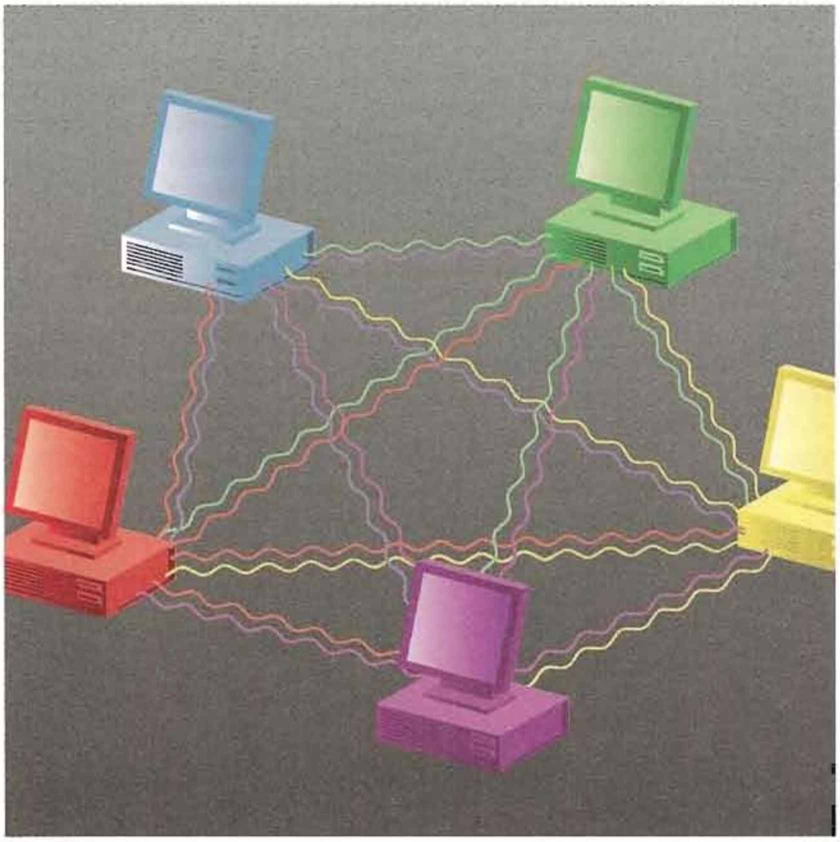
CHAPTER 24

How Local Area Networks Work



A **local area network (LAN)** is, for many people, the entry point to the Internet. A LAN physically links several PCs to each other and often to a server that hosts shared data or provides access to the Internet. This is accomplished with a variety of materials—twisted-wire cables, fiber optics, phone lines, and even infrared light and radio signals.

Whatever the technology, the goal is the same—to send data from one place to another. Usually, the data is in the form of a message from one computer to another. The message might be a query for data, the reply to another PC's data request, an instruction to run a program that's stored on the network, or a message to be forwarded to the Internet.

If the data or program for which the message asks isn't on the Internet, it might be stored on a PC used by a co-worker on the network, or on a **file server**, which is a specialized computer. A file server is usually a high-performance PC with multiple large hard drives that are not used exclusively by any individual on the network. Instead, it exists only to serve all the other PCs using the network—called **clients**—by providing a common place to store data that can be retrieved as rapidly as possible by the clients. Similarly, a network might include an Internet server that links the LAN to the Net, CD-ROM jukebox servers, or print servers that everyone on the LAN can use for printing. A **print server** is a PC connected to a printer, or a network printer that can be connected to a network without an intervening PC.

If a network does not have a dedicated server, it is a **peer-to-peer network**. In a peer-to-peer network, each individual's PC acts as a server to other PCs—its peers—on the network and also is a client to all its peers acting as servers.

The network must receive requests for access to it from individual PCs, or **nodes**, linked to the network, and the network must have a way of handling simultaneous requests for its services. When a PC has the services of the network, the network needs a way of sending a message from one PC to another so that only the node for which it's intended recognizes it, and it doesn't pop up on some other unsuspecting PC. And the network must do all this as quickly as possible while spreading its services as evenly as possible among all the nodes on the LAN. LANs are a microcosm of the Internet, even as the LANs are a part of the Internet.

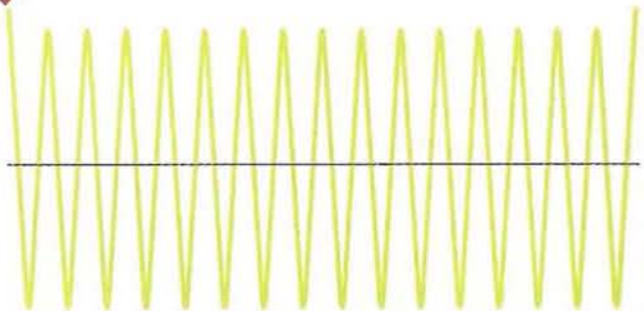
In this chapter, we'll look at the most common types of networks, including the notorious file-sharing networks and the works of the most common LAN configuration, Ethernet.

How Packets Divvy Up Data

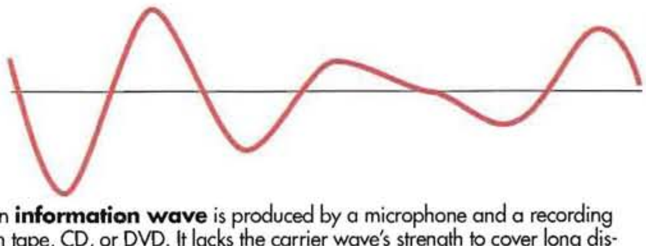
Sending information digitally isn't all that new. Samuel Morse sent the first telegraphed message in the U.S.—"A patient waiter is no loser."—in 1838. He used a binary system—dots and dashes—to represent letters in the alphabet. Before Morse, smoke signals did much the same thing, using small and large puffs of smoke from fires. But for a good chunk of the 20^{th} century, analog signals in telephones, radio, recordings, and TV became the standard ways to send data over great distances. With networking and the Internet, however, digital communications are once more in vogue, even replacing analog signals used in television, radio, and telephone. What makes this all possible is something called a **packet**.

How Analog Data Works

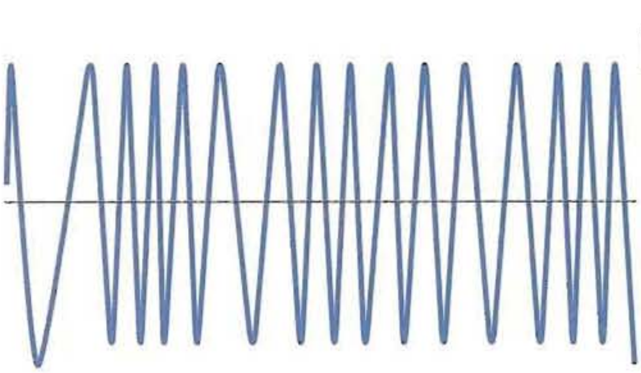
1 Analog communication works with two types of waves.



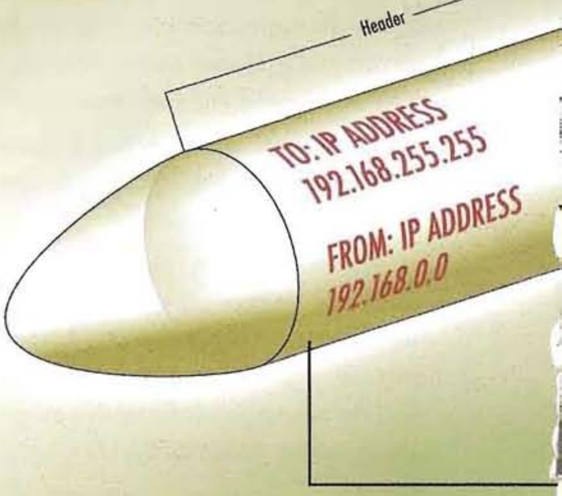
A **carrier wave**, or **carrier signal**, is a steady, strong wave that carries no information of its own. It is usually sinusoid, which means it has a constant waveform, both for **amplitude** (its loudness) and **frequency** (how many times it cycles from its high point to low point and back again in a second). An FM radio station broadcasting at 104.5 "on the dial!" is broadcasting a carrier that cycles 104.5 million times a second.



An **information wave** is produced by a microphone and a recording on tape, CD, or DVD. It lacks the carrier wave's strength to cover long distances. And unlike the carrier signal, it is irregular, changing form constantly due to the processes that produce it.



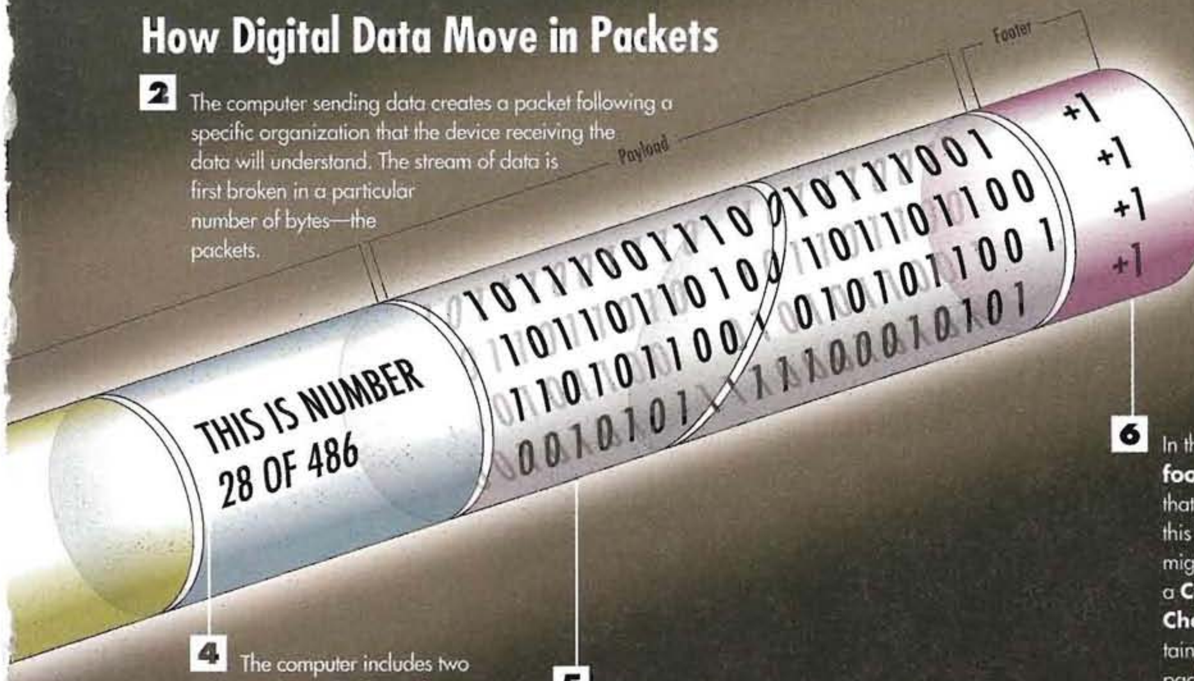
2 When the information wave is superimposed on the carrier, the information wave **modulates** the carrier (modulate simply means to change something). The informational signal could vary the amplitude or the frequency of the carrier. Speech is an example of a modulation. Vowels are the carrier that let you project your words far enough and clearly enough for others to hear you. Consonants are the information signals that transform the "ee" vowel into "me," "we," "see," and other variations on the basic "ee" sound. When the modulate signal is received (by a radio, TV, amplifier, or human ear), the receiver strips away the known values of the carrier signal. What is left is the original information signal.



1 For digital data transfers, it's convenient to think of the **packet** as the equivalent of a carrier signal. A packet itself has no information, but it encloses, metaphorically at least, the real information traveling to another computer or to a component within the same computer. But there are more advantages in packets than simple bundling. Packets permit addressing, error correction, and the use of multiple pathways to get the information from one spot to another. The organization of data packets varies to match the type of data they contain, and they may be called **frames**, **segments**, or **blocks,** depending on their data. We'll look at the most common packet you'd encounter—the Internet packet.

How Digital Data Move in Packets

2 The computer sending data creates a packet following a specific organization that the device receiving the data will understand. The stream of data is first broken in a particular number of bytes—the packets.



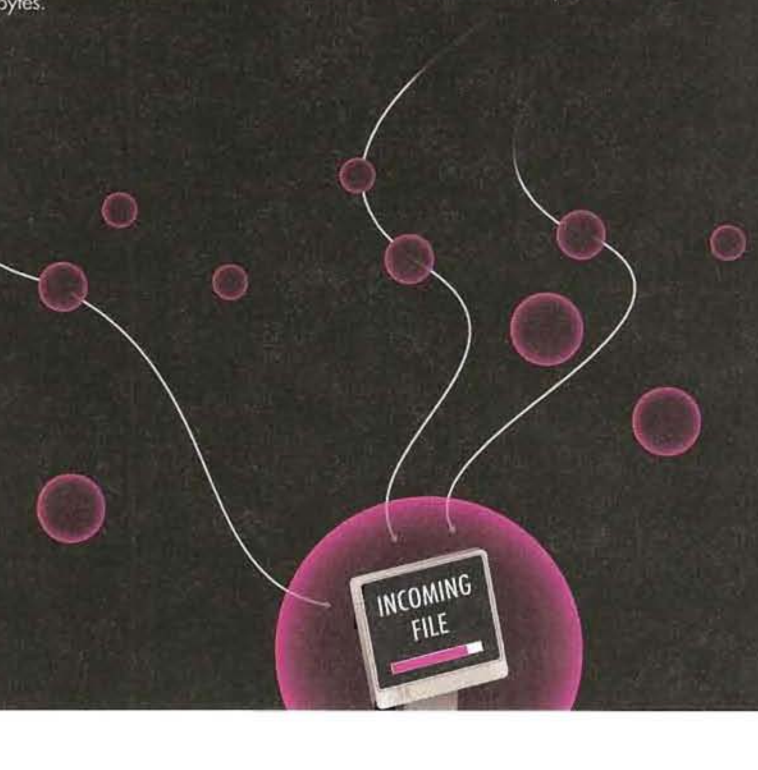
4 The computer includes two numbers. The first is the number of packets the information is divided into. The second is the sequence number of this particular packet.

5 The computer follows the form for bundling the actual data—the **payload**—set out by the **Transmission Control Protocol/Internet Protocol (TCP/IP).** Each packet holds 1,000–1,500 bytes.

6 In the packet's **trailer** or **footer**, there are a few bits that tell the receiving computer this is the end of the packet. It might also include the results of a **Cyclic Redundancy Check (CRC)**. The CRC contains the sum of all the 1s in the packet. The receiving computer does the same calculation, and if the results don't match, the receiver asks the sender to retransmit the packet.

3 To each packet's **header**, the computer adds the **IP address** that the packet is supposed to go to and the sender's IP address.

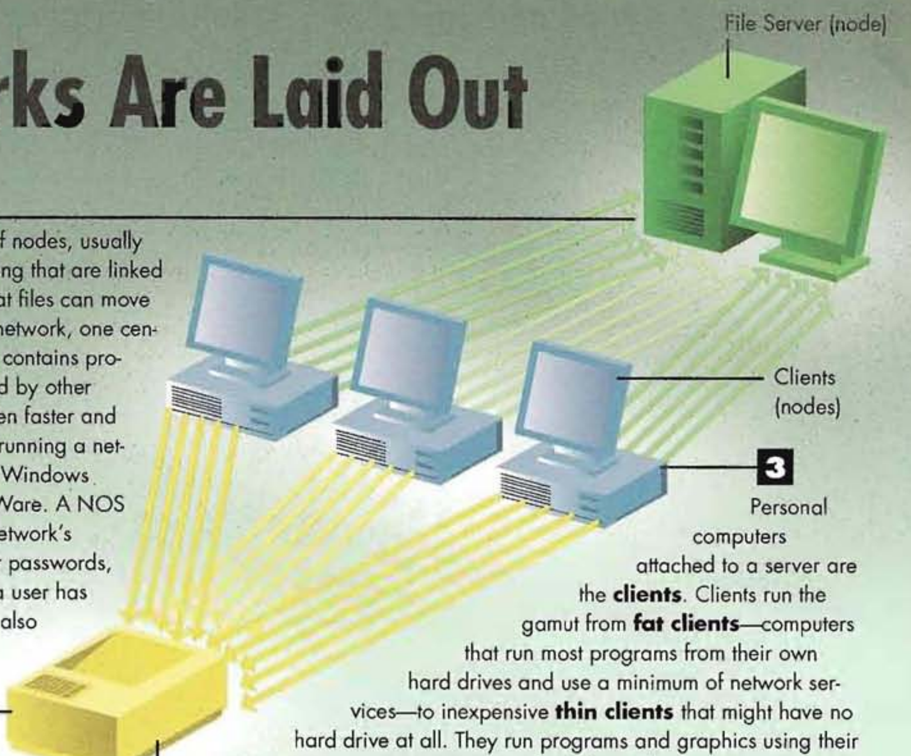
7 The computer sends each packet into the Internet separately, and each packet takes the best route available at the time it shoves off. This method allows the network to spread the traffic out more evenly, and in the event of serious traffic jam, not all the packets are stuck in the same place. As the packets arrive, they may not be in the correct order. The receiving computer puts them into a buffer and, using their sequence numbers, builds the entire message as the packets arrive.



How Networks Are Laid Out

Client/Server Networks

1 A local area network (LAN) is made up of nodes, usually two or more computers in the same building that are linked together with wires or radio signals so that files can move among the computers. In a client/server network, one central computer is the file server. The server contains programs and data files that can be accessed by other computers in the network. Servers are often faster and more powerful than personal computers, running a network operating system, or NOS, such as Windows Server 2003, Unix, Linux, or Novell NetWare. A NOS manages the movement of files and the network's security by maintaining lists of users, their passwords, and the drives and directories for which a user has been given access privileges. A server is also called a host computer.

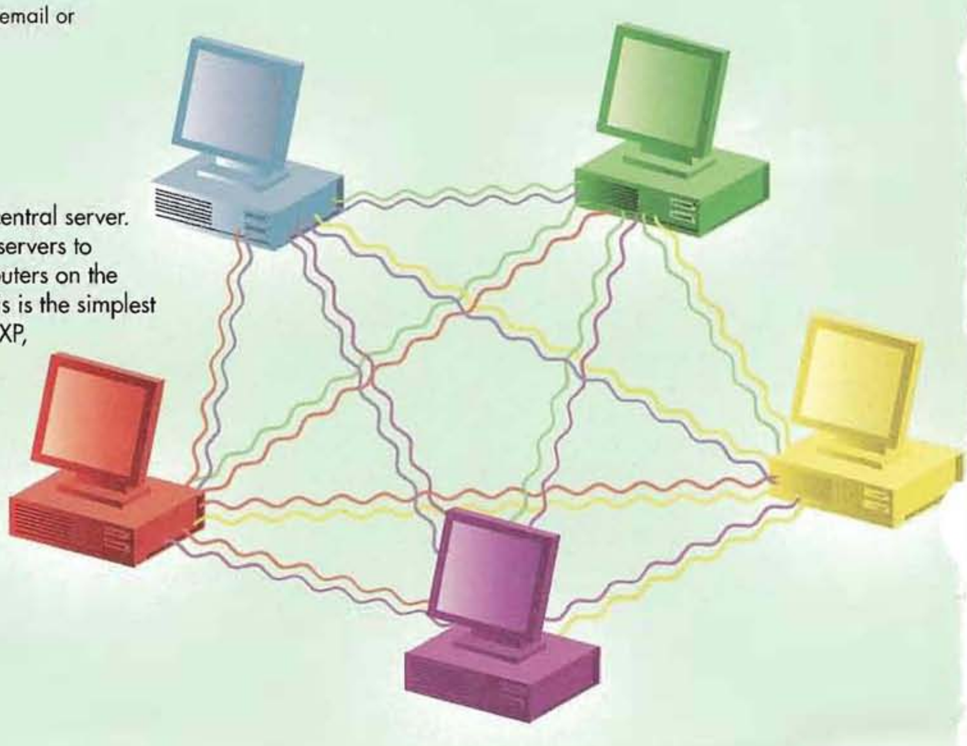


2 Some servers specialize in functions other than passing out files. A print server lets everyone on a network share a printer. The printer can be attached to a computer on the network; some printers designed for network use can be connected directly to the network without a host PC. Other specialized servers provide shared access to the Internet, banks of CD-ROM drives, and tape backup. Some servers specialize in running programs that are designed for network-wide use, such as an email or database server.

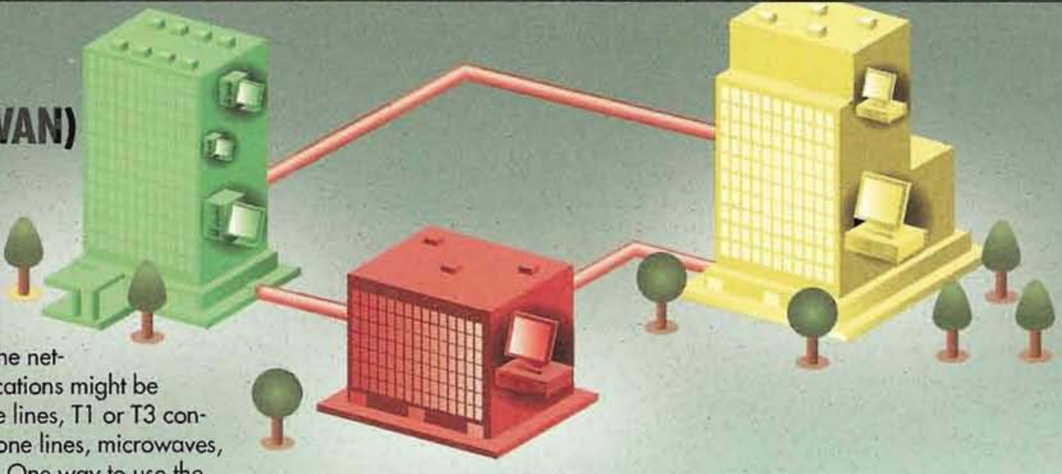
3 Personal computers attached to a server are the **clients**. Clients run the gamut from **fat clients**—computers that run most programs from their own hard drives and use a minimum of network services—to inexpensive **thin clients** that might have no hard drive at all. They run programs and graphics using their own microprocessor, but depend entirely on a server to access programs and store data files. A **dumb terminal** is a monitor, keyboard, and the bare minimum of hardware needed to connect them to the network. It uses the server's microprocessor to perform all functions.

Peer-to-Peer Networks

In a **peer-to-peer network**, there is no central server. Instead, all computers on the network act as servers to every other node. At the same time, all computers on the network act as clients to all the other PCs. This is the simplest type of network to install. Windows 98, Me, XP, and Vista come with the software to set up a peer-to-peer network.



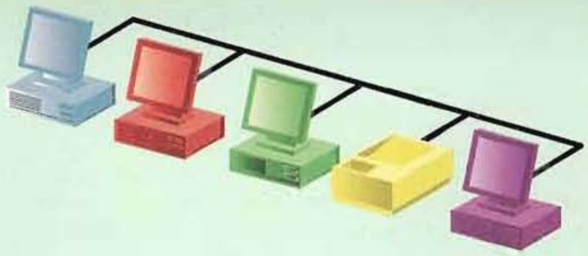
Wide-Area Network (WAN)



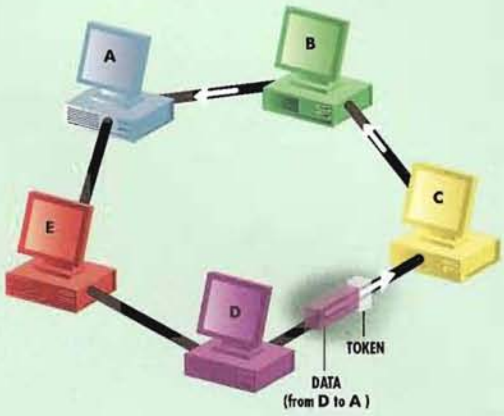
When components of a network are spread among several buildings, it becomes a **wide-area network**. Chunks of the network in different locations might be connected by phone lines, T1 or T3 connections, leased phone lines, microwaves, or the Internet itself. One way to use the Internet for a WAN is through a **virtual network**, software that uses heavy encryption to maintain privacy among Internet-connected PCs so that they work and fend off hackers as if the scattered nodes were at the ends of Ethernet cables in the next room.

The Shapes of LANs

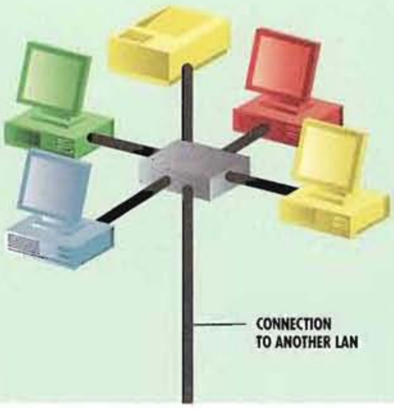
The way that data moves from one node to others in a LAN determines the network's **topology**—its shape.



Bus topology All the nodes in a LAN are connected along a single cable—the bus—stretching from one node to the next. It is inexpensive and simple to set up, but a bad connection at one of the nodes also takes other nodes off the network.



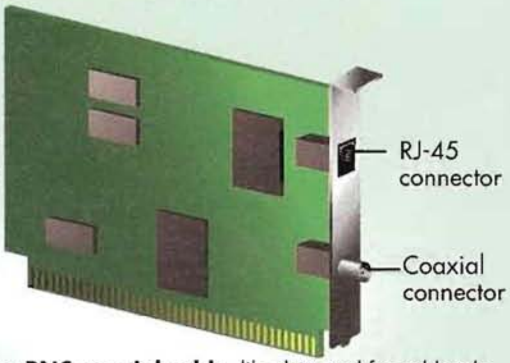
Token ring All the nodes are connected to a giant ring of cable that has no real beginning or end. Data travels from one node to another by one node grabbing a **token** of code that endlessly loops through the network. The node replaces the token on the ring with the node's data and the address of the node for which it's intended. The message circles through the ring until another node recognizes that the data is addressed to it.



Star topology The most common shape for a LAN is the star. Several nodes are linked to the network by a cable, radio signals, optic fiber, and so on. They lead to a common point at the center of the star, where there's a hub, switch, or router (which are explained in the next illustration). Data from a node travels to the center of the star, where the device located there passes the data along to the node to which the data's addressed. Star configurations are often used to connect two LANs.

How Network Nodes Connect

To become part of a network, a personal computer uses a **network interface card (NIC) or an RJ-45 connector that's part of the motherboard.** (For portable computers, the interface can be in the form of a PC Card or USB adapter.) Communications signals pass from the PC's RAM and through the connection to a LAN's **backbone**, the part of the network that carries the most traffic. The backbone and connections leading to and from it might use **coaxial** cable, **fiber-optic** cable, **twisted-pair** cable, **radio waves**, and phone and power wiring to link PCs. The combination of connector, circuitry, wiring, and other hardware determines the network's bandwidth.



Coaxial Cable

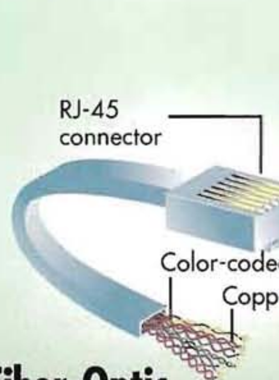
From the connector, data can be sent along **BNC coaxial cable**, like that used for cable television. (*BNC* stands for *Bayonet Neill-Concelman*, a fact you will not be quizzed on.) Coaxial consists of a single copper wire, which is sheathed by plastic and braided copper that shields the center wire from electrical disturbances. Each end of a segment of cable has a **bayonet connector**, which requires only a quarter of a turn to attach the cable.

Twisted-Pair Wiring

A more common alternative to coaxial is twisted-pair wiring. A plastic outer jacket encloses four pairs of insulated wire that are twisted with a different number of turns per inch. The twists cancel out electrical **noise** from adjacent pairs of wires and from motors and other electrical devices in the same building.

Each end of the cable terminates in a plastic **RJ-45** connector, which resembles the common RJ-11 phone plug. (*RJ* stands for *registered jack*.)

Each node on the network has a separate twisted-pair cable that connects the node to a central **hub**, **router**, or **switch**, which is the center of a star configuration. All of these devices let the signals from any one computer travel to any other node on the network. Any of the connections can be broken without affecting other nodes.

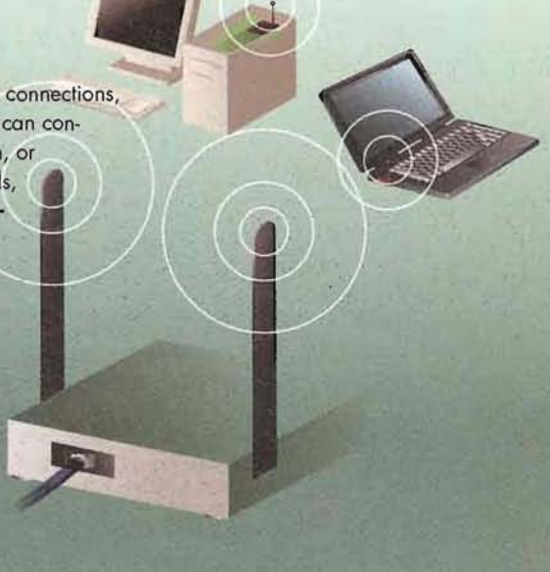


Fiber-Optic

On networks connecting directly to the Internet or in LANs for which speed is crucial, **fiber-optic** cable carries 1 billion bits a second, enough to carry tens of thousands of telephone calls. Hair-thin fibers consist of two layers of pure silica glass covered with a reflective **cladding**, like a tunnel lined with mirrors. Varying pulses of light from a laser or LED carry the data along the twists and turns of the cable by bouncing off the cladding.

Wireless

Instead of using cable connections, nodes on the network can connect to the hub, switch, or router via radio signals, such as those that **Wi-Fi** systems use (see Chapter 29). In fact, all of the connection methods described here can be used together on the same LAN.



The Ethernet Packet

An Ethernet network sends data from one node to another in **packets** (see, "How Packets Divvy Up Data," **p. 316**). **Switches** and **routers** use the information to determine where to forward the packet. In a network joined by **hubs**, the nodes themselves check the address data to determine which packets to pay attention to and which to ignore.

- **Preamble**—Synchronizes the network nodes.
- **Destination Address**—A single PC or all PCs on a network.
- **Source Address**—The address of the computer from which the packet originated.
- **Type**—Defines the format used for the data.
- **Data**—The actual information.
- **CRC**—Cyclical Redundancy Check, which is used to spot transmission errors.

Hubs, Routers, and Switches

In a star configuration, a network uses hubs, switches, and/or routers as traffic cops to move data to the right destination and to ward off intruders from the Internet. Each of these devices is a simple box with several plugs to accept RJ-45 or fiber-optic cables.

Hubs

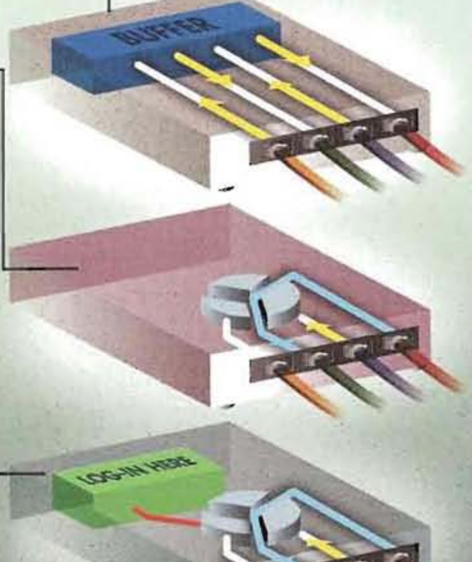
1. A hub receives incoming data packets from different nodes and temporarily places them in a memory buffer if the hub is busy with another packet.

2. Each packet the hub receives is sent to every other node regardless of the packet's addressing. Nodes ignore any packets that are not addressed to them.

Switches

1. A switch functions similarly to a hub, but a switch knows which of its connections lead to specific nodes. The switch reads a packet's addressing information and transmits the packet out only on the line that leads to the node it's addressed to.

2. Some packets—for example, one announcing that another computer has come online—arrive addressed for **broadcast**. This means the sending node wants all other nodes to see the packet. The switch sends copies of the packet.



Routers

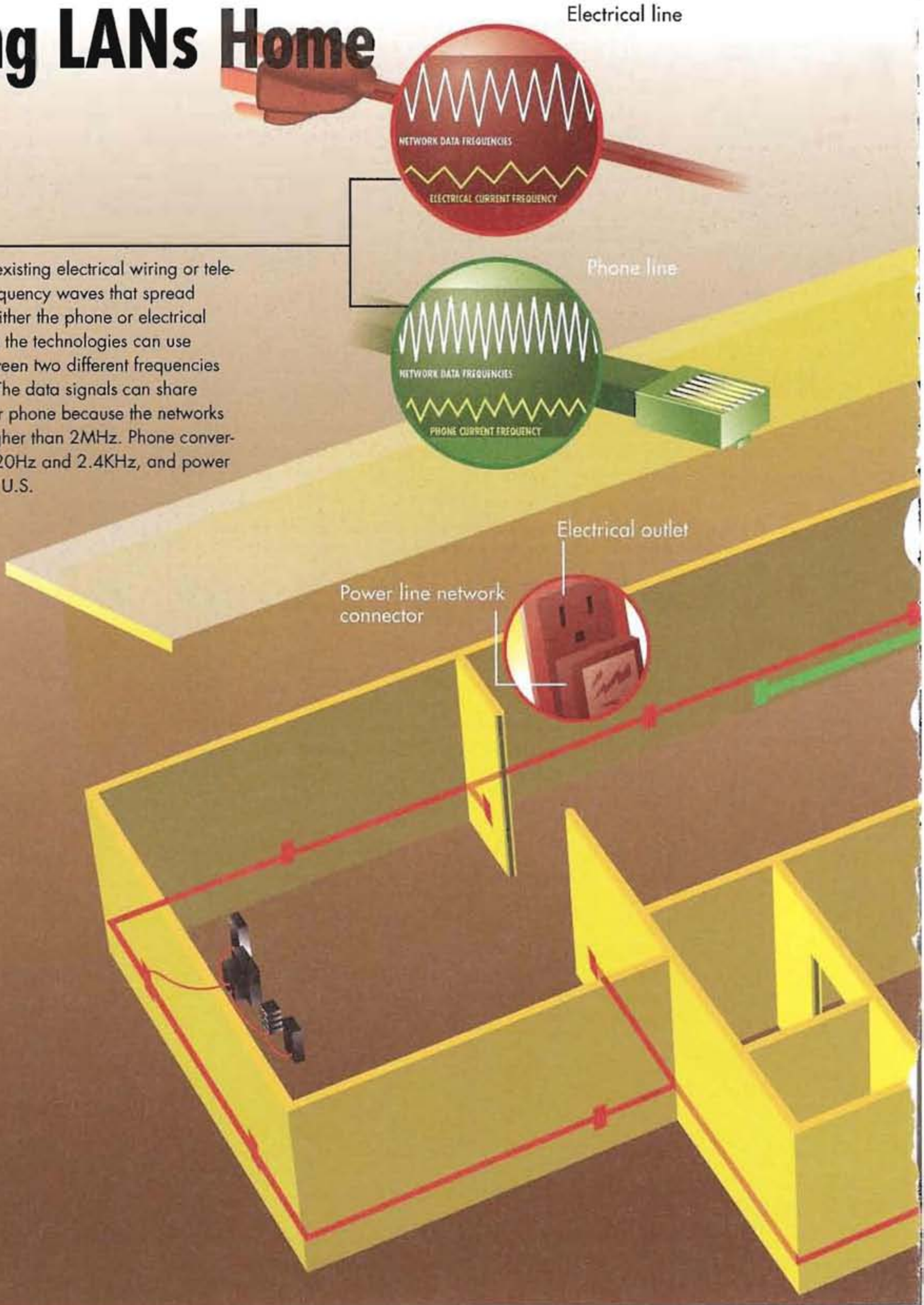
1. A router is similar to a switch, except that a router does not accept or transmit broadcast packets. A router requires a specific delivery address for a node located on the LAN. (But most routers also have switch capability.)

2. Routers provide connections to the Internet at the same time they protect the LAN from the Internet. The rules might, for example, require the router to block any LAN packet that has a destination address outside the LAN and somewhere in the Internet.

3. If the packet comes from the Internet and is headed toward a node on the LAN, the router can send the signal to a log-in routine or reject it entirely.

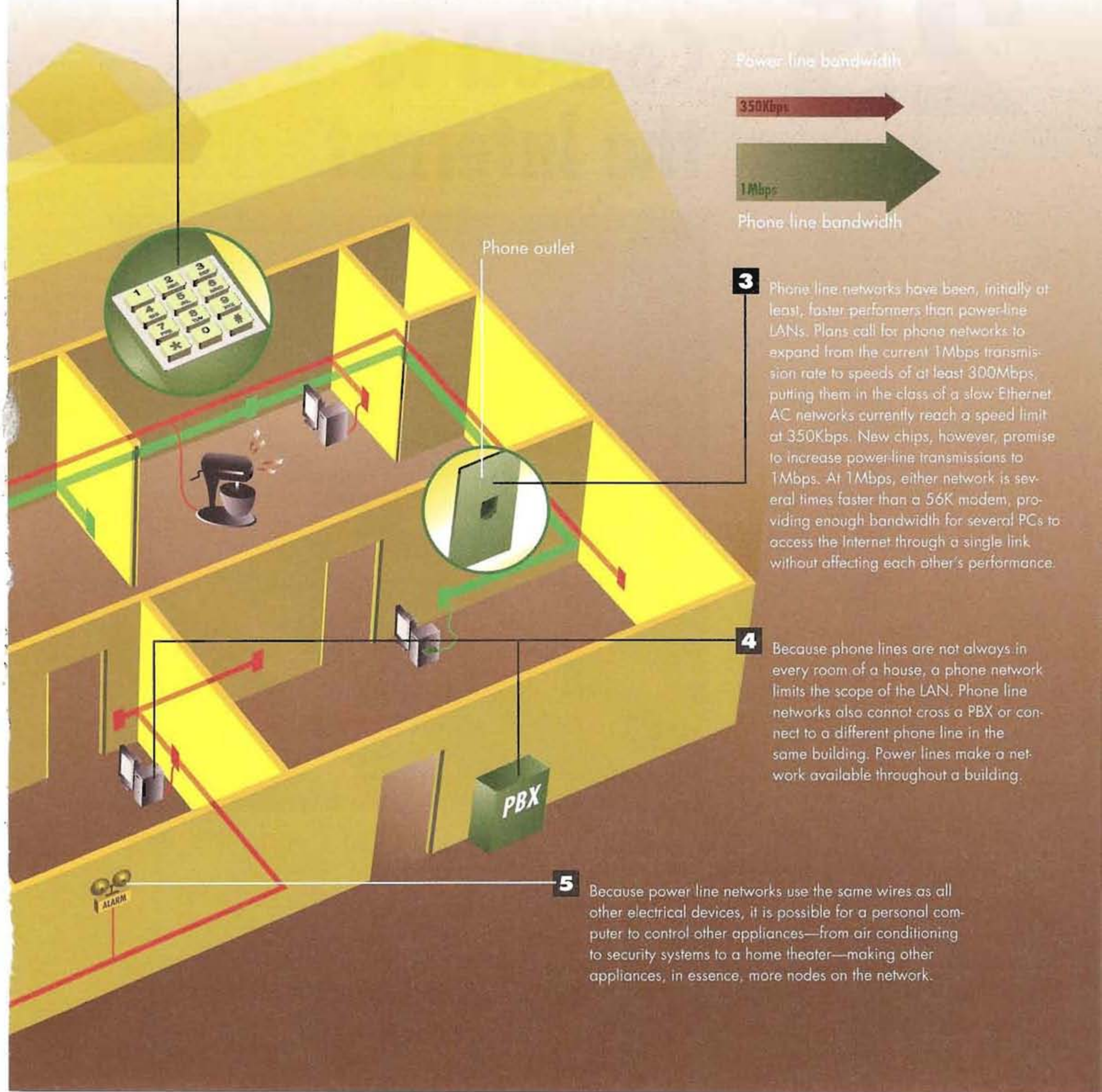
4. If the destination address is valid—say, for an email server on the LAN—the router lets the packet into the network. Before sending the data to its destination, some routers check the packet's CRC segment for errors that have occurred en route. If a packet has an error, the router discards it and sends a message to the origination address, requesting a fresh packet of the same data.

How Phone and Power Lines Bring LANs Home



1. Networks that work over existing electrical wiring or telephone wires use radio frequency waves that spread through all the wiring in either the phone or electrical systems. The variations on the technologies can use on/off pulses or shift between two different frequencies to represent bits of data. The data signals can share wires used for electrical or phone because the networks operate at frequencies higher than 2MHz. Phone conversations operate between 20Hz and 2.4KHz, and power lines cycle at 60Hz in the U.S.

2 Because other uses of the lines dramatically affect their electrical characteristics, both networks must adapt instantly to changes in current or voltage. By avoiding the frequencies involved in electrical current and phone signals, electrical noise does not contaminate data on the lines. Phone conversations, fax transmissions, and use of appliances plugged into power lines continue normally without affecting or being affected by the network transmissions.



3 Phone line networks have been, initially at least, faster performers than power-line LANs. Plans call for phone networks to expand from the current 1Mbps transmission rate to speeds of at least 300Mbps, putting them in the class of a slow Ethernet. AC networks currently reach a speed limit at 350Kbps. New chips, however, promise to increase power-line transmissions to 1Mbps. At 1Mbps, either network is several times faster than a 56K modem, providing enough bandwidth for several PCs to access the Internet through a single link without affecting each other's performance.

4 Because phone lines are not always in every room of a house, a phone network limits the scope of the LAN. Phone line networks also cannot cross a PBX or connect to a different phone line in the same building. Power lines make a network available throughout a building.

5 Because power line networks use the same wires as all other electrical devices, it is possible for a personal computer to control other appliances—from air conditioning to security systems to a home theater—making other appliances, in essence, more nodes on the network.