PART II

The Basic LAN

CHAPTER 4

Hardware Concepts

The Network+ exam expects you to know how to

- Recognize the following logical or physical network topologies given a diagram, schematic, or description: star, bus, mesh, ring
- Recognize the following media types and describe their uses: Category 3, 5, 5e, and 6; UTP (Unshielded Twisted Pair); STP (Shielded Twisted Pair); coaxial cable; SMF (Single Mode Fiber) optic cable; MMF (Multimode Fiber) optic cable

To achieve these goals, you must be able to

- Explain the different types of network topology
- Describe the different types of network cabling
- Describe and distinguish among the 802.2, 802.3, and 802.5 IEEE networking standards

Every network must provide some method to get data from one system to another. In most cases, this method consists of some type of cabling (usually copper or fiber-optic) running between systems, although many networks skip wires and use wireless methods to move data. Stringing those cables brings up a number of critical issues you need to understand to work on a network. How do all these cables connect the computers together? Does every computer on the network run a cable to a central point? Does a single cable snake through the ceiling, with all the computers on the network connected to it? These questions need answering! Furthermore, we need some standards so that manufacturers can make networking equipment that works well together. While we're talking about standards, what about the cabling itself? What type of cable? What quality of copper? How thick should it be? Who will define standards for cables so that they'll all work in the network?

This chapter answers these questions in three parts. First, you will learn about the critical, magical concept called *network topology*—the way that cables and other pieces of hardware connect to one another. Second, you will tour the most common standardized cable types used in networking. Third, you will discover the all-important IEEE committees that combine these issues into solid standards.

Historical/Conceptual

Topology

If a bunch of computers connect together to make a network, there must be some logic or order to the way that they connect. Perhaps each computer connects to a single main line that snakes around the office. Each computer might have its own cable, with all the cables coming together to a central point. Or maybe all the cables from all the computers connect to a main loop that moves data along like a merry-go-round, picking up and dropping off data like a circular subway line.

A network's *topology* describes the way that computers connect to each other in that network. The most common network topologies are called *bus*, *ring*, *star,* and *mesh*. Figure 4-1 shows all four types: a *bus topology*, where all computers connect to the network via a main line called a bus cable; a *ring topology*, where all computers on the network attach to a central ring of cable; a *star topology*, where the computers on the network connect to a central wiring point (usually called a hub); and a *mesh topology*, where each computer has a dedicated line to every other computer. Make sure you know these four topologies!

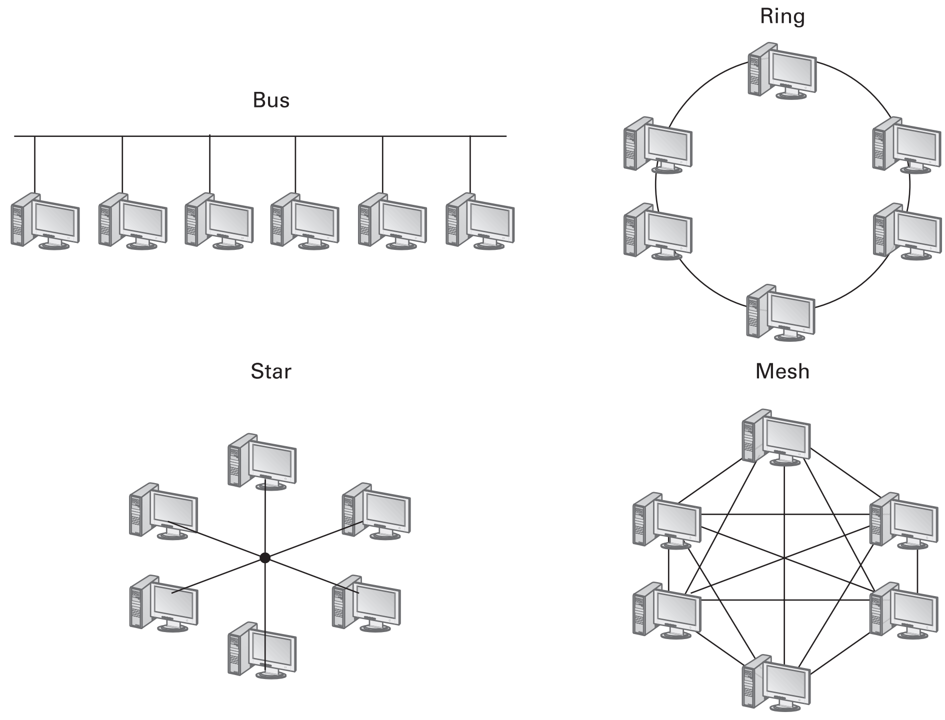


Figure 4-1 Clockwise from top left: bus, ring, mesh, and star topologies

If you're looking at the figure and thinking that a mesh topology looks amazingly resilient and robust, it is—at least on paper. Because every computer physically connects to every other computer on the network, even if half the PCs crash, the network still functions as well as ever (for the survivors). In a practical sense, however, implementing a true mesh topology network would be an expensive mess. For example, even for a tiny network with only 10 PCs, you would need *45* separate and distinct pieces of cable to connect every PC to every other PC. What a mesh mess! Because of this, mesh topologies have never been practical in a cabled network.

But what if you didn't have to use physical wires to connect the PCs? You wouldn't have the expense of buying the wires, or the mess of having a zillion cables lying around. In fact, most *wireless* networks can use a mesh topology if configured to do so! You'll learn more about wireless networks in Chapter 9, "Wireless Networking."

While a topology describes the method by which systems in a network connect, the topology alone doesn't describe all of the features necessary to make a cabling system work. The term *bus topology*, for example, describes a network that consists of some number of machines connected to the network via the same piece of cable. Notice that this definition leaves a lot of questions unanswered. What is the cable made of? How long can it be? How do the machines decide which machine should send data at a specific moment? A network based on a bus topology can answer these questions in a number of different ways.

Most techs make a clear distinction between the *logical topology* of a network—how the network is laid out on paper, with nice straight lines and boxes—and the physical topology. The *physical topology* describes the typically messy computer network, with cables running diagonally through the ceiling space or snaking their way through walls. If someone describes the topology of a particular network, make sure you understand whether they're talking about the logical or physical topology.

Over the years, particular manufacturers and standards bodies created several specific network technologies based on different topologies. A *network technology* is a practical application of a topology and other critical technologies to provide a method to get data from one computer to another on a network. These network technologies have names like Ethernet, Token Ring, and FDDI. The next three chapters describe all these network technologies in great detail, but for now, concentrate on learning the different topologies.

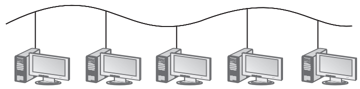
TIP Make sure you know your topologies: bus, ring, star, and mesh!

Test Specific

Hybrid Topologies

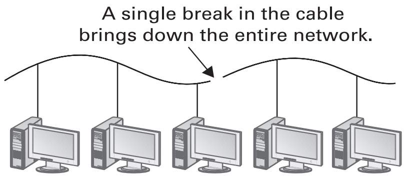
Of the four types of topologies just described, the bus topology was by far the most commercially successful. But bus topologies have a problem: the bus itself. *Ethernet*, the first network technology that used the bus topology, literally had a single cable—the bus—running around the networked area, usually up in the ceiling (see Figure 4-2). Each computer on the network connected to the bus.

Figure 4-2
Ethernet bus-topology network



If someone or something broke the bus cable (see Figure 4-3), the entire network would no longer function. The amount of network traffic would explode and packets would trample all over each other. (I'll explain why in detail in Chapter 5, "Ethernet Basics.") A true bus network has no *fault tolerance*, which means it cannot survive a problem on *any* node or cable.

Figure 4-3
A single break wreaking havoc on an Ethernet network



In the real world, bus breaks happened enough to motivate the Ethernet folks to develop an improved, fault-tolerant Ethernet network technology that shrunk the entire bus into a box called a *hub* (see Figure 4-4). Each computer connected to the hub with its own cable. If one of those cables broke, only the one computer connected to that hub was affected (see Figure 4-5); the rest of the network continued to run normally.

Figure 4-4
Improved Ethernet put the entire bus into the hub.

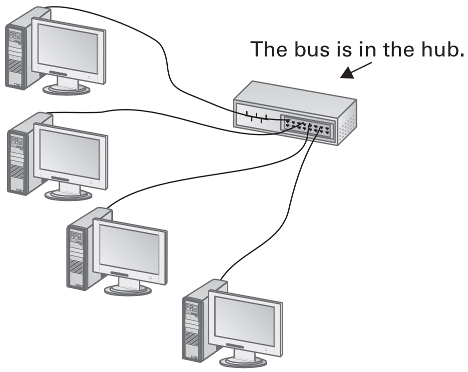
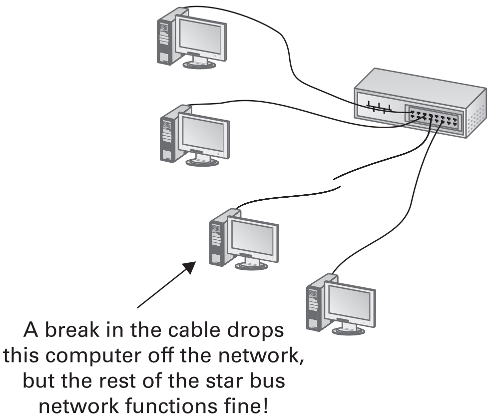


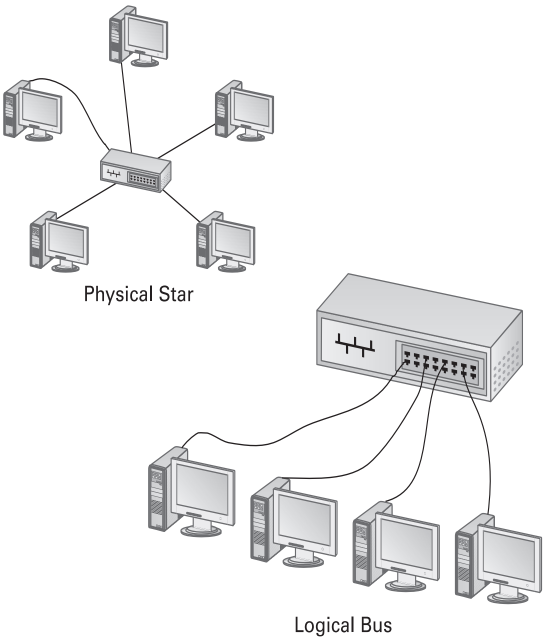
Figure 4-5
With a hub, a cable break affects only one system.



NOTE Fault tolerance refers to a system's capability to continue functioning even when some part of the system has failed. When bad things happen, a robust or fault-tolerant system continues to operate, at least to some degree.

This new type of Ethernet (see Figure 4-6) completely messed up the idea of topology. Physically, this new Ethernet had a central hub with wires coming out of it, so it looked like a star topology. But the hub was nothing more than a drastically shortened bus, so from an electronic (we like to use the term *logical*) standpoint, the network used a bus topology.

Figure 4-6
Star or bus?



NOTE A good way to separate logical topology from physical topology is to think about an electronic schematic diagram. The schematic shows how everything connects, but does not represent the way that the piece of electronics physically appears.

The answer to this topology dichotomy was simple—this type of topology was christened the *star bus*. A star bus topology is a *hybrid*, or blend, of the star and bus topologies. Star bus networks use a physical star design, which provides improved reliability, and a logical bus to maintain compatibility with existing bus-topology Ethernet standards. Star bus is overwhelmingly the most common topology used today.

Star bus is not the only hybrid topology. Many years ago, IBM invented a networking technology called *Token Ring* that employs a hybrid topology called *star ring*. A star ring topology works basically the same way as star bus. As with star bus, a central hub connects to the computers via cabling. The only difference is that instead of a logical bus, it uses a logical ring. Token Ring once held a large part of the installed base of networks, but this has slipped considerably over the years as many networks have switched to Ethernet. Token Ring still has a fairly large installed base, however, and the Network+ exam expects you to know its topology. Be warned: in many cases the Token Ring topology is simply referred to as a "star," even though in reality it is a star ring (see Figure 4-7)—be prepared to see it written either way!

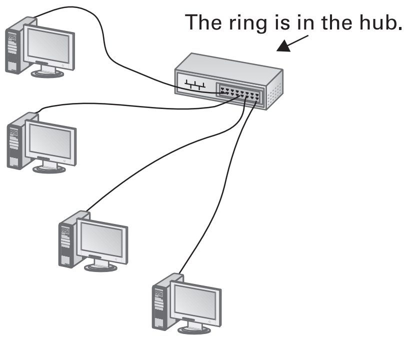


Figure 4-7 Token Ring topology is a star ring.

Every network uses some type of topology. A *topology* simply describes the method by which systems in a network connect. Make sure you know the four basic types of topology: star, ring, bus, and mesh. Also understand that many networks today use one of two hybrid types of topologies: star bus or star ring. Most networks use the star bus topology, but a substantial minority use star ring.

Cabling

The vast majority of networked systems are linked together using some type of cabling. Different types of networks over the years have used a number of different types of cables—and you get the job of learning about all these cables to pass the Network+ exam!

In this section, we'll explore both the cabling types used in older networks and those found in today's networks.

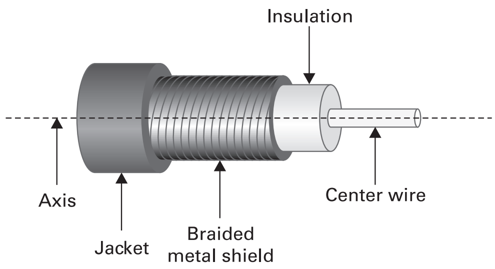
Some cabling types are used by a variety of networks, while other network types use their own unique cabling. Some of the cables I'll discuss have uses outside the networking industry; you'll probably recognize a number of them from their use in cable TV, recording equipment, and telephone systems. Don't assume that a particular cable type listed here is used only in networks!

All cables used in the networking industry separate into three distinct groups: coaxial (coax), twisted pair, and fiber-optic. Let's look at all three.

Coax

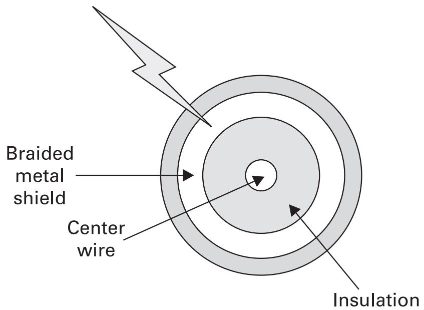
Coaxial cable contains a central conductor wire surrounded by an insulating material, which in turn is surrounded by a braided metal shield. The cable is referred to as coaxial (coax for short) because the center wire and the braided metal shield share a common axis or centerline (see Figure 4-8).

Figure 4-8
Cut-away view of a coaxial cable



Coaxial cable is designed to shield data transmissions from *electro-magnetic interference (EMI)*. Many devices in the typical office environment generate magnetic fields, including lights, fans, copy machines, and refrigerators. When a metal wire encounters these magnetic fields, electrical current is generated along the wire. This extra current can shut down a network because it is easily misinterpreted as a signal by devices like NICs. To prevent EMI from affecting the network, the outer mesh layer of a coaxial cable shields the center wire (on which the data is transmitted) from interference (see Figure 4-9).

Figure 4-9
The braided metal shield prevents interference from reaching the wire.



Only three types of coax cable have ever been used in networking: RG-8, RG-62, and RG-58. All coax cables have an *RG rating*; these ratings were developed by the military to provide a quick reference for the different types of coax. The only important measure of coax cabling is its *Ohm rating*, a relative measure of the resistance (or more precisely, characteristic impedance) on the cable. You may run across other coax cables, which may not have acceptable Ohm ratings although they look just like network-rated coax. Fortunately, most coax cable types display their Ohm ratings on the cables themselves (see Figure 4-10).

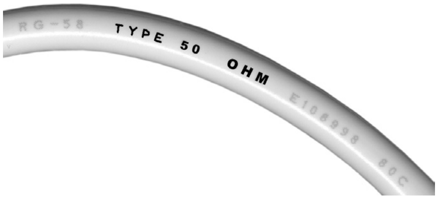


Figure 4-10 Ohm rating on a coax cable

TIP Know the Ohm ratings for these cable types!

The Ohm rating of a particular piece of cable describes the impedance of that cable. *Impedance* describes a set of characteristics that define how much a cable resists the flow of electricity. This isn't simple resistance, though. Impedance also factors in things like how long it takes the wire to get a full charge—the wire's capacitance—and other things.

You'd think at first blush that the higher the Ohms rating, the worse the cable would be, but in practice, that's almost irrelevant. The most important aspect of Ohms ratings for network technicians is to use cables with the same rating within a network; otherwise, you'll run into data corruption and data loss. Because almost any kind of coax can use the same connector, take a moment to glance at the Ohms rating before plugging in that handy piece of cable you found lying around!

RG-8

RG-8, often referred to as *Thick Ethernet*, is the oldest coax cabling type still in use. It has the name Thick Ethernet because it is used exclusively with a network technology called—you guessed it—Thick Ethernet! You'll see more on Thick Ethernet (also called Thicknet) and how it uses RG-8 cabling in the next chapter; for now, just make sure you can recognize an RG-8 cable (see Figure 4-11).

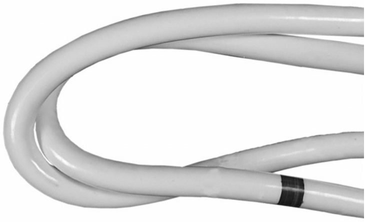


Figure 4-11 Thick coaxial cable (RG-8), marked with a black band every 2.5 meters

RG-8 is rated at 50 Ohms and has a distinct yellow or orange/brown color. The standardized color makes Thick Ethernet cabling unique, as almost all other types of cabling have no fixed color. Some cable types come in a veritable rainbow of colors!

RG-62

RG-62 cable, rated at 75 Ohms, is virtually never installed in networks these days, but you should know about it nonetheless (see Figure 4-12). If you think RG-62 resembles what your cable TV guy hitched up to your television, you aren't imagining things—cable TV uses the similar RG-6 coax. RG-62 cabling saw widespread use in a network technology called ArcNet, which is quite rare in today's networking world.

Figure 4-12
RG-62 coax cable

RG-58

Today, RG-58 stands alone as the only coax cable type still widely used in networks. It's often called *Thin Ethernet* or *Thinnet*, which is the name of the network technology that uses it. Thinnet technology is dated, but still used—in fact, I'll discuss it in detail in the next chapter—so you need to be able to recognize the cabling it uses. At first glance, RG-58 may look like RG-62 (see Figure 4-13), but its 50-Ohm rating makes it different on the inside.

Figure 4-13
RG-58 coax cable

Twisted Pair

The most overwhelmingly common type of cabling used in networks consists of twisted pairs of cables. Networks use two types of twisted-pair cabling: shielded twisted pair (STP) and unshielded twisted pair (UTP). Twisted-pair cabling for networks is composed of multiple pairs of wires, twisted around each other at specific intervals. The twists serve to reduce interference, called *crosstalk*: the more twists, the less crosstalk.

NOTE Have you ever picked up a telephone and heard a distinct crackling noise? That's an example of crosstalk.

Shielded Twisted Pair

Shielded twisted pair (STP) cabling, as its name implies, consists of twisted pairs of wires surrounded by shielding to protect them from EMI. STP cabling is mostly confined to older Token Ring networks (see Chapter 7, "Non-Ethernet Networks") and a few rare high-speed networking technologies. STP is pretty rare, primarily because there's so little need for STP's shielding; it only really matters in locations with excessive electronic noise, such as a shop floor with lots of lights, electric motors, or other machinery that could cause problems for UTP. UTP is cheaper, and in most cases, does just as good a job as STP. Figure 4-14 shows the most common STP type: the venerable IBM Type 1 cable used in Token Ring network technology.

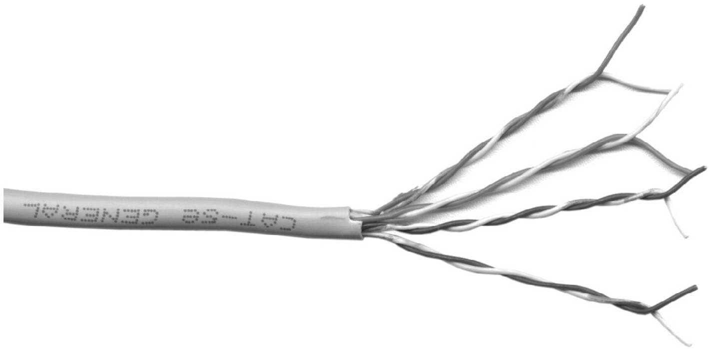
Figure 4-14
IBM Type 1 shielded twisted-pair cable

Unshielded Twisted Pair

Unshielded twisted pair (UTP) is by far the most common type of network cabling used today. UTP consists of twisted pairs of wires surrounded by a plastic jacket (see Figure 4-15). This jacket does not provide any protection from EMI, so some consideration must be used when installing UTP cabling to avoid interference from light, motors, and so forth.

Although more sensitive to interference than coaxial or STP cable, UTP cabling provides an inexpensive and flexible means to cable networks. UTP cable isn't exclusive to networks; many other technologies (such as telephone systems) employ the same cabling. This makes working with UTP a bit of a challenge. Imagine going up into a ceiling

Figure 4-15
UTP cabling



and seeing two sets of UTP cables: how would you determine which is for the telephones and which is for the network? Not to worry—a number of installation standards and tools exist to help those who work with UTP get the answer to these types of questions.

Not all UTP cables are the same! UTP cabling has a number of variations, such as the number of twists per foot, which determine how quickly data can propagate on the cable. To help network installers get the right cable for the right network technology, the cabling industry has developed a variety of grades called *categories* or *CAT ratings*. CAT ratings are officially rated in *megahertz (MHz)*, indicating the highest frequency bandwidth the cable can handle. Table 4-1 shows the most common categories.

UTP cables are rated to handle a certain bandwidth, such as 10 MHz or 100 MHz, which originally translated as the maximum throughput for a cable. On a one-for-one basis, for example, a 10 million cycle per second (10 MHz) cable could accommodate 10 million bits per second (10 Mbps)—1 bit per cycle. Through the use of *bandwidth-efficient encoding schemes*, such as MLT-3, manufacturers can squeeze more bits into the same signal, as long as the cable can handle it. Thus the CAT 5e cable can handle throughput of up to 1000 Mbps, even though it's rated to handle a bandwidth of only up to 100 MHz.

CAT Rating	Bandwidth	Typical Throughput in Networks
CAT 1	< 1 MHz	Analog phone lines—not for data communication
CAT 2	4 MHz	Supports speeds up to 4 Mbps
CAT 3	16 MHz	Supports speeds up to 16 Mbps[1]
CAT 4	20 MHz	Supports speeds up to 20 Mbps
CAT 5	100 MHz	Supports speeds up to 100 Mbps
CAT 5e (Improved CAT 5)	100 MHz	Supports speeds up to 1000 Mbps
CAT 6	200–250 MHz	Supports speeds up to 10,000 Mbps

[1] Note that the throughput for CAT 3 cable listed here applies only to network technologies that use two pairs of wires in the cable, not four pairs.

Table 4-1 UTP Categories

CAT ratings define the speed on a per-pair basis. CAT levels do not say how many pairs of wires are in the cable! UTP cable is made in many variations, with varying numbers of wire pairs. For example, you can purchase CAT 5 cable with two pairs, four pairs, or even more. It's impossible to say how much data a particular cable can carry unless you know the number of pairs. The speed examples listed here assume network technologies that use either two or four pairs of wires in a cable. As we go into different network technologies in later chapters, you'll see how the number of pairs becomes important. For now, simply appreciate that CAT ratings exist and that they have different speeds.

TIP Many people use the term *CAT level* instead of *CAT rating*. Be comfortable interchanging these terms!

As most networks are designed to run at speeds of up to 100 MHz, most new cabling installations use Category 5e (CAT 5e) cabling. CAT 5e cabling currently costs much less than CAT 6, although as CAT 6 gains in popularity, it will undoubtedly drop in price. Make sure you can look at UTP and know its CAT rating. There are two places to look. First, UTP is typically sold in boxed reels, and the manufacturer will clearly mark the CAT level on the box (see Figure 4-16). Second, look on the cable itself. The category level of a piece of cable is usually printed on the cable (see Figure 4-17).

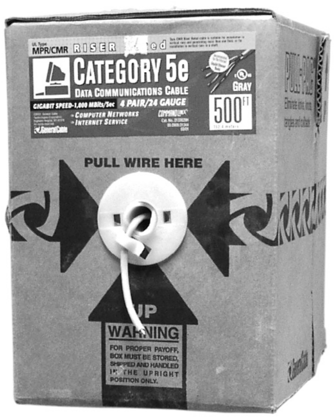


Figure 4-16 Box of UTP showing CAT rating

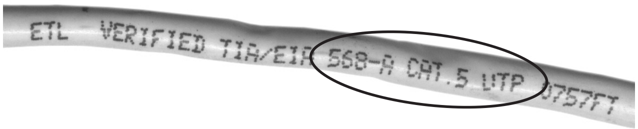


Figure 4-17 Markings on a UTP cable show its category level.

Fiber-Optic

Fiber-optic cabling transmits light rather than electricity, making it attractive for both high-EMI areas and long-distance transmissions. While most copper cables cannot carry data more than a few hundred meters at best, fiber-optic cabling will operate, depending on the implementation, for distances of up to 10 kilometers. A fiber-optic cable has three components: the fiber itself; the *cladding*, which is the part that makes the light reflect down the fiber; and the *insulating jacket*. Fiber-optic cabling is manufactured with many different diameters of fiber and cladding. In a convenient bit of standardization, cable manufacturers use a two-number designator to define fiber-optic cables according to their fiber and cladding measurements. The most common fiber-optic cable size is 62.5/125 μm. Almost all network technologies that use fiber-optic cable require pairs of fibers. In response to the demand for two-pair cabling, manufacturers often connect two fibers together like a lamp cord to create the popular duplex fiber-optic cabling (Figure 4-18).

Figure 4-18
Duplex fiber-optic cable

NOTE For those of you unfamiliar with it, the odd little u-shaped symbol describing fiber cable size (μ) stands for micro, or $1/1000^{th}$. Fiber cables are pretty tiny!

Light can be sent down a fiber-optic cable as regular light or as laser light. The two types of light require totally different fiber-optic cables. Most network technologies that use fiber optics use LEDs (light emitting diodes) to send light signals. Fiber-optic cables that use LEDs are known as *multimode.* Fiber-optic cables that use lasers are known as *single-mode.* Using laser light and single-mode fiber-optic cables enables a network to achieve phenomenally high transfer rates over incredibly long distances. It's difficult to differentiate between single-mode and multimode cable. Well, there's one easy way—single-mode cable is currently quite rare; if you see fiber-optic cabling, you can be relatively sure it's multimode.

Installing fiber-optic cabling is basically a love/hate arrangement. On the love side, fiber-optic cables don't carry electricity, so you can ignore the electrical interference issue. Also, fiber-optic cabling can reach up to 10,000 meters. This depends on the networking technology used, of course, and the most common network technology that uses fiber-optic cabling has a much lower limit of *only* 1000 meters! On the hate side of the fiber-optic equation is the chore of getting it into the walls. Fiber-optic cabling installations are tedious and difficult, although fiber-optic manufacturers continue to make new strides in easing the job. Fiber-optic cabling is fragile and will fail if it is bent much. My advice: leave this job to a professional cable installer.

NOTE Chapter 6, "Modern Ethernet," goes into fiber-optic technology in more detail.

TIP Concentrate on UTP—that's where the hardest Network+ questions lie. Don't forget to give STP and fiber a quick pass, and make sure you understand the reasons for picking one type of cabling over another. Even though Network+ doesn't test too hard on cabling, this is important information that you will use in the real networking world.

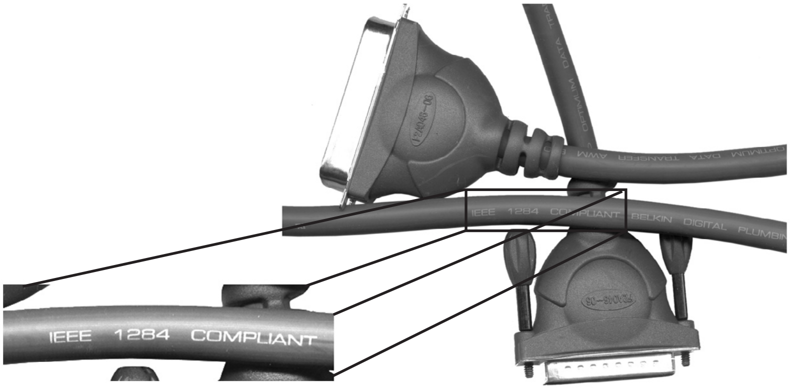
Networking Industry Standards—IEEE

The *Institute of Electrical and Electronics Engineers (IEEE)* defines industry-wide standards that promote the use and implementation of technology. In February of 1980, a new committee called the 802 working group took over the job of defining network standards from the private sector. The IEEE 802 committee defines frames, speed, distances, and types of cabling to use in a network environment. Concentrating on cables, the IEEE recognizes that no single cabling solution can work in all situations, and thus provides a variety of cabling standards.

IEEE committees define standards for a wide variety of electronics. The names of these committees are often used to refer to the standards they publish. The IEEE 1284 committee, for example, sets standards for parallel communication. Have you ever seen a printer cable marked "IEEE 1284-compliant," as in Figure 4-19? This means the manufacturer followed the rules set by the IEEE 1284 committee. Another committee you may have heard of is the IEEE 1394 committee, which controls the FireWire standard.

The IEEE 802 committee sets the standards for networking. Although the original plan was to define a single, universal standard for networking, it quickly became apparent that no single solution would work for all needs. The 802 committee was split into smaller subcommittees, with names such as IEEE 802.3 and IEEE 802.5. Table 4-2 shows the currently recognized IEEE 802 subcommittees and their areas of jurisdiction.

Figure 4-19
An IEEE 1284-compliant printer cable



IEEE 802	LAN/MAN Overview & Architecture
IEEE 802.1	LAN/MAN Bridging and Management (Higher Layer LAN Protocols)
IEEE 802.1s	Multiple Spanning Tree
IEEE 802.1w	Rapid Reconfiguration of Spanning Tree
IEEE 802.1x	Port-based Network Access Control
IEEE 802.2	Logical Link Control (LLC)
IEEE 802.3	CSMA/CD access method (Ethernet)
IEEE 802.3ae	10 Gigabit Ethernet
IEEE 802.4	Token Passing Bus access method and Physical layer specifications
IEEE 802.5	Token Ring access method and Physical layer specifications
IEEE 802.6	Distributed Queue Dual Bus (DQDB) access method and Physical layer specifications (Metropolitan Area Networks)
IEEE 802.7	Broadband LAN
IEEE 802.8	Fiber Optic
IEEE 802.9	Isochronous LANs (standard withdrawn)
IEEE 802.10	Interoperable LAN/MAN Security
IEEE 802.11	Wireless LAN Medium Access Control (MAC) and Physical layer specifications
IEEE 802.12	Demand-priority access method, Physical layer, and repeater specifications
IEEE 802.13	Not used
IEEE 802.14	Cable modems (proposed standard withdrawn)
IEEE 802.15	Wireless Personal Area Network (WPAN)
IEEE 802.16	Wireless Metropolitan Area Network (Wireless MAN)
IEEE 802.17	Resilient Packet Ring (RPR) Access

Table 4-2 IEEE 802 subcommittees

TIP Memorize the 802.2, 802.3, 802.5, and 802.11 standards. Ignore the rest.

Some of these committees deal with technologies that didn't quite make it, and the committees associated with those standards, such as IEEE 802.4, Token Bus, have become dormant. When preparing for the Network+ exam—and more important, for real-life networking situations—concentrate on the IEEE 802.3, 802.5, and 802.11 standards. The others rarely impact the life of a network tech directly. You'll see each of the three main 802 standards in detail in later chapters.

Chapter Review

Questions

1. Which of the following standards defines Token Ring networks?
   - **A.** IEEE 802.3
   - **B.** IEEE 802.5
   - **C.** EIA/TIA 568A
   - **D.** IEEE 1284
2. Token Ring networks use a ______________ physical topology and a _______________ logical topology.
   - **A.** Mesh, ring
   - **B.** Ring, star
   - **C.** Star, ring
   - **D.** Ring, bus
3. Of the topologies listed, which one is the most fault-tolerant and has the most redundancy?
   - **A.** Mesh
   - **B.** Bus
   - **C.** Star
   - **D.** Ring
4. What term is used to describe the logical layout of network components?
   - **A.** Segmentation
   - **B.** Map
   - **C.** Topology
   - **D.** Protocol

5. Which of the following IEEE standards defines wireless networking?
   A. 802.8
   B. 802.9
   C. 802.10
   D. 802.11
6. Which IEEE standard defines the CSMA/CD access method?
   A. 802.2
   B. 802.3
   C. 802.4
   D. 802.5
7. Which of the following is *not* a type of coaxial cable?
   A. RJ-45
   B. RG-58
   C. RG-8
   D. RG-6
8. Which network topology connects nodes with a central ring of cable?
   A. Star
   B. Bus
   C. Ring
   D. Mesh
9. Which network topology uses a central hub?
   A. Star
   B. Bus
   C. Ring
   D. Mesh
10. Which of the following network topologies is the easiest to configure?
   A. Star
   B. Bus
   C. Ring
   D. Mesh

Answers

1. **B.** IEEE 802.5 defines Token Ring networks. EIA/TIA 568A is a cabling standard for UTP cabling that is used in both Token Ring and Ethernet networks.
2. **C.** Token Ring networks use a star physical topology and a ring logical topology.
3. **A.** Mesh topology is the most fault-tolerant and has the most redundancy because each computer has a dedicated connection to every other computer on the network.
4. **C.** *Topology* is the term used to describe the layout of a network: how computers connect to each other without regard to how they communicate.
5. **D.** The IEEE 802.11 standard defines wireless networking.
6. **B.** The IEEE 802.3 standard defines the CSMA/CD access method, part of the Ethernet standard.
7. **A.** RJ-45 is a type of connector used on unshielded twisted pair cables. All the others are types of coaxial cable.
8. **C.** The aptly named ring topology connects nodes with a central ring of cable.
9. **A.** A star topology uses a central hub.
10. **A.** A star topology is the easiest to configure.