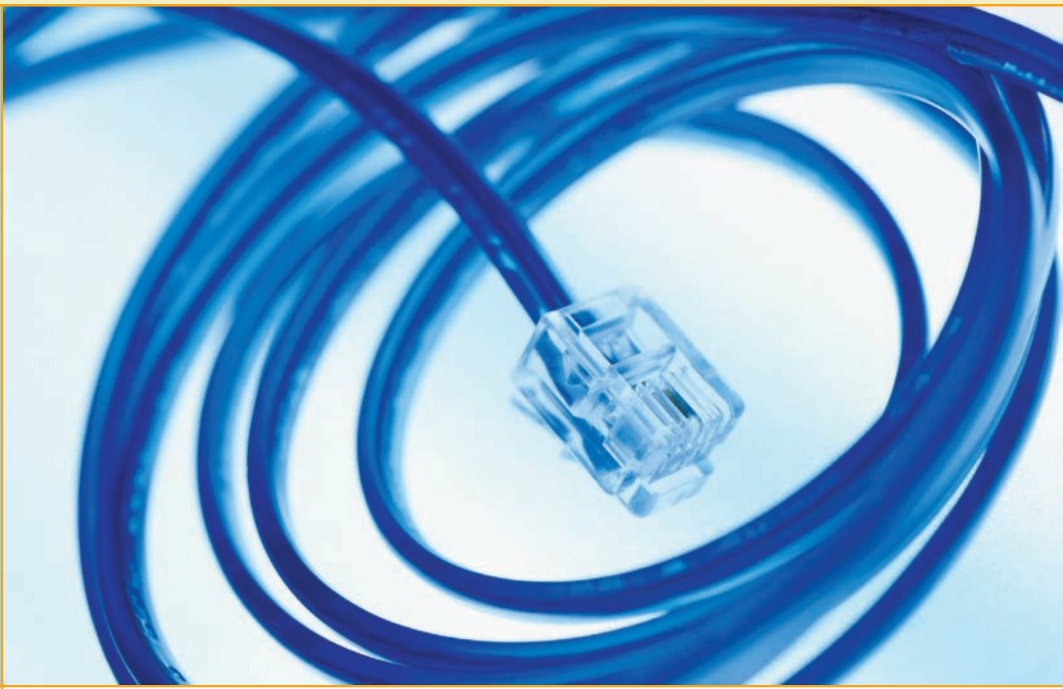
chapter 4

Ethernet Basics

"In theory there is no difference between theory and practice. In practice there is."

—YOGI BERRA



In this chapter, you will learn how to

- **Define and describe Ethernet**
- **Explain early Ethernet implementations**
- **Describe ways to extend and enhance Ethernet networks**

In the beginning, there were no networks. Computers were isolated, solitary islands of information in a teeming sea of proto-geeks, who used clubs and wore fur pocket protectors. Okay, maybe it wasn't that bad, but if you wanted to move a file from one machine to another—and proto-geeks were as much into that as modern geeks—you had to use *Sneakernet*, which meant you saved the file on a disk, laced up your tennis shoes, and hiked over to the other system. All that walking no doubt produced lots of health benefits, but frankly, proto-geeks weren't all that into health benefits—they were into speed, power, and technological coolness in general. (Sound familiar?) It's no wonder, then, that geeks everywhere agreed on the need to replace Sneakernet with a faster and more efficient method of sharing data. The method they came up with is the subject of this chapter.

Historical/Conceptual

Ethernet

In 1973, Xerox answered the challenge of moving data without sneakers by developing **Ethernet**, a networking technology standard based on a bus topology. The Ethernet standard dominates today's networks and defines all of the issues involved in transferring data between computer systems. The original Ethernet used a single piece of coaxial cable in a bus topology to connect several computers, enabling them to transfer data at a rate of up to 3 Mbps. Although slow by today's standards, this early version of Ethernet was a huge improvement over Sneakernet methods, and served as the foundation for all later versions of Ethernet.

Ethernet remained a largely in-house technology within Xerox until 1979, when Xerox decided to look for partners to help promote Ethernet as an industry standard. Xerox worked with Digital Equipment Corporation (DEC) and Intel to publish what became known as the Digital-Intel-Xerox (DIX) standard. Running on coaxial cable, the DIX standard enabled multiple computers to communicate with each other at a screaming 10 Mbps. Although 10 Mbps represents the low end of standard network speeds today, at the time it was revolutionary. These companies then transferred control of the Ethernet standard to the IEEE, which in turn created the **802.3 (Ethernet)** committee that continues to control the Ethernet standard to this day.

Given that Ethernet's been around for so long, we need to start at a common point. I've chosen to use 10BaseT, the earliest version of Ethernet designed to use UTP cabling. At this point, don't worry what 10BaseT means—this chapter will cover the definition. For right now, just get into the idea of how Ethernet works.

Ethernet's designers faced the same challenges as the designers of any network: how to send data across the wire, how to identify the sending and receiving computers, and how to determine which computer should use the shared cable at what time. The engineers resolved these issues by using data frames that contain MAC addresses to identify computers on the network, and by using a process called CSMA/CD (discussed shortly) to determine which machine should access the wire at any given time. You saw some of this in action in Chapter 2, "Building a Network with the OSI Model," but now I need to introduce you to a bunch of new terms, so let's look at each of these solutions.

Topology

Every version of Ethernet invented since the early 1990s uses a hybrid star-bus topology. At the center of the network is a **hub**. This hub is nothing more than an electronic **repeater**—it interprets the ones and zeros coming in from one port and repeats the same signal out to the other connected ports. Hubs do not send the same signal back down the port that originally sent it (Figure 4.1). Repeaters are not amplifiers! They read the incoming signal and send new copies of that signal out to every connected port on the hub.

Tech Tip

IEEE

The source for all things Ethernet is but a short click away on the Internet. For starters, check out www.ieee802.org.

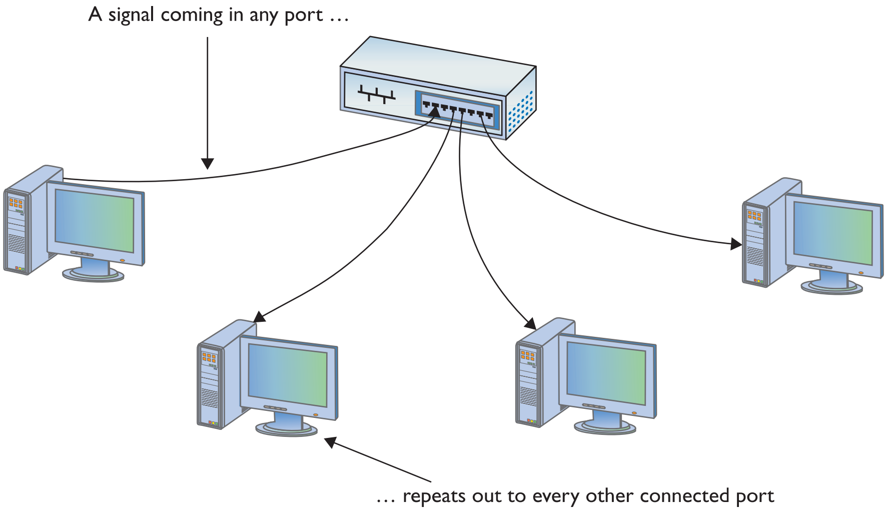
There have been many versions of Ethernet over the years. The earliest versions, named 10Base5 and 10Base2, are long obsolete. As of 2009, CompTIA finally dropped these ancient technologies from the CompTIA Network+ exam. Rest in peace, 10Base5 and 10Base2!

Tech Tip

Defining Ethernet

Providing a clear and concise definition of Ethernet has long been one of the major challenges in teaching networking. This difficulty stems from the fact that Ethernet has changed over the years to incorporate new and improved technology. Most folks won't even try to define Ethernet, but here's my best attempt at a current definition.

Ethernet is a standard for a family of network technologies that share the same basic bus topology, frame type, and network access method. Because the technologies share these essential components, you can communicate between them just fine. The implementation of the network might be different, but the frames remain the same.


A signal coming in any port …
… repeats out to every other connected port

• **Figure 4.1** Ethernet hub

Test Specific

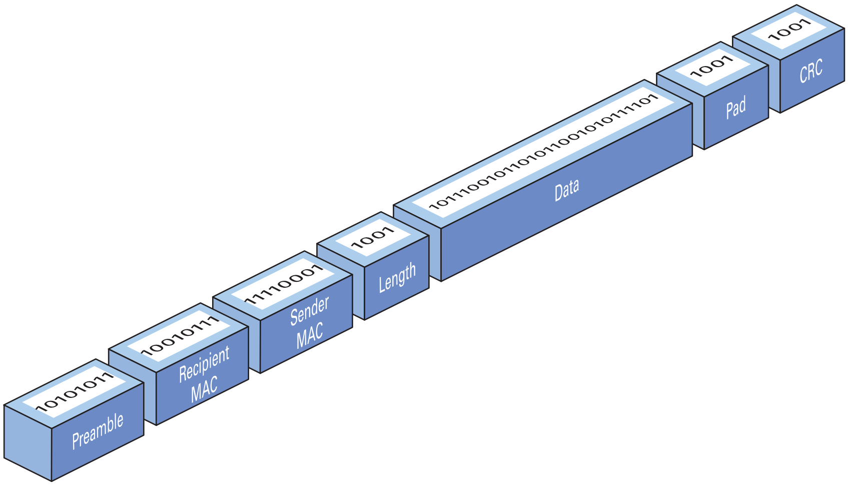
Organizing the Data: Ethernet Frames

The terms *frame* and *packet* are often used interchangeably, especially on exams! This book uses the terms more strictly. You'll recall from Chapter 2, "Building a Network with OSI," that frames are based on MAC addresses; packets are generally associated with data assembled by the IP protocol at Layer 3 of the OSI seven-layer model.

All network technologies break data transmitted between computers into smaller pieces called **frames**, as you'll recall from Chapter 2. Using frames addresses two networking issues. First, it prevents any single machine from monopolizing the shared bus cable. Second, frames make the process of retransmitting lost data more efficient.

The process you saw in Chapter 2 of transferring a word processing document between two computers illustrates these two issues. First, if the sending computer sends the document as a single huge frame, it will monopolize the cable and prevent other machines from using the cable until the entire file gets to the receiving system. Using relatively small frames enables computers to share the cable easily—each computer listens on the **segment**, sending a few frames of data whenever it detects that no other computer is transmitting. Second, in the real world, bad things can happen to good data. When errors occur during transmission, the sending system must retransmit the frames that failed to get to the receiving system in good shape. If a word processing document were transmitted as a single massive frame, the sending system would have to retransmit the entire frame—in this case, the entire document. Breaking the file up into smaller frames enables the sending computer to retransmit only the damaged frames. Because of their benefits—shared access and more efficient retransmission—all networking technologies use frames, and Ethernet is no exception to that rule.

In Chapter 2, you saw a generic frame. Let's take what you know of frames and expand on that knowledge by inspecting the details of an Ethernet frame. A basic Ethernet frame contains seven pieces of information: the preamble, the MAC address of the frame's recipient, the MAC address of the sending system, the length of the data, the data itself, a pad, and a frame check



• Figure 4.2 Ethernet frame

sequence, generically called a cyclic redundancy check (CRC). Figure 4.2 shows these components.

Preamble

All Ethernet frames begin with a **preamble**, a 64-bit series of alternating ones and zeroes that ends with 11. The preamble gives a receiving NIC time to realize a frame is coming and to know exactly where the frame starts. The preamble is added by the sending NIC.

MAC Addresses

Each NIC, more commonly called a **node**, on an Ethernet network must have a unique identifying address. Ethernet identifies the NICs on a network using special 48-bit (6-byte) binary addresses known as **MAC addresses**.

MAC addresses give each NIC a unique address. When a computer sends out a data frame, it goes into the hub that repeats an exact copy of that frame to every connected port, as shown in Figure 4.3. All the other computers on the network listen to the wire and examine the frame to see if it contains their MAC address. If it does not, they ignore the frame. If a machine sees a frame with its MAC address, it opens the frame and begins processing the data.

This system of allowing each machine to decide which frames it will process may be efficient, but because any device connected to the network cable can potentially capture any data frame transmitted across the wire, Ethernet networks carry a significant security vulnerability. Network diagnostic programs, commonly called **sniffers**, can order a NIC to run in **promiscuous mode**. When running in promiscuous mode, the NIC processes all the

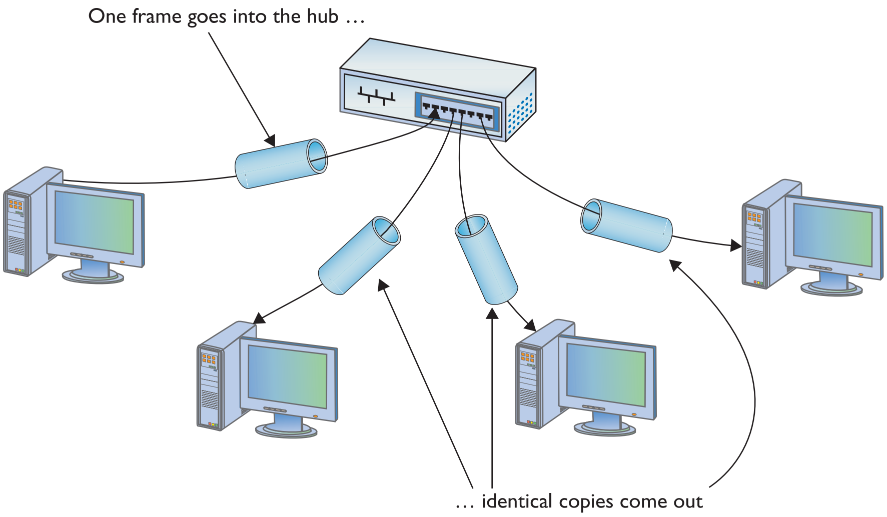
The CompTIA Network+ exam might describe MAC addresses as 48-bit binary addresses or 6-byte binary addresses.

Cross Check

NICs and OSI

You learned about NICs and MAC addresses in Chapter 2, "Building a Network with the OSI Model," so check your memory with these questions. Where does the NIC get its MAC address? How does the MAC address manifest on the card? At what layer or layers of the OSI seven-layer model does the NIC operate?

There are many situations in which one computer might have two or more NICs, so one physical system might represent more than one node.



• Figure 4.3 Frames propagating on a network

frames it sees on the cable, regardless of their MAC addresses. Sniffers are valuable troubleshooting tools in the right hands, but Ethernet provides no protections against their unscrupulous use.

Length

An Ethernet frame may carry up to 1500 bytes of data in a single frame, but this is only a maximum. Frames can definitely carry fewer bytes of data. The length field tells the receiving system how many bytes of data this frame is carrying.

Data

The data part of the frame contains whatever data the frame carries. (If this is an IP network, it will also include extra information, such as the IP addresses of both systems, sequencing numbers, and other information.)

Pad

The minimum Ethernet frame is 64 bytes in size, but not all of that has to be actual data. If an Ethernet frame has fewer than 64 bytes of data to haul, the sending NIC will automatically add extra data—a **pad**—to bring the data up to the minimum 64 bytes.

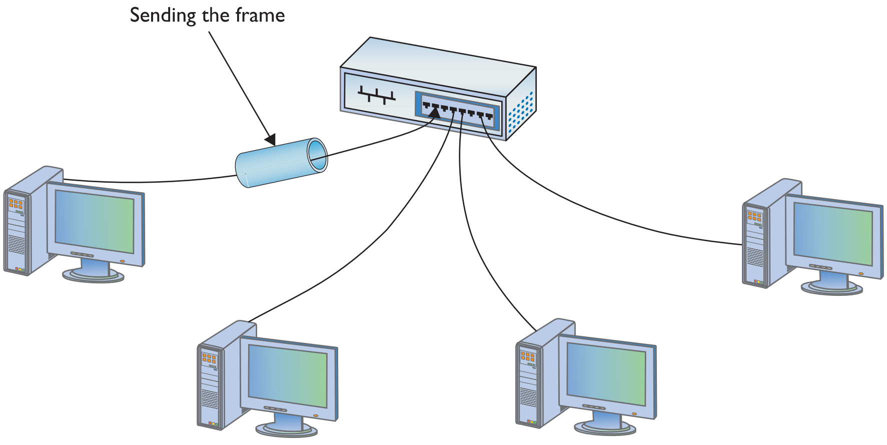
Frame Check Sequence

The **frame check sequence**—Ethernet's term for the cyclic redundancy check—enables Ethernet nodes to recognize when bad things happen to good data. Machines on a network must be able to detect when data has been damaged in transit. To detect errors, the computers on an Ethernet network attach a special code to each frame. When creating an Ethernet frame, the sending machine runs the data through a special mathematical formula and attaches the result, the frame check sequence, to the frame. The receiving machine opens the frame, performs the same calculation, and compares its answer with the one included with the frame. If the answers do not match, the receiving machine asks the sending machine to retransmit that frame.

At this point, those crafty network engineers have solved two of the problems facing them: they've created frames to organize the data to be sent, and put in place MAC addresses to identify machines on the network. But the challenge of determining which machine should send data at which time required another solution: CSMA/CD.

CSMA/CD

Ethernet networks use a system called **carrier sense, multiple access/collision detection (CSMA/CD)** to determine which computer should use a shared cable at a given moment. *Carrier sense* means that each node using the network examines the cable before sending a data frame (Figure 4.4). If another machine is using the network, the node detects traffic on the segment, waits a few milliseconds, and then rechecks. If it detects no traffic—the more common term is to say the cable is "free"—the node sends out its frame.

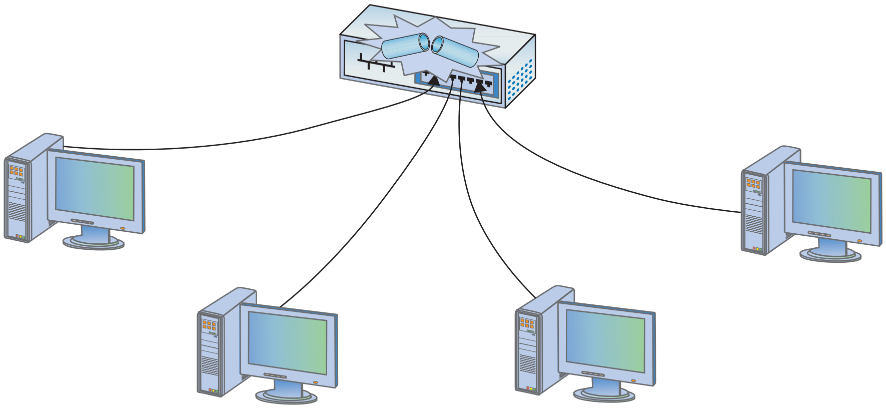


• **Figure 4.4** No one else is talking—send the frame!

Multiple access means that all machines have equal access to the wire. If the line is free, any Ethernet node may begin sending a frame. From the point of view of Ethernet, it doesn't matter what function the node is performing: it could be a desktop system running Windows XP, or a high-end file server running Windows Server 2008 or even Linux. As far as Ethernet is concerned, a node is a node is a node, and access to the cable is assigned strictly on a first-come, first-served basis.

CSMA/CD is a network access method that maps to the IEEE 802.3 standard for Ethernet networks.

So what happens if two machines, both listening to the cable, simultaneously decide that it is free and try to send a frame? A collision occurs, and both of the transmissions are lost (Figure 4.5). A collision resembles the effect of two people talking at the same time: the listener hears a mixture of two voices, and can't understand either one.

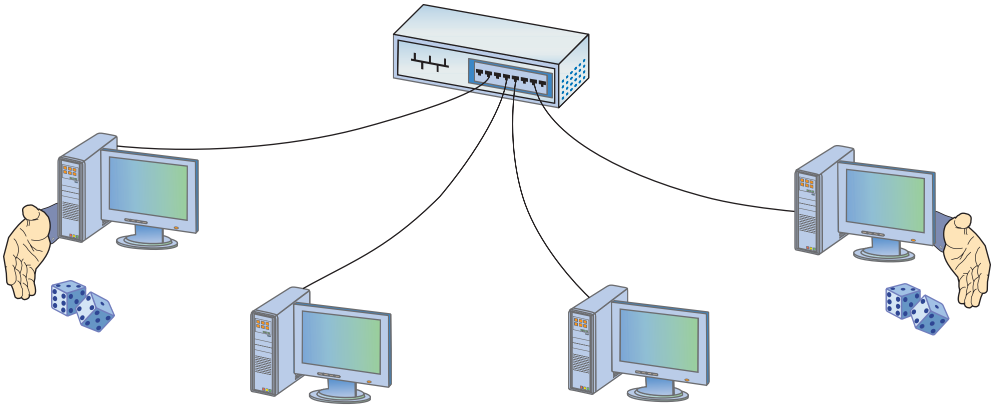


• **Figure 4.5** Collision!

It's easy for NICs to notice a collision. Collisions create nonstandard voltages that tell each NIC another node has transmitted at the same time. If they detect a collision, both nodes immediately stop transmitting. They then each generate a random number to determine how long to wait before trying again. If you imagine that each machine rolls its magic electronic dice and waits for that number of seconds, you wouldn't be too far from the truth, except that the amount of time an Ethernet node waits to retransmit is much shorter than one second (Figure 4.6). Whichever node generates the lowest random number begins its retransmission first, winning the competition to use the wire. The losing node then sees traffic on the wire, and waits for the wire to be free again before attempting to retransmit its data.

In an Ethernet network, a **collision domain** is a group of nodes that hear each other's traffic. A segment is certainly a collision domain, but there are ways to connect segments together to create larger collision domains. If the collision domain gets too large, you'll start running into traffic problems that manifest as general network sluggishness. That's one of the reasons to break up networks into smaller groupings.

Collisions are a normal part of the operation of an Ethernet network. Every Ethernet network wastes some amount of its available bandwidth dealing with these collisions. A properly running average Ethernet network has a maximum of 10 percent collisions. For every 20 frames sent, approximately



• **Figure 4.6** Rolling for timing

2 frames will collide and require a resend. Collision rates greater than 10 percent often point to damaged NICs or out-of-control software.

Early Ethernet Networks

Now we have the answers to many of the questions that faced those early Ethernet designers. MAC addresses identify each machine on the network. CSMA/CD determines which machine should have access to the cable when. But all this remains in the realm of theory—we still need to build the thing! Contemplating the physical network brings up numerous questions. What kind of cables should be used? What should they be made of? How long can they be? For these answers, turn to the IEEE 802.3 standard and two early implementations of Ethernet, 10BaseT and 10BaseFL.

10BaseT

In 1990, the IEEE 802.3 committee created a new version of Ethernet called **10BaseT** to modernize the first generations of Ethernet. Very quickly 10BaseT became the most popular network technology in the world, replacing competing and now long-gone competitors with names like Token Ring and AppleTalk. Over 99 percent of all networks use 10BaseT or one of its faster, newer, but very similar versions. The classic 10BaseT network consists of two or more computers connected to a central hub. The NICs connect with wires as specified by the 802.3 committee.

• **Figure 4.7** Two 10BaseT hubs

10BaseT hubs come in a variety of shapes and sizes to support different sizes of networks. The biggest differentiator between hubs is the number of **ports** (connections) that a single hub provides. A small hub might have only 4 ports, while a hub for a large network might have 48 ports. As you may imagine, the more ports on a hub, the more expensive the hub. Figure 4.7 shows two hubs. On the top is a small, 8-port

Cross Check

Physical vs. Logical

You might be tempted at this moment to define 10BaseT in terms of physical topology versus logical topology—after all, it uses a physical star, but a logical bus. But refer to Chapter 3, "Cabling and Topology," and cross-check your memory. What's a physical topology? And a logical topology? What would you say if you walked into an office building that implemented a 10BaseT network? Yes, if you actually *walked into* it, you'd probably say "Ouch!" But beyond that, think about how you would describe the wires and connectors you would see in terms of physical or logical topology.

hub for small offices or the home. It rests on a 12-port rack-mount hub for larger networks.

Regardless of size, all 10BaseT hubs need electrical power. Larger hubs will take power directly from a power outlet, while smaller hubs often come with an AC adapter. In either case, if the hub loses power, the entire segment will stop working.

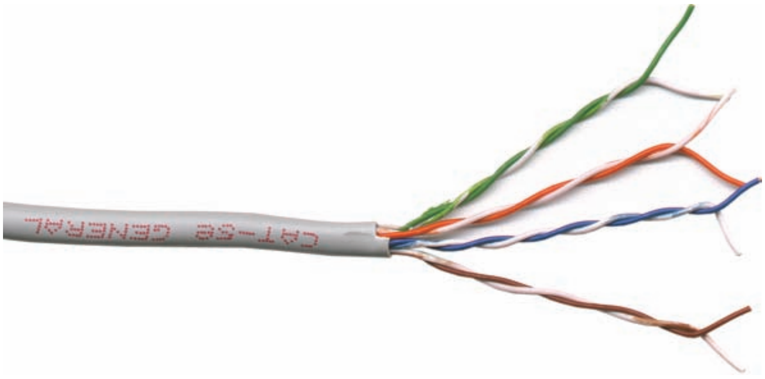
The name 10BaseT follows roughly the naming convention used for earlier Ethernet cabling systems. The number *10* refers to the speed: 10 Mbps. The word *Base* refers to the signaling type: baseband. The letter *T* refers to the type of cable used: twisted-pair. 10BaseT uses unshielded twisted-pair (UTP) cabling.

If you ever run into a situation on a 10BaseT or later network in which none of the computers can get on the network, always first check the hub!

The names of two earlier true bus versions of Ethernet, 10Base5 and 10Base2, gave the maximum length of the bus. 10Base5 networks could be up to 500 meters long, for example, whereas 10Base2 could be almost 200 meters (though in practice topped out at 185 meters).

UTP

Officially, 10BaseT requires the use of CAT 3 (or higher), two-pair, unshielded twisted-pair (UTP) cable. One pair of wires sends data to the hub while the other pair receives data from the hub. Even though 10BaseT only requires two-pair cabling, everyone installs four-pair cabling to connect devices to the hub as insurance against the possible requirements of newer types of networking (Figure 4.8). Most UTP cables come with stranded Kevlar fibers to give the cable added strength, which in turn enables installers to pull on the cable without excessive risk of literally ripping it apart.



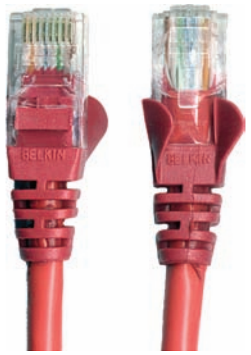
• **Figure 4.8** A typical four-pair CAT 5e unshielded twisted-pair cable

Cross Check

Check Your CATs!

You've already seen CAT levels in Chapter 3, "Cabling and Topology," so check your memory and review the different speeds of the various CAT levels. Could 10BaseT use CAT 2? Could it use CAT 6? What types of devices can use CAT 1?

10BaseT also introduced the networking world to the **RJ-45 connector** (Figure 4.9). Each pin on the RJ-45 connects to a single wire inside the cable; this enables devices to put voltage on the individual wires within the cable. The pins on the RJ-45 are numbered from 1 to 8, as shown in Figure 4.10. The 10BaseT standard designates some of these numbered wires for specific purposes. As mentioned earlier, although the cable has four pairs, 10BaseT uses only two of the pairs. 10BaseT devices use pins 1 and 2 to send data, and pins 3 and 6 to receive data. Even though one pair of wires sends data and another receives data, a 10BaseT device cannot send and receive simultaneously. The rules of CSMA/CD still apply: only one device can use the segment contained in the hub without causing a collision. Later versions of Ethernet will change this rule.

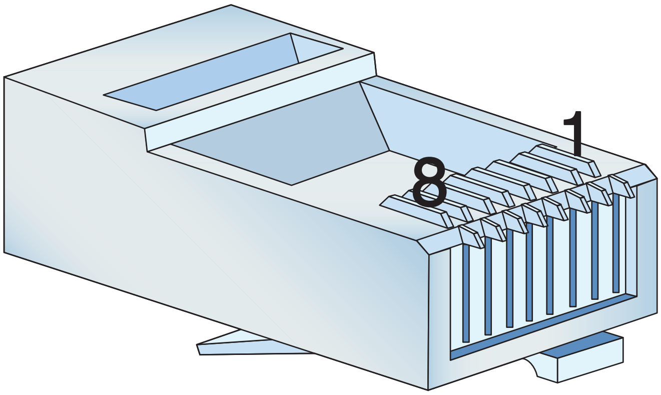


• Figure 4.9 Two views of an RJ-45 connector

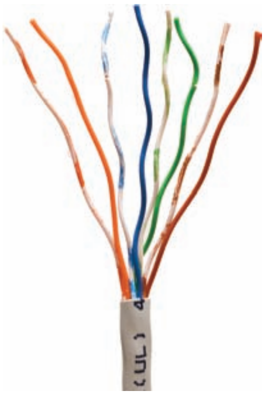
The real name for RJ-45 is "8 Position 8 Contact (8P8C) modular plug." The name RJ-45 is so dominant, however, that nobody but the nerdiest of nerds calls it by its real name. Stick to RJ-45.

An RJ-45 connector is usually called a *crimp*, and the act (some folks call it an art) of installing a crimp onto the end of a piece of UTP cable is called *crimping*. The tool used to secure a crimp onto the end of a cable is a **crimper**. Each wire inside a UTP cable must connect to the proper pin inside the crimp. Manufacturers color-code each wire within a piece of four-pair UTP to assist in properly matching the ends. Each pair of wires consists of a solid-colored wire and a striped wire: blue/blue-white, orange/orange-white, brown/brown-white, and green/green-white (Figure 4.11).

The Telecommunications Industry Association/Electronics Industries Alliance (TIA/EIA) defines the industry standard for correct crimping of four-pair UTP for 10BaseT networks. Two standards currently exist: **TIA/EIA 568A** and **TIA/EIA 568B**. Figure 4.12 shows the TIA/EIA 568A and TIA/EIA 568B color-code standards. Note that the wire pairs used by 10BaseT (1 and 2; 3 and 6) come from the same color pairs (green/green-white and orange/orange-white). Following an established color-code scheme, such as TIA/EIA 568A, ensures that the wires match up correctly at each end of the cable.



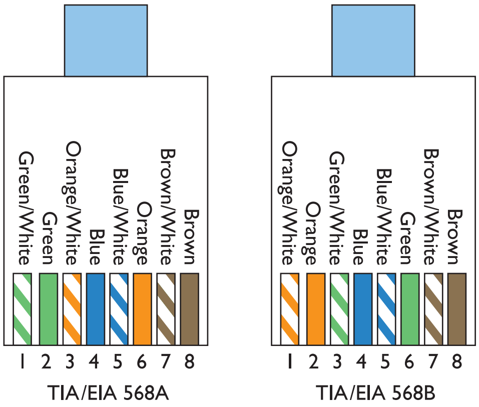
• Figure 4.10 The pins on an RJ-45 connector are numbered 1 through 8.



• Figure 4.11 Color-coded pairs

The ability to make your own Ethernet cables is a real plus for a busy network tech. With a reel of CAT 5e, a bag of RJ-45 connectors, a moderate investment in a crimping tool, and a little practice, you can kiss those mass-produced cables goodbye! You can make cables to your own length specifications, replace broken RJ-45 connectors that would otherwise mean tossing an entire cable—and in the process, save your company or clients time and money.

Why do the 568 standards say to split one of the pairs to the 3 and 6 positions? Wouldn't it make more sense to wire them sequentially (1 and 2; 3 and 4; 5 and 6; 7 and 8)? The reason for this strange wiring scheme stems from the telephone world. A single telephone line uses two wires, and a typical RJ-11 connector has four connections. A single line is wired in the 2 and 3 positions; if the RJ-11 is designed to support a second phone line, the other pair is wired at 1 and 4. TIA/EIA kept the old telephone standard for backward compatibility. This standardization doesn't stop at the wiring scheme: you can plug an RJ-11 connector into an RJ-45 outlet.



• **Figure 4.12** The TIA/EIA 568A and 568B standards

Tech Tip

568A and 568B

An easy trick to remembering the difference between 568A and 568B is the word "GO." The green and orange pairs are swapped between 568A and 568B, whereas the blue and brown pairs stay in the same place!

10BaseT Limits and Specifications

Like any other Ethernet cabling system, 10BaseT has limitations, both on cable distance and on the number of computers. The key distance limitation for 10BaseT is the distance between the hub and the computer. The twisted-pair cable connecting a computer to the hub may not exceed 100 meters in length. A 10BaseT hub can connect no more than 1024 computers, although that limitation rarely comes into play. It makes no sense for vendors to build hubs that large—or more to the point, that *expensive*—because excessive collisions can easily bog down Ethernet performance with far fewer than 1024 computers.

10BaseT Summary

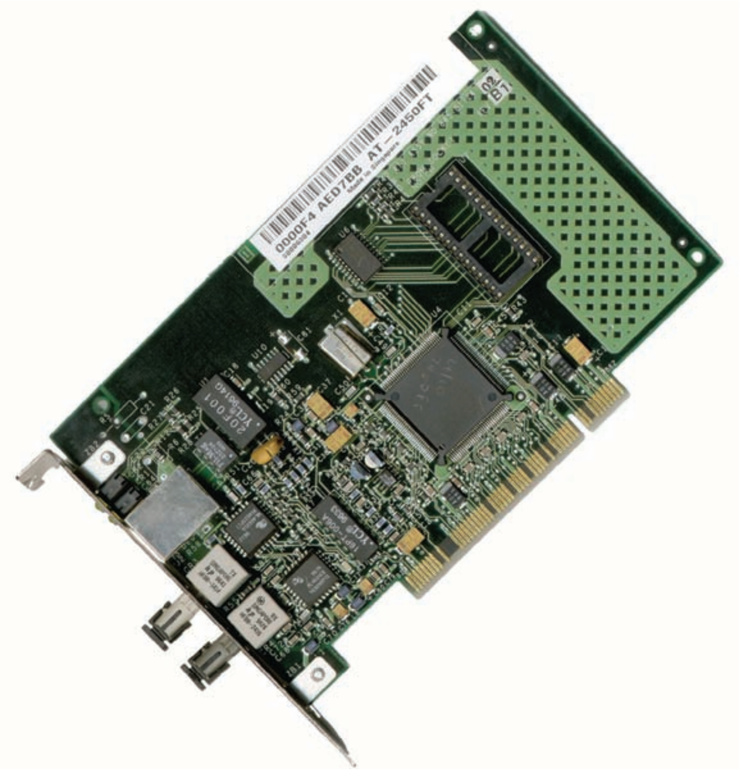
- **Speed** 10 Mbps
- **Signal type** Baseband
- **Distance** 100 meters between the hub and the node
- **Node Limit** No more than 1024 nodes per hub
- **Topology** Star-bus topology: physical star, logical bus
- **Cable type** Uses CAT 3 or better UTP cabling with RJ-45 connectors

For the CompTIA Network+ exam, you won't be tested on the TIA/EIA 568A or B color codes. Just know that they are industry-standard color codes for UTP cabling.

10BaseFL

Just a few years after the introduction of 10BaseT, a fiber-optic version appeared, called **10BaseFL**. As you know from the previous chapter, fiber-optic cabling transmits data packets using pulses of light instead of using electrical current. Using light instead of electricity addresses the three key weaknesses of copper cabling. First, optical signals can travel much farther. The maximum length for a 10BaseFL cable is up to 2 kilometers, depending on how it is configured. Second, fiber-optic cable is immune to electrical interference, making it an ideal choice for high-interference environments. Third, the cable is much more difficult to tap into, making it a good choice for environments with security concerns. 10BaseFL uses *multimode* fiber-optic and employs either an SC or an ST connector.

10BaseFL is often just called 10BaseF.



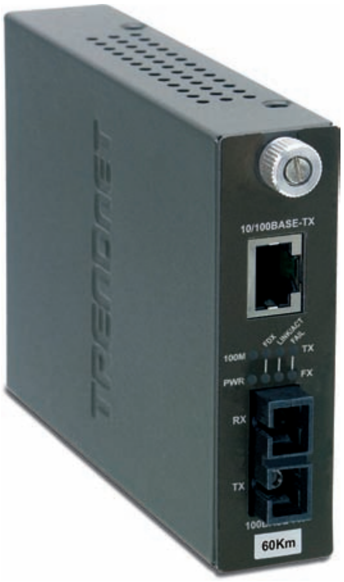
• **Figure 4.13** Typical 10BaseFL card

Figure 4.13 shows a typical 10BaseFL card. Note that it uses two fiber connectors—one to send, and one to receive. All fiber-optic networks use at least two fiber-optic cables. While 10BaseFL enjoyed some popularity for a number of years, most networks today are using the same fiber-optic cabling to run far faster network technologies.

10BaseFL Summary

- **Speed** 10 Mbps
- **Signal type** Baseband
- **Distance** 2000 meters between the hub and the node
- **Node limit** No more than 1024 nodes per hub
- **Topology** Star-bus topology: physical star, logical bus
- **Cable type** Uses multimode fiber-optic cabling with ST or SC connectors

So far you've seen two different flavors of Ethernet, 10BaseT and 10BaseFL. Even though these use different cabling and hubs, the actual packets are still Ethernet packets. As a result, it's common to interconnect different flavors of Ethernet. Since 10BaseT and 10BaseFL use different types of cable, you can use a **media converter** (Figure 4.14) to interconnect different Ethernet types.



• **Figure 4.14** Typical copper-to-fiber Ethernet media connecter (photo courtesy of TRENDnet)

Extending and Enhancing Ethernet Networks

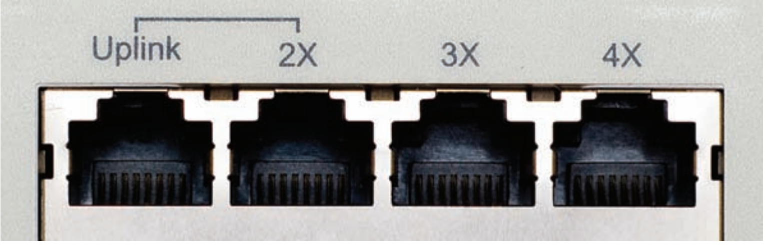
Once you have an Ethernet network in place, you can extend or enhance that network in several ways. You can install additional hubs to connect multiple local area networks, for example. A network bridge can connect two Ethernet segments, effectively doubling the size of a collision domain. You can also replace the hubs with better devices to reduce collisions.

Connecting Ethernet Segments

Sometimes, one hub is just not enough. Once an organization uses every port on its existing hub, adding additional nodes requires additional hubs or a device called a bridge. Even fault tolerance can motivate an organization to add more hubs. If every node on the network connects to the same hub, that hub becomes a single point of failure—if it fails, everybody drops off the network. There are two ways to connect hubs: an uplink port or a crossover cable. You can also connect Ethernet segments using a bridge.

Uplink Ports

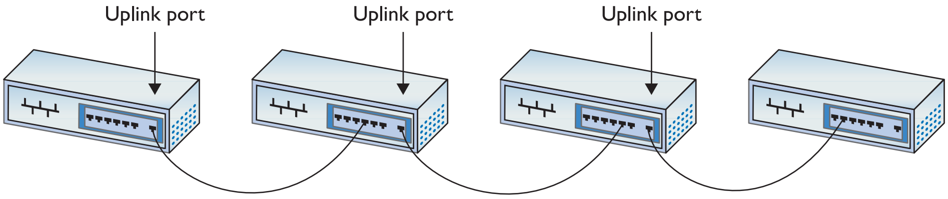
Uplink ports enable you to connect two hubs together using a straight-through cable. They're always clearly marked on the hub, as shown in Figure 4.15. To connect two hubs, insert one end of a cable to the uplink and the other cable to any one of the regular ports. To connect more than two hubs, you must daisy-chain your hubs by using one uplink port and one regular port. Figure 4.16 shows properly daisy-chained hubs. As a rule, you cannot daisy-chain more than four hubs together.



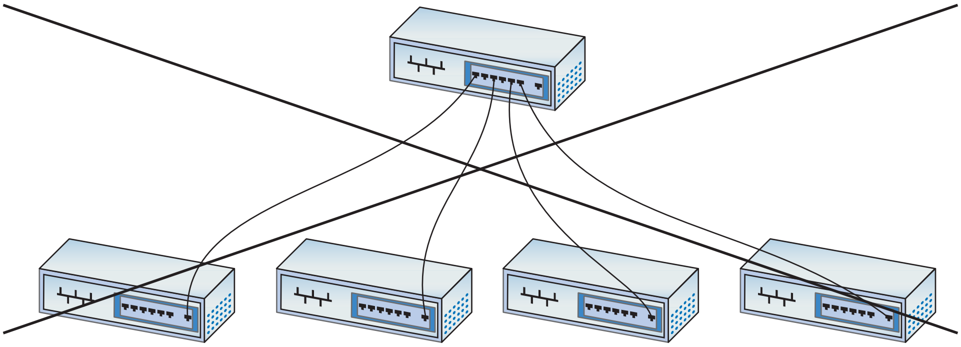
• **Figure 4.15** Typical uplink port

You also cannot use a single central hub and connect multiple hubs to that single hub, as shown in Figure 4.17. It simply won't work.

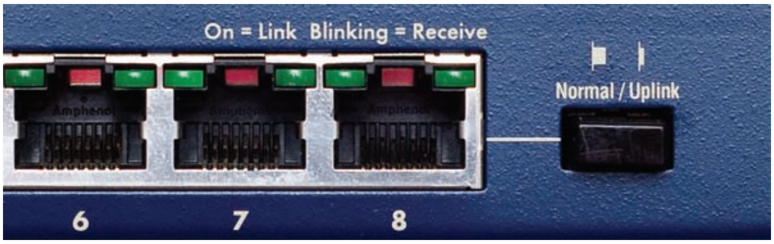
Working with uplink ports is sometimes tricky, so you need to take your time. It's easy to mess up and use a central hub. Hub makers give their uplink ports many different names, such as crossover, MDI-X, and OUT. There are also tricks to using uplink ports. Refer to Figure 4.15 again. See the line connecting the uplink port and the port labeled 2X? You may use only one of those two ports, not both at the same time. Additionally, some hubs



• **Figure 4.16** Daisy-chained hubs



• Figure 4.17 Hierarchical hub configuration. This will not work!



• Figure 4.18 Press-button port

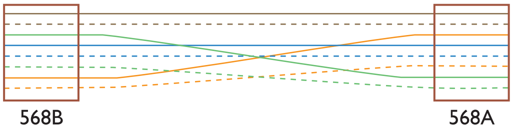
place on one of the ports a switch that you can press to make it either a regular port or an uplink port (Figure 4.18). Pressing the button electronically reverses the wires inside the hub. Be sure to press the button so it works the way you want it to work.

When connecting hubs, remember the following:

- Only daisy-chain hubs.
- Take time to figure out the uplink ports.
- If you plug hubs in incorrectly, no damage will occur—they just won't work.

Crossover Cables

Hubs can also connect to each other via special twisted-pair cables called crossover cables. A standard cable cannot be used to connect two hubs without using an uplink port, because both hubs will attempt to send data on the second pair of wires (3 and 6) and will listen for data on the first pair (1 and 2). A **crossover cable** reverses the sending and receiving pairs on one end of the cable. One end of the cable is wired according to the TIA/EIA 568A standard, while the other end is wired according to the TIA/EIA 568B standard (Figure 4.19). With the sending and receiving pairs reversed, the hubs can hear each other; hence the need for two standards for connecting RJ-45 jacks to UTP cables.



• Figure 4.19 A crossover cable reverses the sending and receiving pairs.

A crossover cable connects to a regular port on each hub. Keep in mind that you can still daisy-chain even when you use crossover cables. Interestingly, many hubs, especially higher-end hubs, do not come with any uplink ports at all. In these cases your only option is to use a crossover cable.

Try This!

Examine Your Uplink Ports

While most hubs come with uplink ports, they all seem to have different ways to use them. Some hubs have dedicated uplink ports, and some have uplink ports that convert to regular ports at the press of a button. Take a look at some hubs and try to figure out how you would use an uplink port to connect it to another hub.

In a pinch, you can use a crossover cable to connect two computers together using 10BaseT NICs with no hub between them at all. This is handy for the quickie connection needed for a nice little home network or when you absolutely, positively must chase down a friend in a computer game!

Be careful about confusing crossover cables with uplink ports. First, never connect two hubs by their uplink ports. Take a regular cable; connect one end to the uplink port on one hub and the other end to any regular port on the other hub. Second, if you use a crossover cable, just plug each end into any handy regular port on each hub.

Bridges

The popularity and rapid implementation of Ethernet networks demanded solutions or workarounds for the limitations inherent in the technology. An Ethernet segment could only be so long and connect a certain number of computers. What if your network went beyond those limitations?

A **bridge** acts like a repeater or hub to connect two Ethernet segments, but it goes one step beyond—filtering and forwarding traffic between those segments based on the MAC addresses of the computers on those segments. This preserves precious bandwidth and makes a larger Ethernet network possible. To *filter* traffic means to stop it from crossing from one network to the next; to *forward* traffic means to pass traffic originating on one side of the bridge to the other.

A newly installed Ethernet bridge initially behaves exactly like a repeater, passing frames from one segment to another. Unlike a repeater, however, a bridge monitors and records the network traffic, eventually reaching a point where it can begin to filter and forward. This makes the bridge more "intelligent" than a repeater. A new bridge usually requires only a few seconds to gather enough information to start filtering and forwarding.

Although bridges offer a good solution for connecting two segments and reducing bandwidth usage, these days you'll mainly find bridges used in wireless, rather than wired, networks. (I cover more on those kinds of bridges in Chapter 16, "Wireless Networking.") Most networks instead have turned to a different magic box, a switch, to extend and enhance an Ethernet network.

Switched Ethernet

As any fighter pilot will tell you, sometimes you just feel the need—the need for speed. While plain-vanilla 10BaseT Ethernet performed well enough for first-generation networks (which did little more than basic file and print sharing), by the early 1990s networks used more-demanding applications, such as Lotus Notes, SAP business management software, and Microsoft Exchange, which quickly saturated a 10BaseT network. Fortunately, those crazy kids over at the IEEE kept expanding the standard, giving the network tech in the trenches a new tool that provided additional bandwidth—the switch.

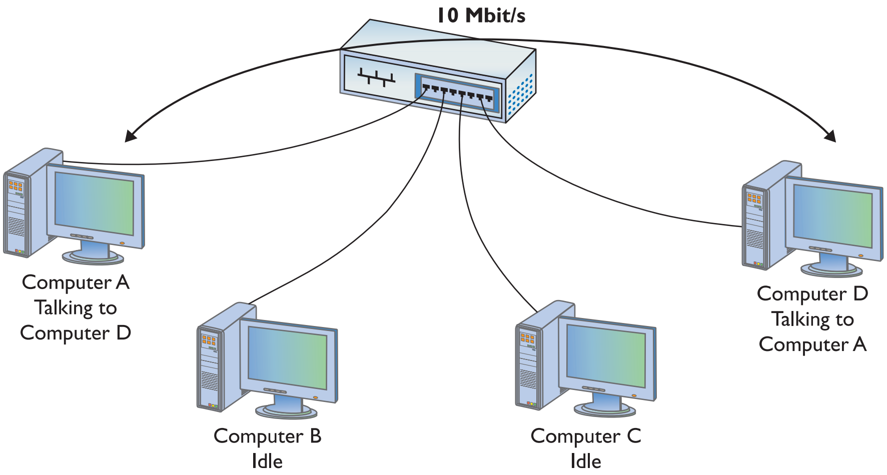
Tech Tip

Crossing Crossovers

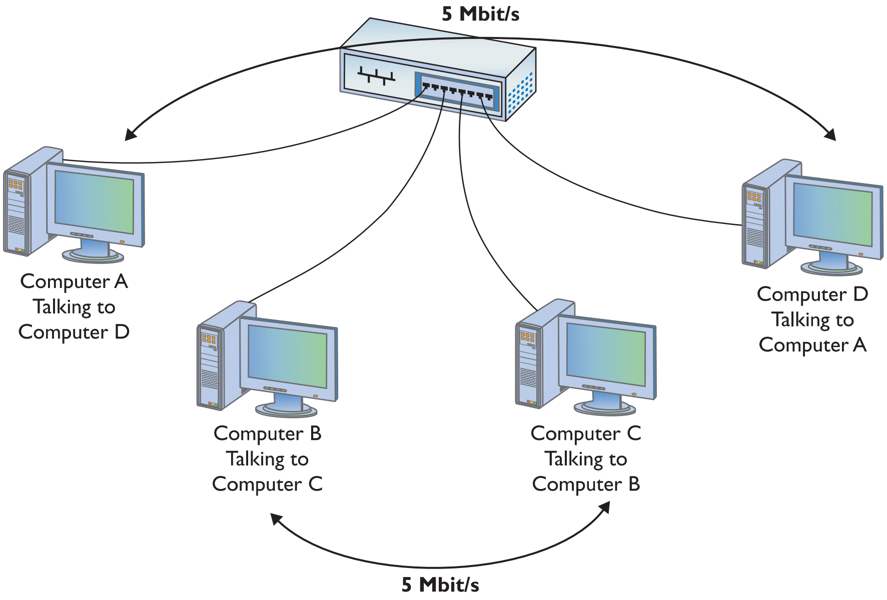
If you mess up your crossover connections, you won't cause any damage, but the connection will not work. Think about it. If you take a straight cable (that is, not a crossover cable) and try to connect two PCs directly, it won't work. Both PCs will try to use the same send and receive wires. When you plug the two PCs into a hub, the hub electronically crosses the data wires, so one NIC sends and the other can receive. If you plug a second hub to the first hub using regular ports, you essentially cross the cross and create a straight connection again between the two PCs! That won't work. Luckily, nothing gets hurt (except your reputation if one of your colleagues notes your mistake!).

Because bridges work with MAC addresses, they operate at Layer 2, the Data Link layer of the OSI networking model.

SAP originally stood for Systems Applications and Products when the company formed in the early 1970s. Like IBM, SAP is now just referred to by the letters.



• **Figure 4.20** One conversation gets all the bandwidth.



• **Figure 4.21** Two conversations must share the bandwidth.

The classic difference between a hub and a switch is in the repeating of packets during *normal use*. Although it's true that switches *initially* forward all frames, in regular use they filter by MAC address. Hubs never learn and always forward all frames.

The Trouble with Hubs

In a classic 10BaseT network, the hub, being nothing more than a multiport repeater, sends all packets out on all ports. While this works well, when you get a busy network with multiple conversations taking place at the same time, you lose speed. The problem with hubs is that the total speed of the network—the bandwidth—is 10 Mbps. To appreciate the problem with hubs, take a look at the two computers sending data in Figure 4.20.

Since only one conversation is taking place, the connection speed between Computer A and Computer D runs at 10 Mbps. But what happens if Computer B and Computer C wish to talk at the same time? Well, CSMA/CD kicks in and each conversation runs at only ~5 Mbps (Figure 4.21).

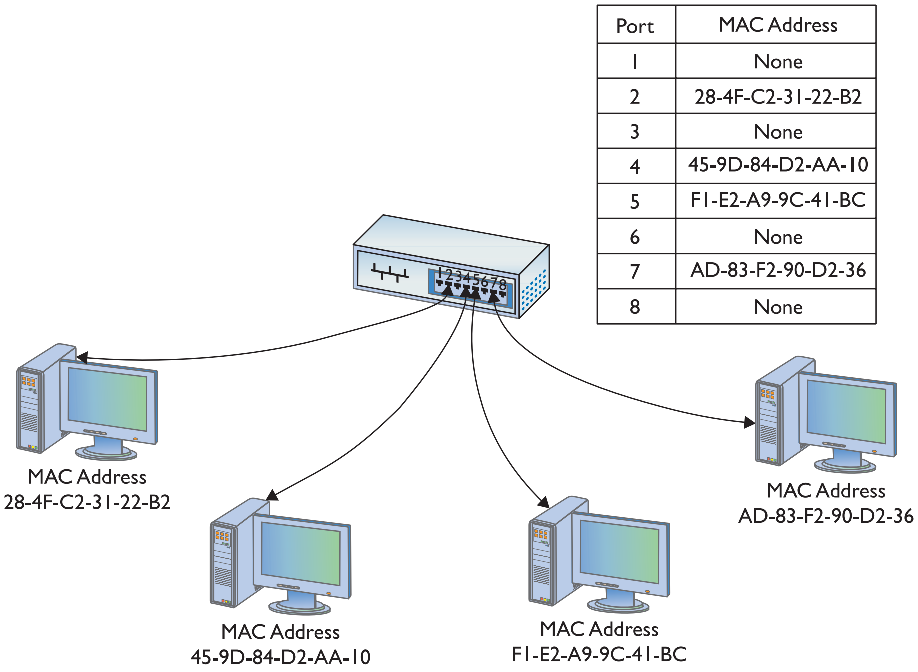
Imagine a network with 100 computers, all talking at the same time! The speed of each conversation would deteriorate to a few hundred thousand bits per second, way too slow to get work done.

Switches to the Rescue

An Ethernet **switch** looks and acts like a hub, but comes with extra smarts that enable it to take advantage of MAC addresses, creating point-to-point connections between two conversing computers. This effectively gives every conversation between two computers the full bandwidth of the network.

To see a switch in action, check out Figure 4.22. When you first turn on a switch, it acts exactly as though it were a hub, passing all incoming frames right back out to all the other ports. As it forwards all frames, however, the switch copies the source MAC addresses and quickly (usually in less than one second) creates an electronic table of the MAC addresses of each connected computer.

As soon as this table is created, the switch begins to do something amazing. The moment it detects two computers talking to each other, the switch starts to act like a telephone operator, creating an on-the-fly, hard-wired



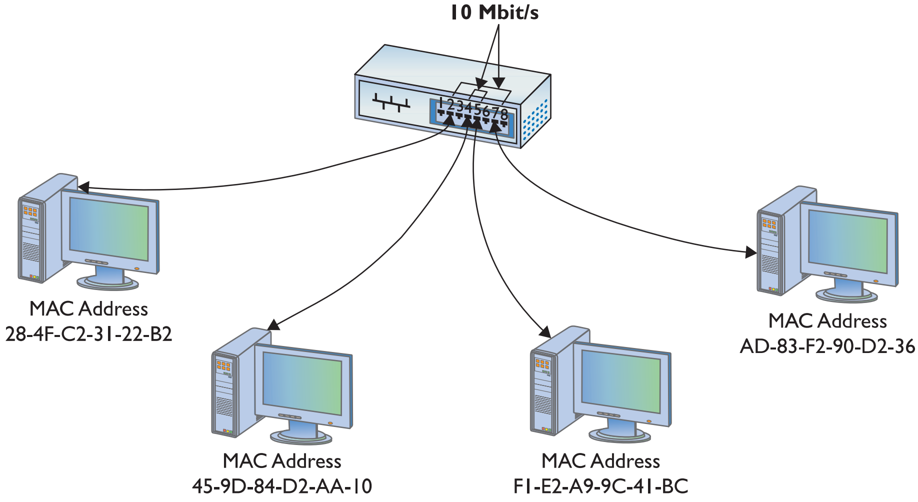
Port	MAC Address
1	None
2	28-4F-C2-31-22-B2
3	None
4	45-9D-84-D2-AA-10
5	F1-E2-A9-9C-41-BC
6	None
7	AD-83-F2-90-D2-36
8	None

• **Figure 4.22** A switch tracking MAC addresses

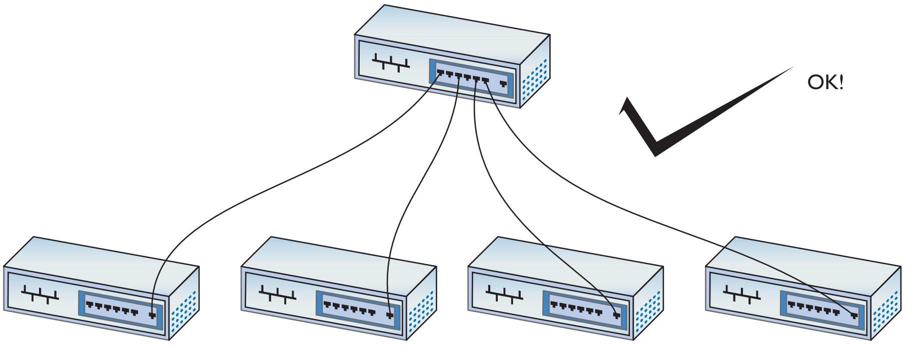
connection between the two devices. While these two devices communicate, it's as though they are the only two computers on the network. Figure 4.23 shows this in action. Since each conversation is on its own connection, each runs at 10 Mbps.

Speed isn't the only benefit switches bring to a 10BaseT network. When you use switches instead of hubs, the entire CSMA/CD game goes out the window. Forget about daisy-chain only! Feel free to connect your switches pretty much any way you wish (Figure 4.24).

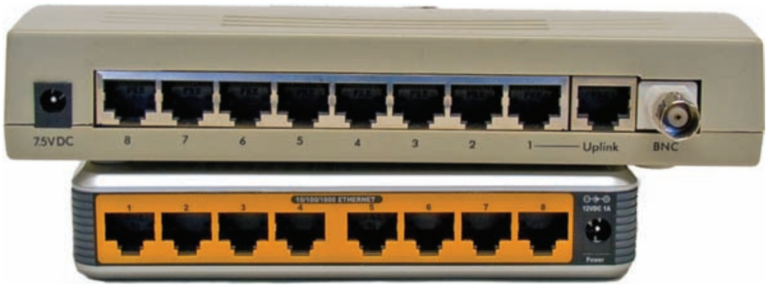
Because a switch filters traffic on MAC addresses (and MAC addresses run at Layer 2 of the OSI seven-layer model), they are often called *Layer 2 switches*.



• **Figure 4.23** A switch making two separate connections



• Figure 4.24 Switches are very commonly connected in a tree organization.



• Figure 4.25 Hub (top) and switch (bottom) comparison

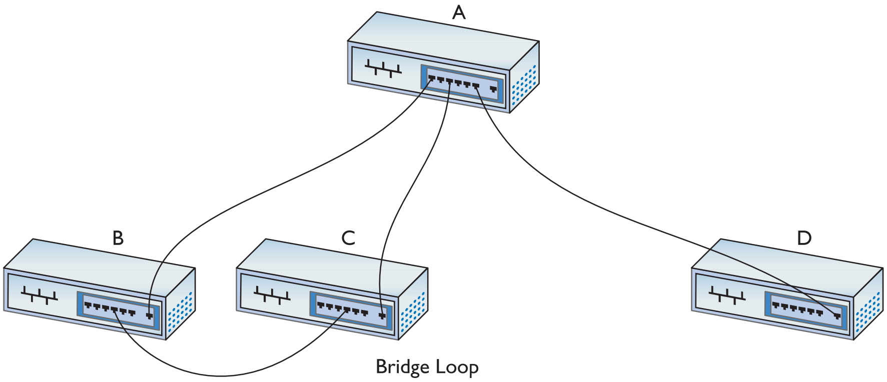
Physically, an Ethernet switch looks much like an Ethernet hub (Figure 4.25). Logically, because the switch creates a point-to-point connection between any two computers, eliminating CSMA/CD, the entire concept of collision domain disappears because there are no longer any collisions. Instead, the common term used today is **broadcast domain**, because all devices connected to a switch will hear a broadcast sent from any one system.

Spanning Tree Protocol

The ease of interconnecting switches makes them prone to a nefarious little problem called **bridge loops**. As its name implies, a bridge loop is nothing more than an interconnection of switches in such a fashion that they create a loop. In the network shown in Figure 4.26, for example, packets going between switches A, B, and C have multiple paths. This creates a problem.

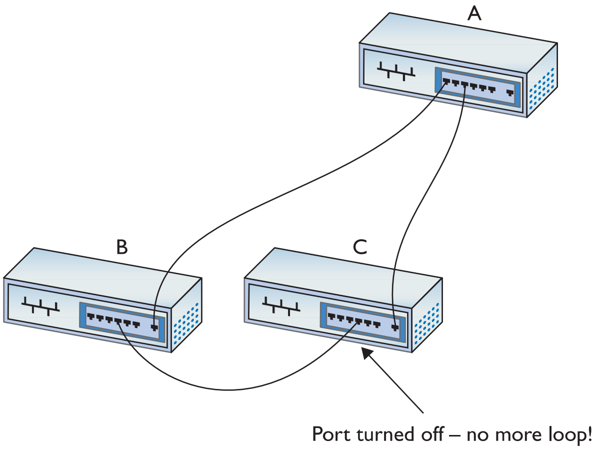
A bridge loop using the first generations of Ethernet switches was a very bad thing, creating a path sending packets in an endless loop and preventing the network from working. To stop this, the Ethernet standards body

Collisions (and CSMA/CD) can still take place on a switched Ethernet network, for example, if two devices tried to broadcast at the same time and collided. In these rare situations, switches still fall back to CSMA/CD.



• Figure 4.26 Bridge loops are bad!

adopted the **Spanning Tree Protocol (STP)**. STP adds a little more intelligence to switches that enables them to detect bridge loops. If detected, the switches communicate with each other and, without any outside interaction, turn off one port on the loop (Figure 4.27).



• **Figure 4.27** Port turned off, disaster averted

Chapter 4 Review

Chapter Summary

After reading this chapter and completing the exercises, you should understand the following about networking.

Define and describe Ethernet

- Ethernet is based on a family of network technologies from a bus topology. Ethernet enables computers to send data across a network, identify sending and receiving computers, and determine which computer should use the cable at which time. Early Ethernet networks originally used a single coax cable as a physical bus.
- The IEEE 802.3 committee controls the Ethernet standard.
- Ethernet networks use a hybrid star-bus topology with a hub at the center. Hubs repeat the incoming signal to every connected port.
- Ethernet frames prevent any single computer from monopolizing the cable, while making the retransmission of lost data efficient.
- Ethernet frames contain seven basic parts: the preamble, the MAC address of the destination computer, the MAC address of the sender, the length of data, the data itself, a pad, and a frame check sequence.
- CSMA/CD stands for carrier sense, multiple access/collision detection. Carrier sense means that the node checks the network cable before sending to see if anyone else is transmitting. Multiple access means all computers have equal access to the network cable. Collision detection is when nodes detect that a transmission did not complete.

Explain early Ethernet implementations

- Modern Ethernet networks use 10BaseT cabling. The physical topology of 10BaseT is a physical star; however, the data uses a logical bus topology with a central hub. So, 10BaseT actually uses a hybrid star-bus topology to accomplish moving data frames through the network.
- 10BaseT supports speeds up to 10 Mbps over baseband.
- 10BaseT requires the use of CAT 3 or higher, two-pair, unshielded twisted-pair cable. These cables utilize RJ-45 connectors, which are crimped to the cable.
- Correct crimping follows either the TIA/EIA 568A or the TIA/EIA 568B color-code standard.
- A good network technician knows the limits and specifications of 10BaseT, such as the maximum speed and distance, maximum nodes per hub, and supported cabling types.
- 10BaseFL is a fiber-optic version of 10BaseT that uses multimode fiber-optic cable and SC or ST connectors. One major advantage of 10BaseFL is its increased maximum distance between hub and node.

Describe ways to extend and enhance Ethernet networks

- Because hubs act as repeaters, hubs can be used to connect multiple segments together. Most hubs also have a crossover port, sometimes labeled uplink, crossover, MDI-X, OUT, or other another creative name.
- A crossover cable may be used to connect two hubs without an uplink port.
- A bridge filters and forwards traffic between Ethernet segments based on the MAC addresses of the computers on those segments. A bridge monitors and records the network traffic, eventually forwarding only the traffic that needs to go from one side of the bridge to the other. This helps reduce network bandwidth usage.
- Busy networks may suffer decreased bandwidth when using hubs. A switch solves this problem by creating a point-to-point connection, based on MAC addresses, between the sending and receiving nodes.
- Switches eliminate collision domains and instead create broadcast domains where all devices connected to a switch hear a broadcast sent from any other node.
- Connecting switches the wrong way can lead to bridge loops, which in turn can break the network. Switches that support the Spanning Tree Protocol are immune to bridge loops, even if wired in a physical loop.

Key Terms

10BaseFL *(67)*
10BaseT *(64)*
802.3 (Ethernet) *(59)*
bridge *(71)*
bridge loop *(74)*
broadcast domain *(74)*
collision domain *(63)*
crimper *(66)*
crossover cable *(70)*
CSMA/CD (carrier sense, multiple access/collision detection) *(62)*
Ethernet *(59)*
frame *(60)*
frame check sequence *(62)*
hub *(59)*
MAC address *(61)*
media converter *(68)*
node *(61)*
pad *(62)*
ports *(64)*
preamble *(61)*
promiscuous mode *(61)*
repeater *(59)*
RJ-45 connector *(66)*
segment *(60)*
sniffer *(61)*
Spanning Tree Protocol (STP) *(75)*
switch *(72)*
TIA/EIA 568A *(66)*
TIA/EIA 568B *(66)*
uplink port *(69)*

Key Term Quiz

Use the Key Terms list to complete the sentences that follow. Not all terms will be used.

1. The ________________ is unique to each individual NIC.
2. When extra "filler" data is needed in a packet, a(n) ________________ is added.
3. Another name for a packet is a(n) ____________.
4. A NIC that is listening for all packets sent along the wire is said to be in ________________.
5. The first item in a data packet is the __________.
6. A hub acts as a(n) ______________ in that it copies all incoming signals to every connected port.
7. Connecting switches incorrectly can create a(n) ______________, which can make the whole network stop working.
8. Hubs can be daisy-chained through their ____________, or the use of a(n) ____________.
9. ______________ has a maximum distance between node and hub of 100 meters while ______________ has a maximum distance of 2000 meters.
10. A(n) ______________ can be used to interconnect different Ethernet types.

Multiple-Choice Quiz

1. What is another term commonly used for frame?
   - **A.** Network
   - **B.** Packet
   - **C.** Pad
   - **D.** Segment
2. How are the connectors wired on a crossover cable?
   - **A.** One end is TIA/EIA 568A; the other end is TIA/EIA 568B.
   - **B.** Both ends are TIA/EIA 568A.
   - **C.** Both ends are TIA/EIA 568B.
   - **D.** One end is an RJ-45; the other end is an RG-6.

3. What items below make up the CSMA/CD system used in Ethernet networks? (Select three.)

   A. Collision avoidance

   B. Carrier sense

   C. Multiple access

   D. Collision detection

4. What happens when two computers transmit through a hub simultaneously?

   A. Nothing happens.

   B. The terminators prevent any transmission problems.

   C. Their signals are reflected back down the cable to their points of origin.

   D. A collision occurs.

5. What is a group of nodes that hear each other's traffic?

   A. Collision domain

   B. Ethernet

   C. Fast Ethernet

   D. Sneakernet

6. Which committee is responsible for Ethernet standards?

   A. IEEE 803.2

   B. IEEE 803.3

   C. IEEE 802.2

   D. IEEE 802.3

7. What type of cabling do modern Ethernet networks use?

   A. 10Base2

   B. 10Base5

   C. 10BaseT

   D. 10Base-Cat5

8. What is the purpose of a preamble in an Ethernet frame?

   A. It gives the receiving NIC time to realize a frame is coming and to know when the frame starts.

   B. It provides the receiving NIC with the sending NIC's MAC address so communication can continue.

   C. It provides error-checking to ensure data integrity.

   D. It contains a description of the data that is to follow so the receiving NIC knows how to reassemble it.

9. What is a valuable network tool that can be used to examine all frames on the network, regardless of their intended recipient?

   A. Repeater

   B. Media converter

   C. STP

   D. Sniffer

10. For what purpose is a crimping tool used?

   A. To splice a 10BaseT cable with a 10BaseFL cable.

   B. To attach an RJ-45 connector to a UTP cable.

   C. To attach a 10BaseT cable to a media converter.

   D. To connect two hubs together.

11. Which of the following is not a limitation on 10BaseT cable?

   A. Maximum speed of 10 Mbps

   B. Maximum distance between hub and node of 100 feet

   C. Maximum of 1024 nodes per hub

   D. Minimum CAT 3 or better UTP with RJ-45 connectors

12. Which of the following is not a limitation on 10BaseFL cable?

   A. Maximum speed of 10 Mbps

   B. Maximum distance between hub and node of 2000 meters

   C. Maximum of 1024 nodes per hub

   D. Minimum CAT 3 or better UTP with RJ-45 connectors

13. Upon looking at the front of a hub, you notice something labeled as MDI-X. What is this for?

   A. It is a special receptacle for the power cable.

   B. It is a regular port used to connect computers.

C. It is an uplink port used to connect the hub to another hub.

D. It is the brand name of the hub.

14. Which statement best describes the main difference between hubs and switches?

A. A hub repeats signals whereas a switch amplifies them.

B. A hub repeats incoming signals to all connected ports whereas a switch only repeats an incoming signal to the destination port.

C. Hubs use 10BaseT but switches use 10BaseFL.

D. Hubs can be daisy-chained but switches cannot.

15. What feature of switches prevents the problem of bridge loops?

A. STP

B. TCP/IP

C. IEEE 802.3

D. UTP

Essay Quiz

1. Describe two ways that using frames helps move data along a network.
2. Define the term *CSMA/CD*, using simple descriptions to explain each of the three parts: CS, MA, and CD.
3. Describe what a hub does and some of its limitations. Then explain how a switch works to overcome the problems of a hub.

Lab Projects

• Lab Project 4.1

On a blank sheet of paper, use one side to list the basic facts you must know about 10BaseT for the CompTIA Network+ certification exam. Use the other side to list the essential facts you must know about 10BaseFL. Double-check your work, either by yourself or with a classmate, to ensure its accuracy. Save this sheet to use as a quick-reference study aid when you're preparing to sit for your exam—it will help!

• Lab Project 4.2

In this chapter you learned about the basic functionality of switches. Use the Internet to delve deeper and research the difference between a managed switch, an unmanaged switch, and a smart switch. Create a chart to compare the similarities and differences between them. In addition to the differences in features and functionality, research and report on the pricing differences for similarly sized switches. For example, what is more expensive, a 24-port managed, unmanaged, or smart switch? What do you get for the extra money? Is it worth it?

• Lab Project 4.3

Use the Internet to research freeware or shareware programs that will "sniff" the data on your network. With your instructor's permission, download a program that you find, and then install it on your classroom lab network. Try to sniff data going to and from your machine, as well as other traffic. Have fun, and document your findings.