twists in nearby pairs.

Twisted-pair cable has been around for quite a while. In fact, early telephone signals were sent over a type of twisted-pair cable. Just about every building today still uses twisted-pair cable to carry telephone and other signals. Evolving from 1200 bps to over 100 Mbps, signals have become more

complex over the years. Today, there are many more sources of interference that might disrupt those signals than there were at the turn of the century. Coaxial cable and fiber optic cable were developed to support emerging technologies and handle higher bandwidth applications. Now, high-data-rate signals can be carried because of the evolution of twisted-pair cable.

To reduce the potential for electromagnetic interference (EMI), some twisted-pair cables contain a metal shield. Signals from other sources such as electric motors, power lines, high-power radio, and radar signals cause EMI. If these signals are in the vicinity, they may cause disruptions or interference, called noise. Thus, STP cable encases the signal-carrying wires in a conducting shield. At first glance, it may appear that because STP cable is physically encased in a shield, all outside interference is automatically blocked. However, this is not true.

The shield acts as an antenna (just like a wire) when it has been properly grounded, converting received noise into current flowing in the shield. In turn, this current induces an opposite and equal current flowing in the twisted pairs. The two currents cancel each other out and deliver no net noise to the receiver as long as they are symmetrical. However, the current in the twisted pairs is interpreted as noise if any discontinuity in the shield or other asymmetry in the current in the shield exists. As long as the entire end-to-end link is shielded and properly grounded, STP cable is effective at preventing radiation or blocking interference. Every component of a shielded cabling system must be just that—fully shielded—in order to work properly.

STP cable also has drawbacks. For instance, STP cable's attenuation may increase at high frequencies. Also, STP cable's balance (or longitudinal conversion loss) may decrease if the effects of the shield are not compensated for (which leads to cross talk and signal noise). The shielding effectiveness depends on the material of the shield, its thickness, the type of EMI noise field, its frequency, the distance from the noise source to the shield, the grounding structure used, and any shield discontinuity. There's also no guarantee that the shield itself will contain no imperfections.

A thick, braided shield is used by some STP cables. Harder to install than their UTP counterparts, these cables are heavier and thicker. A relatively thin overall outer foil shield is also used by some STP cables. Thinner and less expensive than braided STP cable, these cables are also known as screened twisted-pair (ScTP) cables or foil twisted-pair (FTP) cables. However, they are not any easier to install. When these cables are installed, the minimum bending radius and maximum pulling tension force must be rigidly observed; otherwise, the shield may experience a tear.

On the other hand, UTP cable does not rely on physical shielding to block interference. But UTP does rely on balancing and filtering techniques through media filters and/or baluns. Noise is induced equally on two conductors. The noise then cancels out at the receiver. This technique is easier to maintain than the shielding continuity and grounding of an STP cable if the UTP cable has been properly designed and manufactured.

UTP cable has evolved over the years, with the result that there are different varieties of UTP cable available for different needs. Basic telephone cable (also known as direct-inside wire, or DIW) is still available. Improvements over the years (such as variations in the twists or in individual wire sheaths or overall cable jackets), have led to the development of EIA/TIA-568 standard-compliant Category 5 (for specifications on signal bandwidth up to 100 MHz and greater) UTP cable, Category 4 (for specifications on signal bandwidth up to 20 MHz), and Category 3 (for specifications on signal bandwidth up to 16 MHz). Millions of nodes have been and continue to be wired with UTP cable (even for high-data-rate applications), because UTP cable is lightweight, thin, and flexible, as well as versatile, reliable, and inexpensive. UTP cable should be used as part of a well-engineered structured cabling system for best performance.

STP Cabling Systems Versus UTP Cabling Systems

Overall signal quality will be degraded if STP cable is combined with improperly shielded connectors (connecting hardware or outlets, or if the foil shield itself is damaged). Also, degradation of emission and immunity performance can often result if the connectors are improperly shielded. Therefore, every component within the cabling system must be fully and seamlessly shielded, as well as properly installed and maintained for it to succeed totally in interference reduction.

An STP cabling system, likewise, requires good earthing and grounding practices. A primary source of emissions and interference can result if a system is improperly grounded. The frequency of the application dictates whether this ground is at one end or both ends of the cable run. At a minimum (for high-frequency signals), an STP cabling system must be grounded at both ends of the cable run, and, it must be continuous. There is no effect against magnetic field interference if a shield is grounded at one end. A source of problems can also be the length of the ground conductor itself. It no longer acts as a ground if it is too long. Therefore, since it depends on the application, optimum grounding for an STP cabling system is not possible. This problem does not exist with UTP cabling systems.

A UTP cabling system inherently has fewer points for potential failure and is easier to install. Moreover, an STP cabling system is dependent on

such factors as physical continuity of the cable shield itself or installation with adequately shielded and grounded components.

EMC and STP Versus UTP Cabling Systems

Another factor to consider when choosing a cabling system relates to the recent adoption of the electromagnetic compatibility (EMC) directive. This directive is in addition to requirements for precision design and manufacture, as well as end-to-end integrity. EMC refers to the ability of an electronic system to function properly in its environment. This would be an environment where several pieces of equipment are located in the same workspace, each radiating electromagnetic emissions. EMC becomes increasingly more important here (with the existence of an increased amount of electronic equipment in the average workspace) as excess radiation from one piece of equipment can adversely affect performance of another piece of equipment. This means that every electronic system (which includes either an STP or UTP cabling system) must meet this directive.

EMC regulations have existed for years in some countries, such as the U.S. and Germany. However, attention on EMC has refocused since the implementation of the European EMC Directive in 1989. The European EMC Directive 89/336/EEC states that all electronic equipment and apparatus must comply with the directive. These systems must pass the essential requirements of the directive before they can be sold anywhere in the European Economic Area (EEA). Some national regulations (such as Amtsblatt Verfugung 243/91 of Germany) exempted STP-based systems from immunity testing. However, as of January 1, 1996, these national regulations no longer apply, and all systems must be tested. Those that do not pass will not be able to be sold in the EEA.

How well do STP- and UTP-based systems stand up to rigorous EMC testing? Not all STP based systems can automatically pass EMC tests (contrary to some popular assumptions), while a well-designed UTP cabling system can. Further discussions on this topic will be addressed in Chapter 5, "Types of Vendor and Third-Party Cabling Systems."

Coaxial Cable

Now let's briefly look at the third type of copper media: coaxial cabling. This is the copper media type most frequently used in cable television systems, the transmission line for television and radio signals.

Coaxial can be a good solution for small networks. Because it is generally wired in a bus topology, it requires less cable than other solutions and doesn't require a hub. Generally it is easy to install the connections. Coaxial

Figure 1–3
Coaxial cable.

also offers relatively high immunity to interference from noise sources, so it is often used in manufacturing environments.

Coaxial cabling has a single copper conductor at its center. A plastic layer provides insulation between the center conductor and a braided metal shield, as shown in Figure 1–3 [4]. As previously mentioned, the metal shield also helps to block any outside interference from fluorescent lights, motors, and other computers.

Coaxial cabling is highly resistant to signal interference, despite the fact that it is difficult to install. Also, it can support greater cable lengths between network devices than twisted pair cable. The two types of coaxial cabling are thin coaxial and thick coaxial.

Thin coaxial cable is also referred to as thinnet. 10Base2 refers to the specifications for thin coaxial cable carrying Ethernet signals, as shown in Table 1–2 [5]. The *2* refers to the approximate maximum segment length of 200 meters. In actual fact, the maximum segment length is 185 meters. Thin coaxial cable is popular in school networks, especially linear bus networks.

Table 1–2 Ethernet Cable Comparison Summary

Cable Type	*10BaseF*	*10Base5*	*10Base2*	*10BaseT*	*Single-Mode Fiber*	*Multi-mode Fiber**	*Standard AUI*	*Office AUI*
Maximum length	2000 m	500 m	185 m	100 m	5 Km	1 Km	50 m	16.5 m
Number of taps	n/a	100	30	n/a	n/a	n/a	n/a	n/a
Tap spacing	n/a	2.5 m	5 m	n/a	n/a	n/a	n/a	n/a
Propagation delay	n/a	≤ .00433	≤ .00514	≤ .0057	≤ .005	≤ .005	≤ .00514	≤ .0156
Maximum segment delay	n/a	2.165 micro-seconds	.95 micro-seconds	1.0 micro-seconds	25 micro-seconds	5.0 micro-seconds	.257 micro-seconds	.257 micro-seconds
Velocity of propagation	n/a	≥ .77 c	≥ .65 c	≥ .585 c	≥ .66 c	≥ .66 c	≥ .65 c	≥ .65 c

* The IEEE 802.3 Fiber Optic Inter-Repeater Link (FOIRL) standard specifies 1 kilometer, while the 802.3j standard allows for 2 kilometers.

Thick coaxial cable is also referred to as thicknet. 10Base5 refers to the specifications for thick coaxial cable carrying Ethernet signals, as shown in Table 1–2. The *5* refers to the maximum segment length of 500 meters. Thick coaxial cable has an extra protective plastic cover that helps keep moisture away from the center conductor. This makes thick coaxial a great choice when running longer lengths in a linear bus network. One disadvantage of thick coaxial is that it is difficult to install and does not bend easily.

However, there are some disadvantages to coaxial. The same bus topology that makes it less expensive makes it more difficult to isolate problems. Currently its LAN use is pretty much confined to 10BASE2 Ethernet. The new high-speed networks are not supporting coaxial, so this cabling may be a dead end.

Coaxial used for Ethernet networks is 50 ohms. Coax for cable television (CATV) is 75 ohms. Using the wrong cable for your network will cause network problems.

Ohms is defined as a measure of resistance. One ohm allows one ampere of current to flow across a one-volt potential.

Coaxial Cable Connectors

The most common type of connector used with coaxial cables is the Bayone-Neill-Concelman (BNC) connector, shown in Figure 1–4 [6]. Different types of adapters are available for BNC connectors, including a T-connector, terminator, and barrel connector. The weakest points in any network are the connectors on the cable. Always use the BNC connectors that crimp, rather than screw onto the cable, to help avoid problems with your network. For further information on copper media, please see Chapter 10, "Copper Design Considerations."

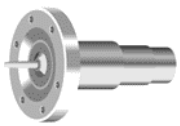

Figure 1–4 BNC connector.

FIBER OPTIC MEDIA

Let's look at the next type of cabling media: fiber optic cable. With the relentless pursuit of bandwidth, fiber optic cabling is being deployed at an ever increasing rate. This cable, which uses glass to carry light pulses, poses both advantages and challenges. Fiber optic cabling has much to offer, and in most cases, its use will provide benefits that warrant the implementation. We will get into an indepth discussion of fiber optic cabling in Part III, "Fiber Optic Systems: A Hands-On Approach" (Chapters 12–20).

Furthermore, fiber optic cable offers the possibility of near infinite bandwidth and perfect immunity to noise. The trade-off is simply cost and difficulty in installation. It costs significantly more to purchase fiber optic cable, connectors, patch panels, jumper cables, tools, and network interface cards (NICs).

Since the invention of the telegraph by Samuel Morse in 1838, there has been a constant push to provide data at higher and higher rates. Today, the push continues. Just as RS-232 attached terminals gave way to 10 Mbps Ethernet and 4 and 16 Mbps token ring. These are giving way to Fast Ethernet (100 Mbps), FDDI (100 Mbps), ATM (155 Mbps), Fiber Channel (1062 Mbps), and Gigabit Ethernet (1000 Mbps). With each of these increases in speed, the physical layer of the infrastructure is placed under more stress and more limitations. The cabling installed in many environments today cannot support the demands of Fast Ethernet, let alone ATM, Fiber Channel, or Gigabit Ethernet.

Fiber optic cabling thus provides a viable alternative to copper. Unlike its metallic counterpart, fiber cabling does not have the astringent speed and distance limitations that plague network administrators wishing to upgrade their networks. Because it is transmitting light, the limitations are on the devices driving it more than on the cable itself. By installing fiber optic cabling, the high cost of labor and the time associated with the cabling plant can be expected to provide service for the foreseeable future.

Plastic optical fiber (POF) technology is making fiber even more affordable and easier to install. Because the core is plastic instead of glass (more on cores and fiber construction follows), terminating the cable is easier. The trade-off for this lower cost and ease of installation is shorter distance capabilities and bandwidth limitations.

This section is intended to give you an understanding of fiber optic cable technology and its applications as well as presenting this light-speed technology through fiber optic systems, where 10BaseF (as shown in Table 1–2) refers to the specifications for fiber optic cable carrying Ethernet signals. It's one of the most sophisticated cabling media solutions available

today, with a range of more than 70 miles (120 kilometers) and certified performance up to gigabit speeds.

Fiber Optic Components

Fiber optic cabling consists of a center glass core surrounded by several layers of protective materials, as shown in Figure 1–5 [7]. It has the following components (starting in the center and working out): core, cladding, coating, strength member, and jacket (Figure 1–6) [Advanced Cable Connection Inc., 1]. The design and function of each of these will be defined later.

The core is in the very center of the cable and is the medium of propagation for the signal. The core is made of silica glass or plastic (in the case of POF) with a high refractive index (discussed in detail later). The actual core is very small (compared to the wire gauges that most of us are used to). Typical core sizes range from 8 microns (millionth of a meter) for single-mode silica glass cores and up to 1,000 microns for multimode POF.

Figure 1–5 Fiber optic cable.

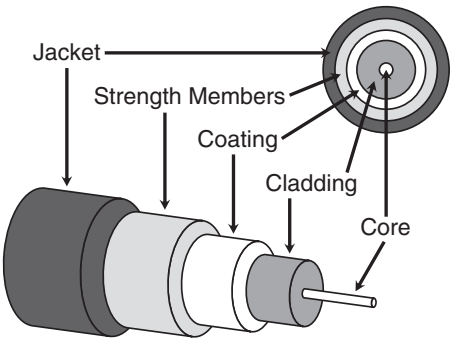

Figure 1–6 Fiber optic cable construction.

The cladding is a material with a lower index of refraction that surrounds the core. This difference in index forms a mirror at the boundary of the core and cladding. Because of the lower index, it reflects the light back into the center of the core, forming an optical wave guide. This is the same effect as looking out over a calm lake and noting the reflection, while looking straight down you see through the water. It is this interaction of core and cladding that is at the heart of how optical fiber works.

The coating (also referred to as buffer or buffer coating) is a protective layer around the outside of the cladding. It is typically made of a thermoplastic material for tight buffer construction and a gel material for loose buffer construction. As the name implies, in tight buffer construction, the buffer is extruded directly onto the fiber, tightly surrounding it. Loose buffer construction uses a gel-filled tube that is larger than the fiber itself. Loose buffer construction offers a high degree of isolation from external mechanical forces such as vibration. Tight buffer construction, on the other hand, provides for a smaller bend radius, smaller overall diameter, and crush resistance.

To further protect the fiber from stretching during installation, and to protect it from expansion and contraction due to temperature changes, strength members are added to the cable construction. These members are made from various materials from steel (used in some multistrand cables) to Kevlar. In single- and double-fiber cables, the strength members are wrapped around the coating. In some multistrand cables, the strength member is in the center of the bundle.

The jacket is the last item in the construction, and provides the final protection from the environment in which the cable is installed. Of concern here is the intended placement of the cable. Different jackets provide different solutions for indoor, outdoor, aerial, and buried installations.

So, how would you know which is the right fiber cable type for your network? The next section addresses this question.

The Right Fiber Optic Cable

One of the design considerations is the type of fiber to use when deciding to install optical fiber in buildings or across a campus. What should you install: single-mode (SMF), multimode (MMF), or both types of fiber? The choice is usually guided by a few key issues. For example, the primary considerations are: intended applications support, distance, data (baud) rate, and the difficulty and expense of retrofitting at a later time. Table 1–3 addresses the first three considerations for LANs and video applications.

Single-mode and/or multimode are fiber cable that use light pulses instead of electricity to carry data. In multimode cable, the light bounces off the cable's walls as it travels down, which causes the signal to weaken sooner and therefore data cannot travel as much distance as with single mode fiber. In SMF cables, the light travels straight down the cable. The size of the cable/cladding is 62.5/125 micron for MMF, and 8/125 micron for SMF.

Table 1–3 Standardized Distances for LANs over Single Mode and Multimode

Application	*Data rate*	*Fiber distance (meters) and type*	
		Single Mode (9/125 micron)	*Multimode (62.5/125 micron)*
10BaseF (Ethernet)	20 Mbaud	nonstandard	2,000
100BaseFX	125 Mbaud	nonstandard	2,000
100VG-AnyLAN	120 Mbaud	nonstandard	2,000
1000BaseX	1250 Mbaud	3,000	440 (draft)
ATM and SONET	155 Mbaud	40,000	2,000
	622 Mbaud	40,000	500
Baseband Video	6 MHz	65,000	10,000
Broadband Video	500 MHz	20,000	n/a
FDDI	125 Mbaud	60,000	2,000
Fiber Channel	133 Mbaud	nonstandard	1,500
	266 Mbaud	10,000	1,500
	531 Mbaud	10,000	350
	1062 Mbaud	10,000	300
Token Ring	32 Mbaud	2,000	nonstandard

As previously mentioned, the most common size of multimode fiber used in networking is 62.5/125 fiber. This fiber has a core of 62.5 microns and a cladding of 125 microns. This is ideally suited for use with 850 nm and 1300 nm wavelength drivers and receivers. For single-mode networking applications, 8.3/125 is the most common size. Its smaller core is the key to single mode operation (defined later).

Numerical aperture and acceptance angle are two different ways of expressing the same thing. For the core/cladding boundary to work as a mirror, the light needs to strike at a small/shallow angle (referred to as the angle of incidence). This angle is specified as the acceptance angle and is the maximum angle at which light can be accepted by the core, as shown in Figure 1–7 [Advanced Cable Connection Inc., 1]. Acceptance angle can also be specified as Numerical Aperture, which is the SIN of the acceptance angle (Numerical Aperture = SIN [acceptance angle]).

To date, all LAN standards specify 62.5/125 micron multimode fiber and some also specify single-mode fiber. Table 1–3 lists the standardized distances for LANs over both media. All LANs operating up to 266 megabaud have sufficient distance capability on multimode fiber to span most campuses. Above that rate, the distance capabilities of multimode fiber LANs are sufficient to cable most buildings using single-point administration (centralized cabling) architecture. For longer distances, single-mode fiber provides the LAN solution at these higher rates. Multimode-to-single-mode converters are available to convert multimode signals to single mode, even for those LANs where single-mode fiber is non-standard. Converters typically have 20- to 50-kilometer single-mode capability.

For video, multimode fiber is capable of delivering baseband (single channel) video over distances exceeding the span of most campuses. Multimode fiber is also capable of providing several channels of video (multichannel), but not capable of cost-effective broadband (20–80 channel) video delivery today. However, single-mode fiber is quite capable of providing broadband video services.

As Table 1–3 indicates, multimode fiber has the capability to meet both the distance and data rate demands of most LAN networks. Generally, multimode systems cost far less than single-mode systems, since the optoelectronics that can be used with multimode fiber are much less costly than those used with single-mode fiber. This cost advantage explains the popularity of multimode fiber over single-mode fiber in premises networks.

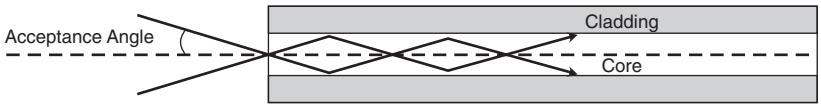

Figure 1–7 Fiber optic specifications.

Optoelectronics has a rapidly growing range of applications that includes optical communications, optical data storage, and optical sensing. It is fundamentally concerned with the interaction of light and matter and with devices that interface between electronics and optics.

However, single-mode fiber is practically the only fiber used by telephone and cable television companies. These industries require the very long distance capability and high information carrying capacity of single-mode fiber. In these longer distance applications, single-mode systems are cost-effective because fewer optoelectronic devices are needed overall.

Today, most premises networks are being installed with multimode fiber in the building backbone and campus backbone segments. Some forward-thinking companies are also installing single-mode fiber in backbones along with the multimode fiber.

"Backbone" is a fairly nebulous term for a part of the network that interconnects other parts of the network. For example, a campus might have an FDDI ring that interconnects a number of Ethernets. The FDDI ring could be called the network's backbone.

Multimode fiber is also growing in the horizontal cabling scheme, bringing the benefits of fiber all the way to the desktop. A few companies are even installing single-mode fiber to these work areas. Most of these companies are not using the single-mode fiber at this time, but are installing it in the event that they will need its higher information-carrying capacity in the future. Also, because of its popularity with telephone and cable television companies, single-mode fiber is capable of extending telephony and cable services throughout a campus. For information regarding cost-related issues with installing both single-mode and multimode fiber at the same time, see Chapter 24, "Installation."

Horizontal cabling extends from the telecommunications outlet/connector to the horizontal cross-connect. All horizontal wiring must be placed in a physical star topology with the floor wiring closet (FWC) as the center. Physical topology is a star (each telecommunications outlet/connector has its own mechanical termination position at the horizontal cross-connect in the telecommunications closet).

The published building cabling standards, ANSI/TIA/EIA-568-A, ISO/IEC 11801, and EN-50173, recognize both multimode and single-mode fiber for building and campus backbones. However, these standards do not recognize single-mode fiber for horizontal segments to the work area or desktop. This position reflects the present view of fiber-based services within premises networks, taking into consideration practical issues of active equipment availability, relative cost, and the remote likelihood of needing at the desktop the type of information-carrying capacity that single-mode fiber can provide. Looking into the future from a fiber distribution perspective, the most likely scenario (for data that may be delivered to a building or campus on single-mode fiber) is that the single-mode fiber will terminate at an electronic multiplexing device. This multiplexer then extracts lower-speed signals for delivery to the desktop over multimode fiber.

Looking into the future from a technology perspective, several technologies exist for extending the capability of multimode fiber. For example, no LAN standards have yet to use multilevel coding on multimode fiber to increase transmission capacity using less bandwidth, a technique very popular in copper-based LANs. Nor have any LANs used wavelength division multiplexing (WDM), which provides additional channels over the same fiber by using different colors of light. However, some multichannel video links on multimode fiber and long-distance telephony on single-mode fiber use WDM today. Also, new devices, such as short wavelength lasers and vertical cavity surface emitting lasers (VCSELs), are emerging as the transmitter technology capable of providing cost-effective gigabit-rate data links over multimode fiber.

Considering these largely untapped technologies, it appears that multimode fiber has the capability to provide desktop LAN services far into the future. In the backbone however, where speeds and distances are generally 10 times greater than to the desktop, the clear trend is toward single-mode solutions.

The remaining consideration is the cost of retrofitting a network with single-mode fiber at a later time. This issue depends on many variables that are customer-specific and often complex. For example, items such as the cable placement method (directly buried, in conduits, or aerial), obstacles (streets, lakes, rivers, fire stops), right-of-way passage, and work disruption all affect this decision. For these reasons it is often prudent, particularly in campus backbones, to place both multimode and single-mode cables at the same time. Again, for information regarding cost-related issues with installing both single-mode and multimode fiber at the same time, see Chapter 24, “Installation.”

It is important to install enough fiber to support the present and future applications that will simultaneously share the cable segment. Take into account the type and number of fibers that each application requires and add in spare capacity for future proofing. Generally, LAN applications will each require two fibers, while video applications will require one or two fibers depending on whether they are unidirectional or bidirectional. Video links that use bidirectional communications include those that return video, audio, camera control, or data signals. Add in at least 50 percent spare capacity and round the fiber count upward to the next standard cable size.

If you decide to place both multimode and single-mode fibers along the same route, the general recommendation is that you run separate cables for each type. Composite cable, with both multimode and single-mode fibers in one sheath, are specifically not recommended in outside plant (OSP) applications. Initially, these cable types may appear attractive. However, in practice, OSP composite cable can prove problematic because of increased difficulty in fiber-type identification. This can lead to inappropriate use of splice and connector hardware; and, unintended interconnection of multimode to single-mode fibers at splice points. Using separate OSP cables helps to identify and segregate the two fiber types, reducing confusion during installation, maintenance, and administration. Furthermore, composite cables have more limited availability and higher cost than noncomposite cable. However, for applications inside buildings, the issues of fiber-type identification and resulting mix-ups at splice and termination points have been mitigated by the design of composite building cables. The tight-buffer construction of the composite building cable uses a color-coded plastic coating over each individual fiber within the cable. This buffer carries special markings that easily identify the single-mode fibers within the cable. Therefore, the general recommendation would be to use the composite cable (see Figures 1–8 and 1–9) in buildings where both single-mode and multimode fibers are required along the same route [8].

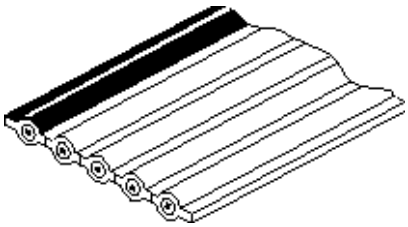

Figure 1–8 Composite cable.

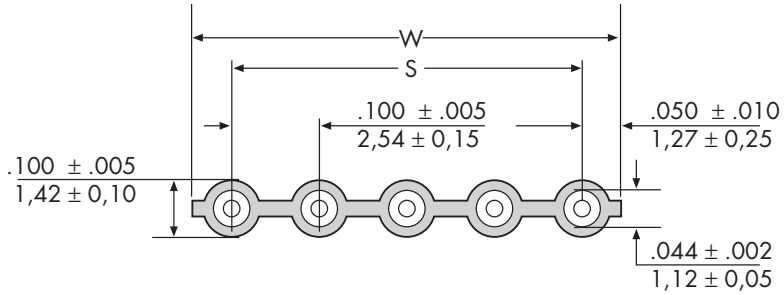

Figure 1–9 Composite cable circuit dimensions.

To improve the management of the fiber system for administration and record keeping, route the two fiber types to separate patch panels in closets or equipment rooms. The fiber type should be identified by distinctive labeling. Color coding the connectors and couplings (adapters) is recommended. The use of blue for single-mode and beige for multimode connections is consistent with ANSI/TIA/EIA-568-A, ISO/IEC 11801, and EN-50173.

Fiber Optic Transmitter

As previously mentioned, fiber optic cabling transmits light rather than electronic signals. This eliminates the problem of electrical interference. Fiber optic is ideal for certain environments that are subject to a large amount of electrical interference. Its immunity to the effects of moisture and lighting has also made fiber optic cabling the standard for connecting networks between buildings.

Fiber optic cable has the ability to transmit signals over much greater distances than twisted pair and coaxial. It also has the capability to carry information at vastly greater speeds. This capacity broadens communication possibilities to include services such as interactive services and video conferencing. The cost of fiber optic cabling is comparable to copper cabling. Nevertheless, it is more difficult to install and modify. A comparison between the two media is given later in the chapter.

There does appear to be an inconsistency as to the cost of fiber. On the one hand, the cost of fiber is substantially more than any other form of cabling. Some industry analysts suggest that it is comparable to copper. Though an argument could be made that fiber is reaching less expensive levels, and may very well be comparable to copper today, it is suggested that the industry analysts take one position or the other, not both.

Specifications

With a basic understanding of fiber construction, explanation of transmitters (the devices that put the pulses of light into the fiber) is in order. From a general level, there are three aspects of transmitters to discuss:

- Type of transmitter.
- Wavelength of transmitter.
- Power of the transmitter.

Transmitters can be divided into two groups: lasers and light emitting diodes (LEDs). LEDs are by far the most common, as they provide low-cost and very efficient solutions. Most multimode transmitters are of the LED variety. When high power is required for extended distances, lasers are used. Lasers provide coherent light and the ability to produce a lot of light energy. The drawbacks to lasers are their cost and electrical power consumption. Equipment using high-power lasers must provide cooling and access to a primary power source such as 120V AC.

Type of Transmitter. Transmitter types can also be broken down into single-mode versus multimode transmitters. Multimode transmitters are used with larger cable (typically 62.5/125 microns for most data networking applications) and emit multiple rays or *modes* of light into the fiber. Each one of these rays enters at a different angle and as such has a slightly different path through the cable. This results in the light reaching the far end at slightly different times. This difference in arrival times is termed "modal dispersion" and causes signal degradation. Single-mode transmitters are used with very small cable (typically 8/125 microns) and emit light in a single ray. Because there is only one mode, all light gets to the far end at the same time, eliminating modal dispersion.

The preceding explains what modal dispersion (MD) is, but does not explain how the system copes or facilitates the communication. Being that this is an introductory chapter, an explanation of how the system copes with MD will be reserved for later chapters.

Wavelength of Transmitter. The wavelength of the transmitter is the *color* of the light. The visible light spectrum starts around 750 nanometer (nm) and goes to 390 nm. The 850 nm transmitters common in multimode Ethernet can be seen because 850 nm is the center of their bandwidth and they emit some visible light in the 750 nm range, giving them their red color.

The 1300 nm and 1550 nm transmitters emit light only in the infrared spectrum. The difference in performance of the various wavelengths is beyond the scope of this section. What is important is an awareness of the wavelengths and that the equipment on both ends of the fiber needs to be matched.

Power of The Transmitter. The final characteristic of transmitters is the output power. This is a measure of the optical energy (intensity) launched into the fiber. It is measured in decibel milliwatt (dBm). A typical value for multimode transmitters used in Ethernet is –15 dBm. Single-mode transmitters have a wide range in power, depending on the application.

Fiber Optic Receiver Specifications

With a knowledge of transmitters, what happens at the other end of the cable is important. The light pulses are terminated and detected with a receiver. Receivers have three basic considerations. These are:

- Wavelength (discussed in the preceding).
- Mode (single vs. multi discussed in the preceding).
- Sensitivity.

Sensitivity is the counterpart to power for transmitters. It is a measurement of how much light is required to accurately detect and decode the data in the light stream. It is expressed in dBm and is a negative number. The smaller the number (remember –40 is smaller than –30), the better the receiver. Typical values range from –30 dBm to –40 dBm.

dB refers to decibel (dB); a unit of relative change of power (for example, –10 dB).

Receive sensitivity and transmitter power are used to calculate the optical power budget available for the cable. This calculation is:

```
Power Budget = Transmitter Power - Receiver Sensitivity
```

Using the typical values given for multimode Ethernet in the preceding, the power budget would be:

```
15 dBm = -15 dBm - (-30 dBm)
```

Therefore, the optical power budget must be greater than all of the cable plant losses (such as attenuation, losses due to splices and connectors, etc.) for the installation to work properly.

Fiber Optic Cable Connectors

Many different connector styles have found their way into fiber optic networking. The most common connector used with fiber optic cable is a straight tip (ST) connector. It is barrel-shaped, similar to a BNC connector. A newer connector, the subscriber connector (SC) is becoming more popular. It has a squared face and is easier to connect in a confined space. The SC connector has recently been standardized by ANSI TIA/EIA-568A for use in structured wiring installations. Many single-mode applications are now only available in the SC style.

FDDI, on the other hand, uses the medium interface connector (MIC), which is a duplex connector. It is physically larger then the SC connector, and the SC connector is gaining acceptance in the FDDI marketplace.

Copper Versus Fiber Cable

At this point in the chapter, it's appropriate to make a quick comparison of copper versus fiber media before going on to wireless media.

There are two main reasons for the broad acceptance and rapid growth of Category 5 UTP as a horizontal media: low initial cost and the ability to deliver high-data-rate LAN services. A standard media for LAN applications up to 155 Mbps is Category 5 UTP. However, copper-based LANs require more complex and expensive electronics as speeds increase. This trend, combined with continuing decreases in fiber media and optoelectronics prices, causes the initial price of the two solutions to converge as data rates increase. Today, for example, the price differential between copper and fiber (fiber being more expensive) for 155 Mbps ATM electronics is as small as 12 percent—with the 12 percent differential gap closing rapidly.

A third reason for the popularity of Category 5 UTP is that it allows customers to use only one media for both voice and data. In some instances, though, customers select lower performance Category 3 UTP to support voice services, leaving the choice between Category 5 UTP and fiber for data services.

Fiber Advantages: Ethernet Networks

Fiber provides several advantages to Ethernet and Fast Ethernet networks. The most common advantage and therefore use of fiber is to overcome the distance limitations of coaxial and twisted-pair copper topologies. Ethernet being run on coax (10Base2) has a maximum distance limitation of 185 m, and Ethernet being run on twisted-pair (10BaseT and 100BaseTX) has a limitation of 100 m. Fiber can greatly extend these distances with multimode fiber providing 2000 m and single-mode fiber supporting 5 km in half-duplex environments, and much more (depending on transmitter strength and receiver sensitivity) in full-duplex installations. Ethernet running at 10 Mbps has a limitation of 4 repeaters, providing some leniency in the solutions available for distance. However, Fast Ethernet only allows for two repeaters and only 5 m of cable between them. As Fast Ethernet becomes more ubiquitous, the need for fiber optic cabling will grow as well. When distance is an issue, fiber provides what may be the only solution.

Even when using coaxial cable or twisted pair (shielded or unshielded), some electrical noise may be emitted by the cable. This is especially true as connectors and ground connections age or weaken. In some environments (medical, for example), the potential risk associated with this is just not acceptable, and costs of alternative cable routings too high. Because fiber optic cabling uses light pulses to send the signal, there is no radiated noise. This makes it perfectly safe to install this cabling in any sensitive environment. Optical fiber adds additional security protection as well. There are no emissions to pick up and decode, and it is not feasible to *tap* into it for the purposes of *eavesdropping*. This makes fiber optic cabling ideal for secure network installations.

Another problem that is common when using copper cabling is other electrical noise getting into the desired electrical networking signal. This can be a problem in noisy manufacturing environments or other heavy industrial applications. The use of optical fiber provides a signal that will be completely unaffected by this noise.

In some instances, fiber provides the advantage that it can withstand more tension during the cable pulling. It is also smaller in size then twisted-pair cables and therefore takes up less room. Compared to Category 5 UTP, most duplex fiber optical cable can also endure a tighter bend radius while maintaining specified performance.

Nevertheless, 62.5/125 micron multimode fiber is already popular as a backbone media and its popularity is growing as a horizontal media. Although fiber is presently deployed in less than 9 percent of horizontal

cabling systems, analysts project it will triple or quadruple in some vertical markets over the next four years. The main reasons for this growth are the need for high-bandwidth services and the desire to never need to install cabling again over the life of the building. In addition, fiber eliminates potential problems of radio frequency interference, cross talk, and lightning, thereby increasing the reliability of the network.

However, many customers may not realize one of fiber's greatest strengths. Fiber's longer distance capability permits cabling architectures that reduce recurring network operational costs. Fiber allows a centralized cabling design with a single point of administration. By collecting all hubs, switches, routers, and gateways into one location, the network requires less active equipment, maintenance, and administration effort. This generates substantial savings in initial and recurring operating costs. For example, the simplicity and flexibility of centralized electronics facilitates rapid rearrangements of distributed workgroup networks, and avoids expensive protocol conversions and switching that are often deployed between traditional horizontal and backbone cabling. In addition, centralization increases electronic equipment efficiencies, resulting in reduced equipment costs due to higher port usage. These savings multiply when supporting more than one LAN technology simultaneously, as is almost always the case when migrating to higher speed networks. All of these advantages can make fiber very cost-effective, even for lower-speed applications.

As mentioned earlier, it is critical to consider the customer's needs and business situation in order to make the best choice of horizontal media. Important issues include present and future data speed requirements, upgrade migration strategy, workgroup rearrangement frequency, building ownership and tenancy, remaining building occupancy, work area environment, horizontal distances, suitability of telecommunications closets, and long-term and short-term cost sensitivity. With these issues in mind, some conditions that indicate a centralized fiber architecture as the best choice for desktop connectivity include:

- A need to migrate efficiently to speeds above 155 Mbps at the desktop.
- A need to configure special workgroup networks quickly and easily.
- A need to support multiple LAN technologies efficiently.
- Long-term single-tenant occupancy.
- High security, high electromagnetic field, high lightning strike, or corrosive environments.
- Extreme intolerance to data errors or radiated emissions.

- Horizontal distances exceeding 100 meters (325 feet).
- Small, overcrowded, or insufficient numbers of telecommunications closets.
- A need to increase control over network operations.
- A need to reduce recurring operational costs.

If the customer's situation matches a number of these conditions, then fiber is probably the best choice. If the match is minimal, or if addressing the condition is not critical, then copper is probably the best choice. For some conditions, such as the need to exceed the standardized rates of UTP or support horizontal distances longer than 100 meters, fiber may be the only solution.

Challenges

However, fiber optical cabling is not a panacea; there are some challenges to be resolved. The first (and probably the best known), is the cost of termination. Because of the need for *perfect* connections, splices and connections must be carefully cut and then polished to preserve the optical characteristics. The connectors must also maintain a very high level of precision to guarantee alignment of the fibers.

The second problem that is encountered when installing fiber cabling is that legacy equipment does not support fiber connections. Very few desktop computers have a fiber network interface, and some critical network equipment does not offer a fiber interface.

In Ethernet, the size of the collision domain can affect the use of fiber. In a half-duplex (shared media) environment, no two devices can be separated by more then 512 bit times. While the propagation of a signal is faster through fiber than copper, it is only about 11% faster and not enough to make a significant difference. This limitation means that there are times when the signal quality and fiber are sufficient to carry the signal but the distance and network design preclude its use.

Solutions

Fortunately, the problems are not without solutions. As fiber deployment increases, the economy of scale for the manufacturers is driving costs down. Also, much work is being done to further reduce these costs. Plastic optical fiber is an example of one such development.

The need to connect to legacy equipment and infrastructure also has a solution. By using copper to fiber media converters, fiber can be connected to almost any legacy environment. Equipment equipped with an attachment unit interface (AUI) port can also make use of fiber transceivers as well. Media converters are small devices that take signals from one media type and retransmit it onto another media type. These converters are usually small enough to fit in the palm of your hand.

For those instances when collision domain restrictions preclude the use of fiber, a two port bridging device (such as a transition networks bridging media converter) with a 10/100-Base-T(X) on one port and fiber on the other can be used. Bridges by definition break collision domains, and when connected to a server, workstation, or another bridge can operate in full-duplex mode. In this mode, there are no limitations imposed by collision domains, and the distance attainable is solely a function of the fiber cable.

ATM/FDDI

As networks move to even faster protocol speeds, such as FDDI and ATM, fiber plays an increasingly important role. FDDI and ATM pose all the same problems and advantages as Ethernet. The copper version of FDDI (CFDDI) has a cable distance limitation of 100 m. Because these topologies are typically used in a campus backbone application, the distance limitations of multimode fiber can present a problem (2 km). By using single-mode fiber, distances of up to 60 km are possible. Since typically only one or two segments need that kind of distance, single-mode to multimode fiber mode converters can be used to convert just those segments to single-mode without incurring that cost for every segment in the network.

The WAN Backbones

Wide area networks (WAN) provide an inherent distance problem, and as a result, fiber has found widespread deployment. Carriers are migrating large portions of their networks to fiber to take advantage of its superior bandwidth and compact size. As more WAN services are provisioned to the customer premises via fiber, the need to convert from single mode (used almost exclusively in the WAN venue) to multimode will grow. Some of the services that are being provided directly on fiber are ATM and synchronous optical network (SONET).

WIRELESS MEDIA

Finally, let's take a look at the last cabling media type: wireless networks. Again, the intent of this final section is not to take away from the very detailed and indepth discussion of wireless media in Chapter 11, "Wireless Design Considerations." But, it is the intent of this section to discuss the basics of how, through wireless media technology, you can create an instant standalone network (that can even link the local area networks of several buildings) with a complete, integrated system of hardware and software. Not all networks are connected with cabling; some networks are wireless. Wireless LANs use high frequency radio signals or infrared light beams to communicate between the workstations and the file server. Each workstation and file server on a wireless network has some sort of transceiver/antenna to send and receive the data. Information is relayed between transceivers as if they were physically connected. For longer distances, wireless communications can also take place through cellular telephone technology or by satellite, as shown in Figure 1–10.

Wireless media is great for allowing laptop computers or remote computers to connect to the LAN. Wireless networks are also beneficial in older buildings, where it may be difficult or impossible to install cables.

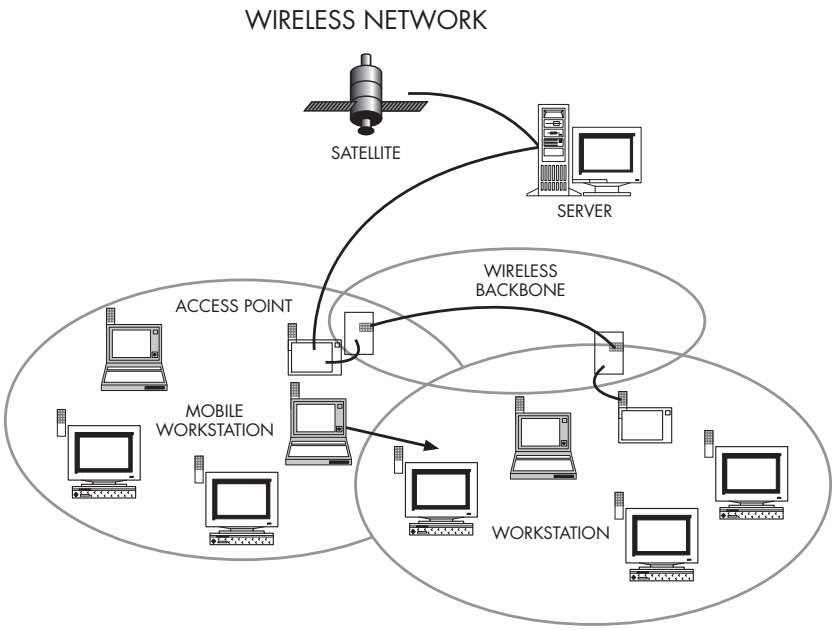

Figure 1–10 Wireless network.

So What Really is a Wireless LAN?

Today, many personal computers are interconnected with local area networks. Individuals are able to access and share data, applications, and services via the LAN. Most of these individuals use their computers in a fixed location where wired networking is possible, as shown in Figure 1–11 [9]. In a wireless LAN, the connection between the client and user is accomplished by the use of a wireless medium such as Radio Frequency (RF) or Infra Red (IR) communications instead of a cable. This allows the remote user to stay connected to the network while mobile or not physically attached to the network. The wireless connection is most usually accomplished by the user having a handheld terminal or laptop that has an RF interface card installed inside the terminal or through the PC card slot of the laptop. The client connection from the wired LAN to the user is made through an access point (AP) that can support multiple users simultaneously, as shown in Figure 1–10. The AP can reside at any node on the wired network and acts as a gateway for wireless users' data to be routed onto the wired network.

However, a growing number of applications require mobility and simultaneous access to a network. Until recently, if an application required information from a central database, it had to be connected to a wired network using a docking station. A wireless LAN enables mobile computers to be in constant contact with servers and each other. Healthcare, warehousing, and education are examples of some of the industries that utilize wireless LANs, as shown in Figure 1–10.

The computers in Figure 1–10 must all be in range of each other to maintain the wireless connection. However, most computers require greater range and flexibility since servers are often located on a wired Ethernet LAN somewhere else in the facility or at another site on an enterprise network. A wireless access point solves this problem by connecting wireless clients to Ethernet, as shown in Figure 1–12 [AMP, 1–2].

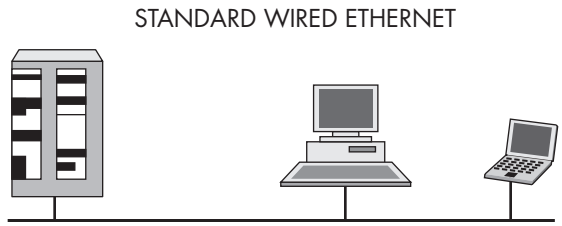

Figure 1–11 Clients communicate with server over standard wired Ethernet LANs.

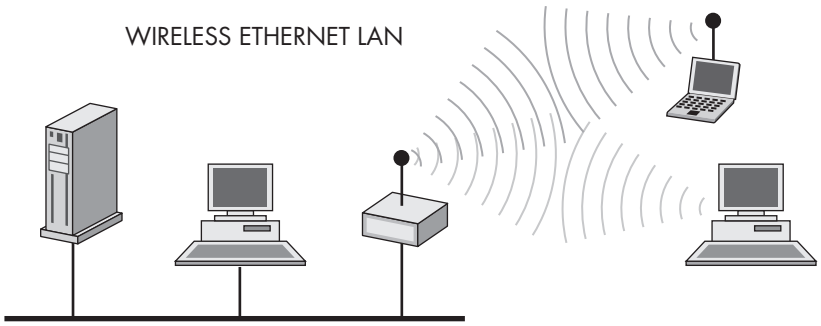

Figure 1–12 Access points connect wireless clients to Ethernet.

The range of these systems is very dependent on the actual usage and environment of the system, but varies from 100 feet inside a solid walled building to over 1,000 feet outdoors, in direct line of sight. This is a similar order of magnitude as the distance that can be covered by the wired LAN in a building. However, much like a cellular phone system, the wireless LAN is capable of roaming from the AP and reconnecting to the network through other APs residing at other points on the wired network. This can allow the wired LAN to be extended to cover a much larger area than the existing coverage by the use of multiple APs such as in a campus environment. In other words, an access point will usually provide 50,000 to 250,000 square feet of coverage depending on your building structure. Numerous access points will allow wireless clients to roam and function in all the necessary areas. Roaming occurs seamlessly and transparently to the wireless client. Figure 1–13 shows roaming conceptualized [AMP, 2]. Implementing mobile or wireless applications in an existing environment consists of two simple steps:

- Step 1: Replace the PCMCIA (PC card) wired network interface card (NIC) or the industry-standard architecture broadcast and unknown server (ISABUS) wired NIC with a wireless NIC.
- Step 2: Replace the Ethernet driver with a wireless Ethernet driver [AMP, 1]

Wireless drivers exist for all versions of Windows and DOS. ND&Is, ODI, and packet drivers are also offered. These drivers support a wide range of network operating systems, protocol stacks (Netware, Vines, TCP/IP, Lantastic, LAN server, etc.), and applications.

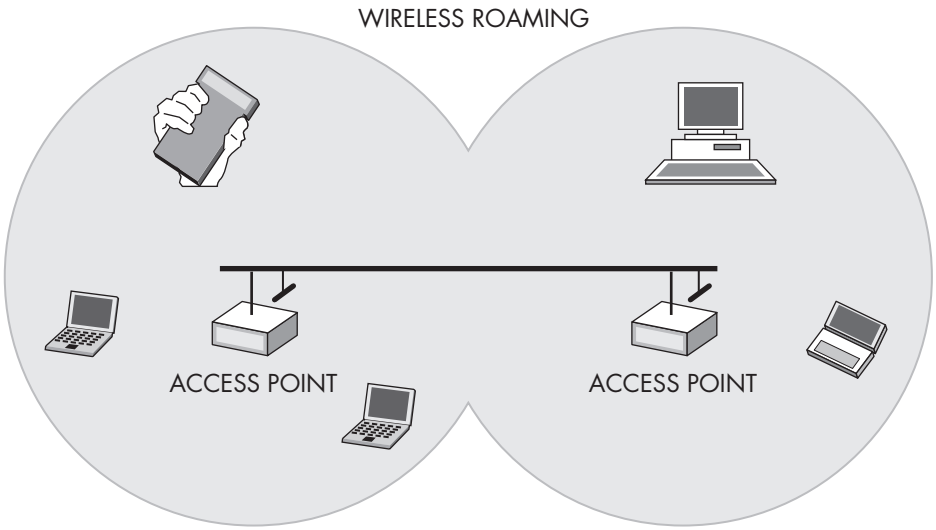

Figure 1–13 Wireless clients roam seamlessly throughout a facility.

Another important feature of the wireless LAN is that it can be used independently of a wired network. It may be used as a standalone network anywhere to link multiple computers together without having to build or extend a wired network. A useful example that is in use today is an outside auditing group inside a client company. If each of the auditors has a laptop equipped with a wireless client adapter, then a peer-to-peer workgroup can immediately be established for transfer or access of data. A member of the workgroup may be established as the server or the network can act in a peer-to-peer mode.

A wireless LAN is also capable of operating at speeds in the range of 1–2 Mbps, depending on the actual system. Both of these speeds are supported by the standard for wireless LAN networks defined by the international body, IEEE. At first approach, this suggests that the wireless network will have throughput that is 5 to 10 times less than the wired network. In practice, however, the real user of wireless networks will see a reduction in throughput compared to a wired network but not as great as the raw numbers suggest. The actual usage of the network is a much better indication of the throughput that can be expected. This is not dissimilar to the model of highway traffic when a surface street is compared to a highway to get from point A to point B. While travel is significantly faster on the highway at the optimum time or at offpeak hours when maximum speeds are possible, during

peak usage, the highway can often be slower than the surface streets due to the load of traffic that the highway has to deal with.

Wireless LANs are billed on the basis of installed equipment cost; once in place there are no charges for use of the network. The network communications take place in a part of the radio spectrum that is designated as *license free*. In this band, 2.4-2.5 GHz, users can operate without a license so long as they use equipment that has been type-approved for use in the license-free bands. In the United States, these licenses are granted by the FCC for operation under part 15 regulations. The 2.4 GHz band has been designated as license free by the International Telecommunications Union (ITU) and is available for use license free in most countries in the world. Unfortunately, the rules of operation are different in almost every country, but they are similar enough that the products can be programmed for use in every country without changing the hardware component.

The Wireless Technology

It is not the intent of this section to detail the technology that makes it possible for a wireless LAN to operate; however, as with many new technologies, it is better for the potential user to understand some of the technical details that will affect the way that the product operates. Without some background, it is very hard to differentiate between the attributes of competing systems. The necessary new specifications that are needed to understand the system are not as obvious as one might think. In a wired world, the connection is a given. It is assumed that if it is designated as there, then it will be. In a wireless network of any kind, it must be assumed that the connection will be a tradeoff between data rate and robustness of the network connection.

Specifications

On first approach, the only issues that a user of a new data communications network usually asks are: *What is the range? What is the data rate?* However, there are other considerations that are even more critical, which are based on the radio portion of the technology, not simply the data protocol, such as: *How robust and interference-resistant is this network?* This is especially important when a wireless network is used in a license-free part of the spectrum where the range of potential interference is very broad. In an unlicensed band, there are many and varied users of the band that can strongly interfere with the high speed data user unless the system has been designed to work in that environment.

The ability to build a dynamically scaleable network is critical to the viability of a wireless LAN as it will inevitably be used in this mode. The interference rejection of each node will be the limiting factor to the expandability of the network and its user density in a given environment.

Radio Frequency Systems

There are two main technologies that are used for wireless communications today: radio frequency (RF) and infra red (IR). In general, they are good for different applications and have been designed into products that optimize particular features of advantage.

RF is very capable of being used for applications where communications are not in the *line of sight* and over longer distances. The RF signals will travel through walls and communicate where there is no direct path between the terminals. In order to operate in the license free portion of the spectrum called the ISM band (industrial, scientific, and medical), the radio system must use a modulation technique called Spread Spectrum (SS). In this mode, a radio is required to distribute the signal across the entire spectrum and cannot remain stable on a single frequency, as shown in Figure 1–14 [10]. This is done so that no single user can dominate the band and that all users collectively look like noise.

Security. Spread spectrum communications were developed during World War II by the military for secure communications links. The fact that such signals appear to be noise in the band means that they are difficult to

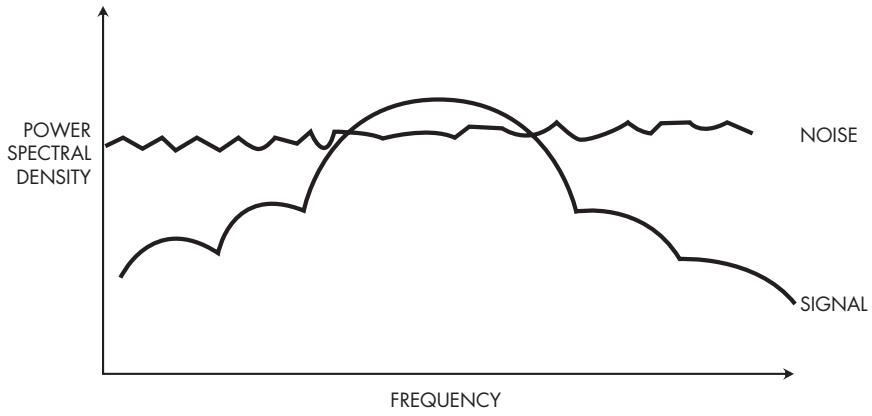

Figure 1–14 Spread spectrum signals.

find and to jam. This technique lends itself well to the expected conditions of operation of a wireless LAN application in this band and is by its very nature difficult to intercept, thus increasing security against unauthorized listeners.

Also, because wireless technology has roots in military applications, security has long been a design criterion for wireless devices. Security provisions are typically built into wireless LANs, making them more secure than most wired LANs. It is extremely difficult for unintended receivers (eavesdroppers) to listen in on wireless LAN traffic. Complex encryption techniques make it impossible for all but the most sophisticated to gain unauthorized access to network traffic. Individual nodes must be security-enabled before they are allowed to participate in network traffic.

Coverage and Range. The distance over which radio frequency (RF) waves can communicate is dependent on the building or environment in which the wireless LAN is installed. Interactions with typical building objects, including walls, metal, and even people, can affect how energy propagates and thus what range and coverage a particular system achieves. A wireless LAN system uses RF because radio waves can penetrate many indoor walls and surfaces. The range of a wireless LAN is up to 500 feet in normal office environments and up to 1,000 feet in open space. Coverage can be extended, and true freedom of mobility via roaming is provided through microcells.

In view of this, the use of spread spectrum is considered to be especially important, as it allows many more users to occupy the band at any given time and place than if they were all static on separate frequencies. As with any radio system, one of the greatest limitations is available bandwidth; and so, the ability to have many users operate simultaneously in a given environment is critical for the successful deployment of a wireless LAN.

There are several bands available for use by license-free transmitters. The most commonly used bands are at 902-928 MHz, 2.4–2.5 GHz, and 5.7–5.8 GHz. Of these, the most useful is probably the 2.4 GHz band, as it is available for use throughout most of the world. In recent years, nearly all of the commercial development and the basis for the new IEEE standard has been in the 2.4 GHz band. While the 900 MHz band is widely used for other systems, it is only available in the United States and has greatly limited available bandwidth. In the license-free bands, there is a strict limit on the broadcast power of any transmitter, so that the spectrum can be reused at a short distance away without interference from a distant transmitter. This is similar to the operation of a cellular telephone system.

Safety. The output power of wireless LAN systems is very low, much less than that of a handheld cellular phone. Since radio waves fade rapidly

over distance, very little exposure to RF energy is provided to those in the area of a wireless LAN system. Wireless LANs must meet stringent government and industry regulations for safety. No adverse health effects have ever been attributed to wireless LANs.

Infra Red Systems

The second technology that is used for wireless LAN systems is infra red—where the communication is carried by light in the invisible part of the spectrum. This system has much to recommend in some circumstances. It is primarily of use for very short distance communications—less than 3 feet where there is a line of sight connection. It is not possible for the infra red light to penetrate any solid material. It is even attenuated greatly by window glass, so it is really not a useful technology in comparison to radio frequency for use in a wireless LAN system.

The application where infra red comes into its element is as a docking function and in applications where the power available is extremely limited (such as a pager or personal digital assistant [PDA]). There is a standard for such products by the Infrared Data Association (IrDA) that has been championed by Hewlett Packard, IBM, and many others. This is now found in many notebook and laptop PCs, and allows a connectionless docking facility at up to 1 Mbps to a desktop machine at up to 2 feet line of sight.

The Infrared Data Association is a group of device manufacturers that developed a standard for transmitting data via infrared light waves. Increasingly, computers and other devices (such as printers) come with IrDA ports. This enables you to transfer data from one device to another without any cables. For example, if both your laptop computer and printer have IrDA ports, you can simply put your computer in front of the printer and output a document, without needing to connect the two with a cable. IrDA ports support roughly the same transmission rates as traditional parallel ports. The only restrictions on their use is that the two devices must be within a few feet of each other and there must be a clear line of sight between them.

Such products are point-to-point communications and not networks, which makes them very difficult to operate as a network, but does offer increased security, as only the user to whom the beam is directed can pick it up. Attempts to provide wider network capability by using a diffused IR system where the light is distributed in all directions have been developed and marketed, but they are limited to 30–50 feet and cannot go through any solid material. There are now very few companies pursuing this implementation.

The main advantage of the point-to-point IR system—increased security—is undermined by the distributing of the light source as it can now be received by any body within range, not just the intended recipient.

Implementation of Spread Spectrum

There are two methods of spread spectrum modulation that are used to comply with the regulations for use in the industrial, scientific, and medical (ISM) band: frequency hopping spread spectrum (FHSS) and direct sequence spread spectrum (DSSS). Let's take a close look at both.

Direct Sequence Spread Spectrum. Historically many of the original systems available used DSSS as the required spread spectrum modulation because components and systems were available from the direct broadcast satellite industry, in which DSSS is the modulation scheme used. However, the majority of commercial investment in wireless LAN systems is now in FHSS and the user base of FHSS products have now exceeded that of DSSS. Most new wireless LAN applications are now FHSS.

The term *direct sequence spread spectrum* is a complicated (and unrelated) way of describing a system that takes a signal at a given frequency and spreads it across a band of frequencies where the center frequency is the original signal, as shown in Figure 1–15 [10]. The spreading algorithm, which is the key to the relationship of the spread range of frequencies, changes with time in a pseudorandom sequence that appears to make the spread signal a

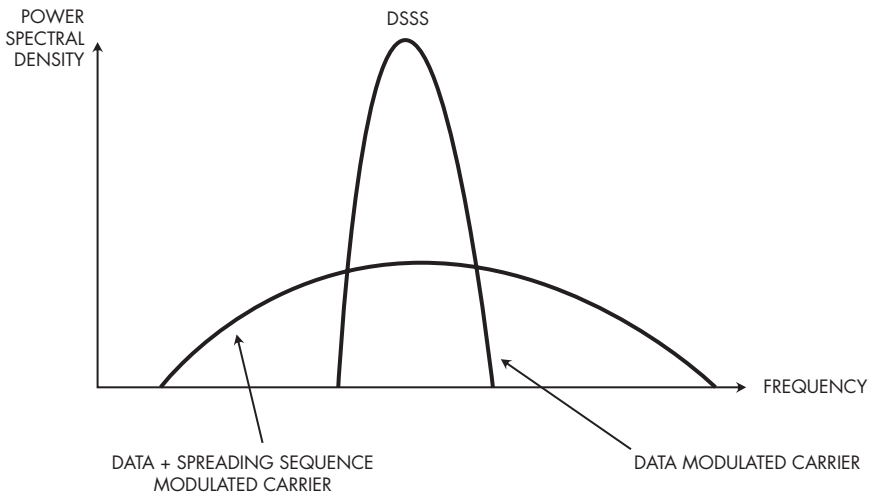

Figure 1–15 Direct sequence spread spectrum.

random noise source. The strength of this system is that when the ratio between the original signal bandwidth and the spread signal bandwidth is very large, the system offers great immunity to interference. For instance, if a 1 Kbps signal is spread across 1 GHz of spectrum, the spreading ratio is one million times, or 60 dB. This is the type of system developed for strategic military communications systems, as it is very difficult to find and even more difficult to jam.

However, in an environment such as wireless LAN in the license-free, ISM band (where the available bandwidth critically limits the ratio of spreading), the advantages that the DSSS method provides against interference become greatly limited. A realistic example in use today is a 2 Mbps data signal that is spread across 20 MHz of spectrum and offering a spreading ratio of 10 times. This is only just enough to meet the lower limit of *processing gain* (a measure of this spreading ratio, as set by the Federal Communications Corporation [FCC], the United States government body that determines the rule of operation of radio transmitters). This limitation significantly undermines the value of DSSS as a method to resist interference in real wireless LAN applications.

Frequency Hopping Spread Spectrum. In simple terms, an FHSS system is not dissimilar to the radio in a car, where the preset buttons are pushed one after another in an apparent random sequence. The time on each channel is very short, but at a data rate of 1 Mbps or higher. Even a fraction of a second provides significant overall throughput for the communications system. On the other hand, with wired LAN systems, actual throughput in wireless LANs is dependent on your set-up. Factors that affect throughput include airwave congestion (number of users), propagation factors such as range and multipath, as well as the latency and bottlenecks on the wired portions of the wireless LAN. Typical data rates range from 1 to 10 Mbps.

The term "multipath" describes a situation in which a transmitted signal follows several propagation paths from a transmitter to a receiver. This may result from the signal reflecting off several objects to arrive at the receiver.

Users of traditional Ethernet LANs generally experience little difference in performance when using a wireless LAN and can expect similar latency behavior. Wireless LANs provide throughput sufficient for the most common LAN-based office applications, including electronic mail exchange, access to shared peripherals, and access to multiuser databases and applications.

Nevertheless, FHSS is an altogether much simpler system to understand than DSSS. It is based on the use of a signal at a given frequency that is constant for a small amount of time and then moves to a new frequency. The sequence of different channels determined for the hopping pattern (where will the next frequency be to engage with this signal source), is pseudorandom. "Pseudo" means that a very long sequence code is used before it is repeated, over 65,000 hops, making it appear to be random. This makes it very difficult to predict the next frequency, at which such a system will stop and transmit or receive data as the system appears to be a random noise source to an unauthorized listener. This makes the FHSS system very secure against interference and interception, as shown in Figure 1–16 [10].

This system is a very robust method of communicating, as it is statistically close to impossible to block all of the frequencies that can be used and as there is no *spreading ratio* requirement that is so critical for DSSS systems. The resistance to interference is actually determined by the capability of the hardware filters that are used to reject signals other than the frequency of interest, and not by mathematical-spreading algorithms. In the case of a standard FHSS wireless LAN system (with a two-stage receive section), the filtering will be provided in excess of 100,000 times rejection of unwanted signals, or over 50 dB for the engineers, as shown in Figure 1–17 [10].

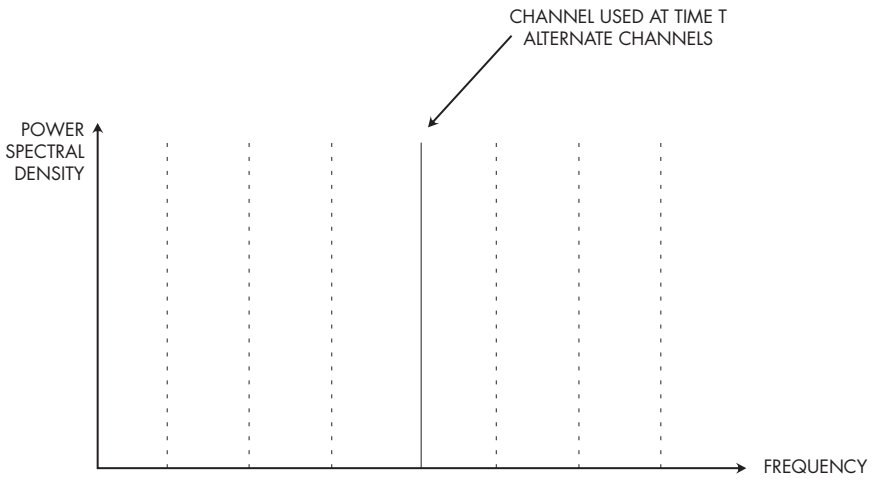

Figure 1–16 FHSS modulation.

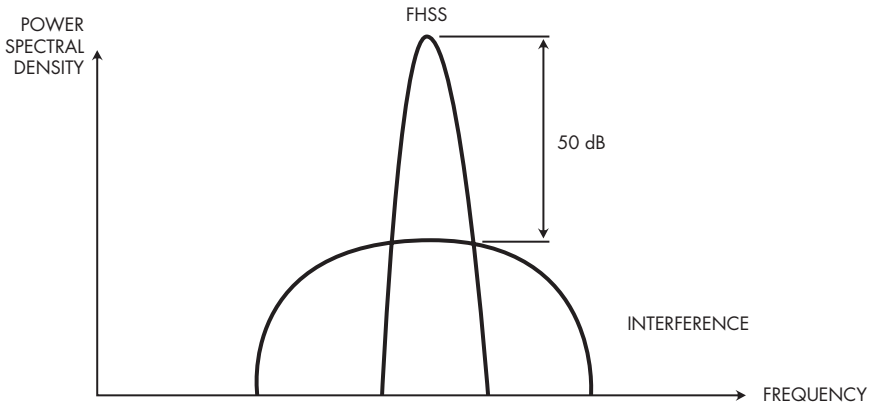

Figure 1–17 FHSS interference rejection.

Comparison DSSS And FHSS

DSSS technology is basically a mathematically derived solution. Therefore, it is useful to use math to analyze the comparative value of such a system. There are some very compelling arguments against DSSS in a constrained bandwidth system that are clearly demonstrated by such an analysis.

The ability to resist interference of a radio system is called the *jamming margin* and can be approximated to the ratio of the interfering signal to the intended signal that can be endured by the system while still functioning. In a standard fixed frequency radio system (the instantaneous equivalent of an FHSS system), this has been designed to be around 100,000 times, or 50 dB. In a DSSS system, it has been shown for the wireless LAN model that the spreading ratio is at best 10 times. This shows that a DSSS system has 10,000 times less interference rejection than is provided by an FHSS system as used in a practical wireless LAN implementation (see Figure 1–18) [10].

Working this backward, it is clear that for a DSSS product to offer the same interference rejection as an FHSS system (100,000 times and that in the license-free ISM bands the maximum practical spread bandwidth is 20 MHz for a DSSS system), the maximum data rate would have to be 20 MHz divided by 100,000. That means that the maximum data rate for a practical DSSS system with good interference rejection is 200 bps!

As a point of reference in other real systems, the global positioning system (GPS) is the largest commercially implemented application of DSSS sys-

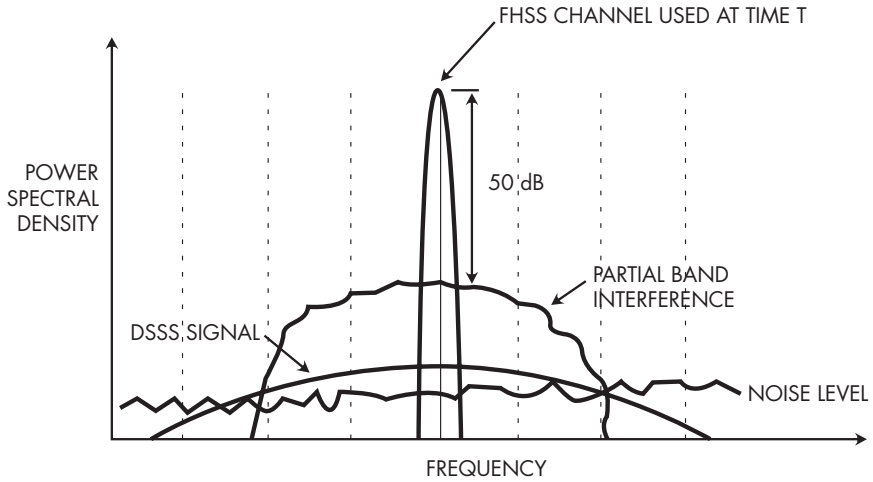

Figure 1–18 DS versus FH interference rejection.

tems. In that system, in order to reject interference, 50 bps are spread across 5 MHz of bandwidth. That is approximately the spreading ratio that was derived for a DSSS wireless LAN for use in the ISM bands—with data rate limited to 200 bps to provide interference rejection. This confirms the value of DSSS for a well-designed application; however, it is not exactly a compelling model for a multimegabit-per-second wireless LAN implementation in a constrained bandwidth spectrum with interference present!

Finally, with regard to the issue of interference rejection, this is actually the controlling specification that will determine if a system will work or not. For wireless LAN products to be successful for users, they need to be available in some quantity to reduce the costs and then become a ubiquitous network. FHSS is clearly the technology of choice to implement wireless LAN systems in unlicensed bands; and most of the commercial development supports this position.

Key Specifications

In looking at the value of the two competing technologies, there are a number of other key specifications that should be reviewed. However, it must be remembered that the DSSS implementation does not meet the minimum acceptable criteria for successful operation, unless very few people buy these systems. Therefore, exceeding a single FHSS specification is somewhat meaningless.

Variations in Data Rate

The most significant variation in data rate can usually be attributed to how well the underlying data transfer protocol is designed and implemented by the specific manufacturer and the quality of the overall systems architecture they have developed, not the spread spectrum implementation used.

Because of the spreading ratio, it is possible for existing DSSS implementations to marginally exceed the performance of FHSS systems (but, they will both nominally be rated at 1–2 Mbps over the air data rate). In effective throughput, the DSSS system has an advantage because the data packets are transmitted continuously—whereas in FHSS, a percentage of the operational time is spent hopping between frequencies and resynchronizing. This time is minimized by design and should not reduce throughput by more than 20 percent.

Some systems are now including data compression that provide 50–100 percent increases in effective data rate under some conditions. However, compression is algorithmic in nature and is very dependent on what sort of data is being transmitted. The algorithm for text compression is capable of around 2–3 times reduction, and is very different from the algorithm used for, say, video compression, where an optimized algorithm can provide 50–100 times reduction. Therefore, compression is most useful when it can be tailored to a known type of data source.

Range Capabilities

In the analysis of range, there is a marginal theoretical difference in the range capabilities of FHSS and DSSS systems. The largest range difference will be caused by two sources: the type and placement of the antenna system, not the spread spectrum modulation used, and the environment that the system is operating in.

Antenna diversity is one of the most significant influences on the range and performance of systems—especially near the edge of the range profile (the marginal area). Antenna diversity is the use of multiple antennas that are physically separated. This is done because the radio waves will reflect off all objects, walls, buildings, bridges, cars, and so on—and cause nulls and peaks randomly distributed in the air. This is much the same as the peaks and troughs that are seen on the surface of water when separate waves encounter each other. This is called *multipath* in the radio environment. With two antennas separated by a quarter of a wavelength (a few inches for 2.4 GHz systems), it is statistically very unlikely that both antennas will be in a null or wave trough at the same time—whereas a single antenna will likely be in a null in a highly reflective environment such as an office building.

Large antennas placed high above the ground will always provide better range than small antennas that extend marginally from a PC card and are low down on the side of a notebook computer. The range of the different system components is therefore different. Single-piece PC cards have the shortest range: 100–500 feet, depending on the environment. Access points with elevated, efficient antennas will achieve 500–3,000 feet. Luckily, in most systems, the client card will communicate with an access point. The overall link will benefit from the better antenna on the access point, though it will still have a shorter range than two access points communicating with each other.

The environment that the system is used in has a very significant influence on the range and performance. This should be of little surprise to anybody that has used a cordless phone—as they suffer from similar range and performance problems as wireless LANs (except that voice quality can be substituted for data rate). When the environment is outside (in line of sight, with little to reflect off and cause multipath), the range is at its best. When the environment is in a solid-walled building (such as an old stone house), the range is greatly reduced. This is the same for a wireless LAN; however, the multipath problem can significantly degrade megabit communications where it will not significantly affect voice quality.

Most office environments and modern homes are constructed of materials that are relatively *translucent* to radio waves at 2.4 GHz. So that the range will not be greatly limited, however, they do tend to present very reflective and refractive environments; and the ultimate limitation will probably be caused by severe multipath problems.

Power, Cost, and Size

Although these are three different and critical specifications, they are very closely linked in the wireless LAN environment. They also align with each other closely in a comparative review of DSSS and FHSS technology. The reason for this is because these specifications are all driven by implementation, which is limited by the required components to implement the spread spectrum and the level of integration of those components.

DSSS is driven by digital signal processing (DSP) multiplication. Therefore, it has a heavy requirement for large, expensive, and power-hungry digital circuitry in its implementation. The spreading can be achieved by multiplying the data signal by the spreading code, which is very DSP-intensive. This is in addition to the baseband processing requirements for the communications protocol being used. While further integration and increases in the capability of DSP processors will reduce the vulnerability of DSSS technology in these specifications, it will probably always lag the simplicity of FHSS systems.

In terms of the radio technology, all practical DSSS systems use phase modulation (PM) as the basic data modulation prior to spreading, whereas all practical FHSS systems use frequency modulation (FM) as the basic data modulation prior to spreading. This is important for several reasons.

FM is a method of modulation in which the frequency represents the value of a digital 1 or 0 as an offset above or below the nominal channel frequency. In this technique, the only information that needs to be recovered from the received signal is the frequency. This requires no linearity of the receive path. It is very cheap and low in power consumption to implement. PM is essentially a version of amplitude modulation (AM), in which the amplitude or size of a signal at a given frequency is measured. The size of this signal represents a digital 1 or 0. In this technique, it is not only necessary to know at which frequency the signal is, but it is also necessary to know the amplitude of the signal (two pieces of information instead of just one for FM). The limitation of such a system is that a change in range from the receiver has a similar effect on amplitude as a change in amplitude that represents a 1 or a 0. Therefore, the system needs to resolve whether an amplitude change is caused by a change in the range of the transmitted signal or a different bit. This requires a linear system, so that the measurement of amplitude has accurate and automatic gain control circuitry (AGC). The requirement to have a linear system costs money and more importantly uses power to implement.

FHSS implementation is effectively the same system that is found in a consumer radio with the addition of a system to hop the frequency through the band. This is a simple and very well understood technique that is simple and cheap to implement. There is no requirement for any DSP to implement FHSS, so the power requirements are significantly reduced from that needed for DSSS with no additional cost for components or extra size for the product.

The Wireless LAN Industry Standard Based System

Industry standards are absolutely critical in the computer business and its related industries. They are the vehicle that provides a large enough target market to be realistically defined and targeted with a single, compatible technological solution that many manufacturers can develop. This process reduces the cost of the products to implement the standard, which further expands the market. The result is not dissimilar to a nuclear chain reaction in terms of the user explosion (see Figure 1–19) [10].

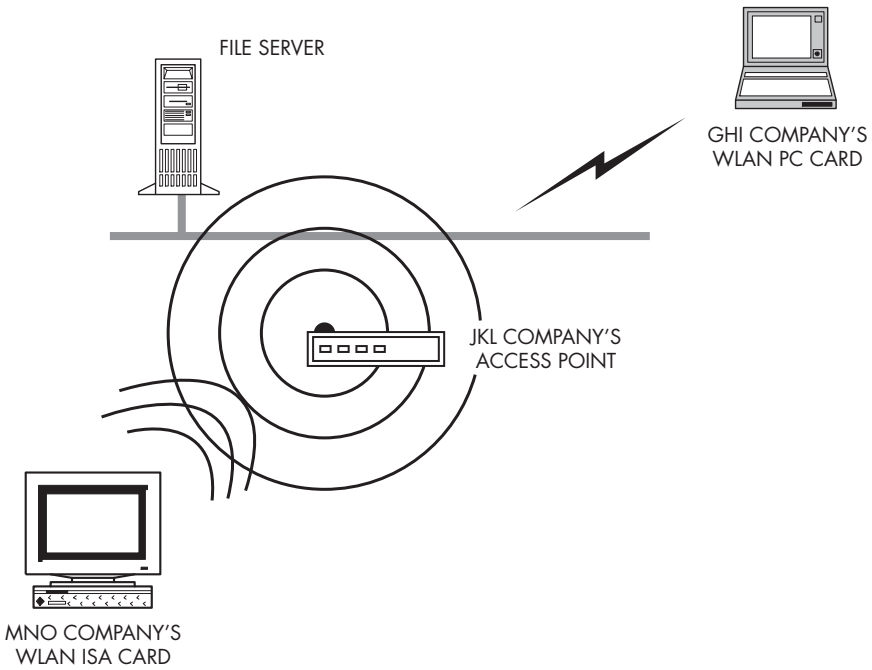

Figure 1–19 Standards-based system.

IEEE 802.11

In 1990, the IEEE 802 standards groups for networking setup a specific group to develop a wireless LAN standard similar to the Ethernet standard. On June 26, 1997, the IEEE 802.11 Wireless LAN Standard Committee approved the IEEE 802.11 specification. This is critical for the industry, as it now provides a solid specification for the vendors to target, both for systems products and components. While there are three sections of the specification representing FHSS, DSSS, and IR physical layers, almost all of the industry and associated commercial development money is now being expended in the FHSS marketplace.

The standard is a detailed software, hardware, and protocol specification with regard to the physical and data link layer of the open system interconnection (OSI) reference model that integrates with existing wired LAN standards for a seamless roaming environment. It is specific to the 2.4 GHz band and defines two levels of modulation that provide a basic 1 Mbps and enhanced 2 Mbps system.

Implications of Standards

The implications of an agreed standard are very significant, and is really the starting point for the wireless LAN industry in terms of a broader horizontal market. To this point, the market has been dominated by vertical implementations that are custom developments—using a specific manufacturer's proprietary protocol and system. The next generation of these products for both vertical and horizontal office systems will be based on the final recitified standard.

At two levels, this standard has already had a strong effect on the market. At the system level, almost everybody is claiming broad *compatibility* with what the standard will be. Most of these different proprietary systems will not communicate with each other. However, they do all have hardware that is capable of meeting the specification without significant change. At a lower level, component companies are starting to release products that are aimed at becoming standard components in winning wireless LAN designs. Especially important is the integrated circuit (IC) integration efforts that are under development, as this has the most significant chance of reducing greatly the cost of these solutions.

All of this effort is starting to reduce the cost of the systems and making the whole concept more appealing to the user community. Many of the market watchers and information companies that have been cold on this market are now starting to warm up and predict lower-cost products and large markets.

Products that are Noncompliant

There are some products available or promised to be available soon that do not intend to meet the IEEE specification. These are aimed at higher performance, more in line with the data rate of a wired Ethernet card (10 Mbps). These systems will probably operate under different regulations for the RF performance, which will limit the range to less than 100 feet due to power output. The method used to achieve the 10 Mbps data rate is somewhat dubious and remains to be proven as viable.

While these systems will be useful in certain circumstances, they will not benefit from the cost reductions that will be achieved through the IEEE standard. It is currently not clear how such systems could offer dual capability to operate as 802.11 wireless LANs. Also, the 10 Mbps systems (both digital and RF hardware) would be significantly different. It will be unlikely that an advanced system will survive on its own without being able to also work as an IEEE-compatible terminal.

Regulatory Compliance of Wireless LAN Systems

The wireless LAN systems discussed in this section and those specified by the IEEE 802.11 standard all operate in the unlicensed spectrum (as detailed earlier). The unlicensed spectrum rules allow a manufacturer to develop a piece of equipment that operates to meet predefined rules and for any user to operate the equipment without a requirement for a specific user license. This requires the manufacturer to make products that conform to the regulations for each country of operation. And, they should also conform with the IEEE 802.11 standard.

While the 2.4 GHz band is available in most countries, each countries' regulatory bodies usually have set requirements that are different in detail. There are three major specification groups that set the trend which most other countries follow. The U.S. FCC sets a standard covered by the Part 15 regulations that are copied in much of the rest of the Americas and the world. The Japanese Nippon Telegraph and Telephone Corporation (NTT) has its own standard. The European countries have set a specification through the European Telecommunications Standards Institute (ETSI) covered by RES 02.

While all of these differ in detail, it is possible to make a single hardware product that is capable of meeting all three specifications with only changes to the operating software. Although the software could be downloaded from a host such as a notebook PC, the changes are required to be set by the manufacturer, not the user, in order to meet the rules of operation.

Flexible and Growing

Finally, the increasing demand for network access while mobile will continue to drive the demand for wireless LAN systems. Because it's wireless, this type of media or network can go where no other network has gone before. It can plug right into your existing network.

But what can a wireless network do for you? You might be surprised. Imagine the gains in productivity you'll achieve when everyone on the factory floor has instant access to your parts database, on the spot, without traveling to a distant terminal for information. Think about how much you'll save in labor costs with a network that requires virtually none of the planning, installation, or reconfiguration traditional LANs require to keep pace with rapidly changing business conditions.

Now, imagine the improvements in both retail sales and customer service you'll achieve when point-of-sale terminals can be moved to areas of peak demand overnight, or even over a lunch break. Next, imagine six note-

book computers hastily opened on a conference table and sharing data minutes later. Imagine being able to do the same thing an hour after that—in a client's office, on a factory floor, or at a trade show.

Also, imagine linking the networks of two buildings a mile apart virtually overnight, without the expense of a leased telephone line. And, think about having an instant LAN set up and ready to cope—anywhere, anytime—when sudden business opportunities beckon or when a midnight phone call brings unthinkable news.

Now, take an empty room, add half a dozen workstations and link them all in a fast, partially secure local area network—within a few minutes. Impossible? Well, the security part may be.

Installing a wireless network actually can be just that simple. There's no wiring or conduit pathways to consider. All you need to create a fully functioning standalone network comes packed in a small box. Plug a card into each computer, install the software and your LAN is ready to go.

Could this unprecedented freedom help solve a few problems for you? Consider the possibilities. Cabling can be difficult or impossible to install in some situations. Asbestos makes older buildings problematic, hospitals can't accommodate new conduit pathways, warehouses can be simply too vast to rewire. But in each case a wireless network can be up and running virtually overnight.

Construction costs of recabling can overwhelm companies that change the workplace frequently. Retailers alter floor plans, manufacturers retool, banks redeploy branches. A wireless network effortlessly glides into place anywhere—and immediately becomes a versatile asset rather than a burdensome construction expense.

Finally, with the arrival of an industry standard, the concentration of manufacturers upon frequency hopping spread spectrum solutions will lower the cost and drive the market growth. The frequency hopping technology has the ability to support significant user density successfully, so there is no limitation to the penetration of such products in the user community. Wireless LAN solutions will be especially viable in new markets such as the small office/home office (SOHO) market, where there is rarely a wired LAN, due to the complexity and cost of wiring. Wireless LAN offers a solution that will connect a generation to *wired* access, but without the wires.

FROM HERE

Today's businesses require constant communication and instant access to information—both in and away from the office. The three cabling media (copper, fiber, and wireless) discussed in this chapter provide you with the mobility and flexibility you need—but you also have to manage the network that provides your communication requirements.

With that in mind, fiber optic cabling is rapidly becoming the most viable choice for data networking infrastructure. With the cost of cable, connectors, installation, and equipment becoming competitive with traditional copper solutions, fiber should be given serious consideration.

Finally, wireless LANs have some disadvantages. They are presently very expensive, provide poor security, and are susceptible to electrical interference from lights and radios. They are also slower than LANs using cabling. But they do have many advantages over traditional LANs. It's the way we're going to be doing business in this century.

The next chapter discusses the seven major types of networks: local area network (LAN), wide area network (WAN), virtual area network (VAN), virtual private network (VPN), intranet, extranet, and Internet. Some companies are fortunate to have all seven types connecting their systems. This chapter will cover how all three cabling media can be used with one or all seven of the network types to allow your organization to soar beyond the traditional constraints of network cabling. The next chapter will show you how and when to expand, contract, or redeploy your network type(s) virtually anywhere, anytime, as quickly as today's accelerating pace of change demands.

NOTES

[1] CompTIA Headquarters, 450 East 22nd St., Suite 230, Lombard, IL 60148-6158, 2000.

[2] "Local Area Network Cables," Remee Products Corp., P. O. Box 488, 186 North Main Street, Florida, NY 10921, USA, 2000, p. 1.

[3] "Connecting Terminals and PCs with DB25 Connectors," Computone Corporation, 1100 Northmeadow Parkway, Suite 150 Roswell, GA 30076, 1997, p. 1.

[4] "CATV, CCTV & Communication Coaxial Cable," Remee Products Corp., P. O. Box 488, 186 North Main Street, Florida, NY 10921, USA2000, p. 2.

[5] "Ethernet Cable Comparison Chart," Cabletron Systems, 35 Industrial Way, Rochester, NH 03866 U.S.A., 2000, p. 1.

[6] Scientific Instrument Services, 1027 Old York Rd., Ringoes, NJ 08551, 1999, p. 1.

[7] "Fiber Optic Cabling Installations," Advanced Cable Connection Inc., 922A E. 124 Avenue, Tampa, FL 33612, 2000, p. 1.

[8] Molex Incorporated, 2222 Wellington Court, Lisle, Illinois 60532 U.S.A., 2000, p. 1.

[9] "What is a Wireless LAN?," Reprinted with the permission of AMP Incorporated, Investor Relations, 176-42, PO Box 3608, Harrisburg, PA USA 17105-3608, 1999, p. 1.

[10] "Wireless LAN Systems—Technology and Specifications," SOHOware, Inc., NDC Communications, Inc., 265 Santa Ana Court, Sunnyvale, CA 94086, USA, 2000