Excerpt from

The Basics of Networking

By

Michael Milone, Ph.D.

Revised by

Rose Hrizuk

Preview

The following is a sample excerpt from a study unit converted into the Adobe Acrobat format. A sample online exam is available for this excerpt.

The sample text, which is from the PC Specialist program, describes one of the most popular methods of linking computers together: a local area network (LAN).

In 1981, when IBM introduced its first PC, the general opinion was that PCs would be operated as stand-alone units in homes or as supplemental processors to mainframes and minicomputers in businesses. By the mid 1980s, however, it became clear that PCs were much more capable than people first thought. Companies and individuals began wanting to link PCs together to share data and resources. Today, *connectivity*, or the linking of computers, is well established. Network hardware and software development are growing faster than any other area of computing.

After reading through the following material, feel free to take the sample exam based on this excerpt.

Contents

EXAMINATION

The Basics of Networking

OVERVIEW

The Advent of the Network

With the advent of the IBM personal computer (PC) in 1981, many employees were provided with their own computers to run their own software applications and manage their own data. They no longer had to depend on the centrally controlled mainframe and mini-computers, run and maintained by a separate department, usually called *management information services (MIS)*. One of the disadvantages to this newfound independence was the inability to share information and expensive peripheral devices, such as printers, with other PC users. Individuals began looking for ways to link their personal computers together to share data and hardware resources. Today, computer networking is a popular computing specialty, and the network hardware and software development are growing faster than any other area of computing.

Building a network is challenging. However, since you'll probably find that many of the personal computers you'll work on are connected to networks, you'll need to thoroughly understand this aspect of computing.

What Is a Network?

A *network* is a system of linked computers and computer peripherals. The purpose of a network is to allow users to share data and program files and other resources such as disk drives and printers (Figure 1).

In general, most networks will have the following characteristics:

- Connections to a number of computers and peripheral devices
- Connections made through some type of cables
- Shared data and resources
- Individual computers in the network that perform some processing functions
- Computers managed by one or more individuals using specialized software
- A common *protocol*, or set of rules, that's used to share data

FIGURE 1—A local area network is a system of linked computers that shares files and other resources such as disk drives and printers.
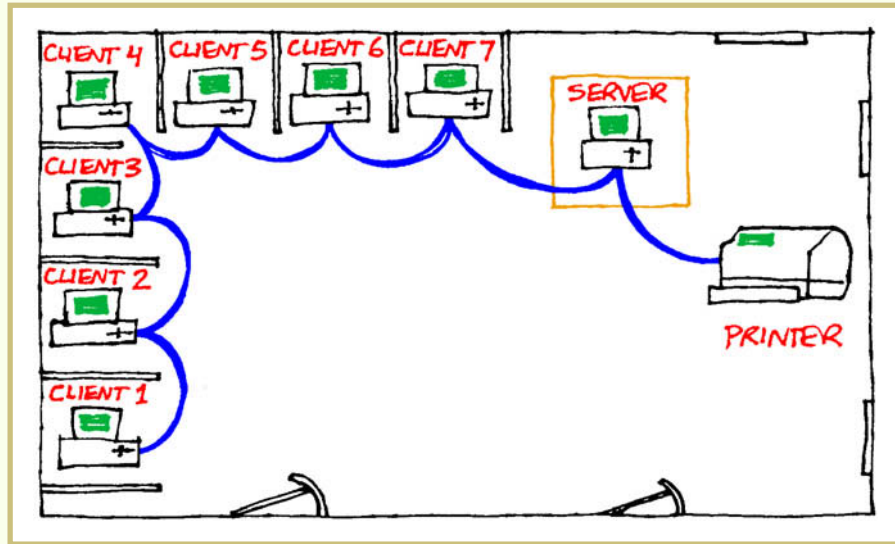
Network Types

There are many different varieties of networks. Some consist of a few computers located in the same room that share data files and the same printer. Others consist of thousands of computers spread out over many cities or even countries. These large networks share hundreds and possibly thousands of printers, exchange electronic mail (E-mail), support video conferencing, and may be protected by sophisticated security systems.

Networks typically grow as the size of the organization and its need to share information grow. Let's take a look at five of the most common types of networks: local area networks, interconnected networks, enterprise networks, metropolitan area networks, and wide area networks.

A *local area network* is a small network usually located within a single building or group of buildings of one organization. (We'll give you a more detailed description of a LAN later in this study unit.)

An *interconnected network* or *internetwork* is formed when two or more LANs are connected to form an organization-wide system. For example, departmental LANs that are connected together would be an interconnected network. Large networks are usually split into smaller LAN segments to improve performance and management.

An *enterprise network* ties all the computers within an organization together, no matter which operating system they use. It may connect a LAN to a mainframe computer, or it may connect several LANs that use different network operating systems (NOS)—along with Unix servers or workstations, a minicomputer, and PCs with various operating systems.

Metropolitan area networks and wide area networks typically provide connections to distant networks and other communication resources. A *metropolitan area network (MAN)* is a high-speed network that connects LANs in a specific area such as an industrial park or city. A *wide area network (WAN)* provides countrywide or global connections via telephone lines and satellite. Large companies that have regional or worldwide offices use WANs to connect their networks. A very good example of a WAN is the Internet, which connects many networks worldwide.

Network Benefits

From the material you've read so far in this study unit, you've probably been able to anticipate some of the advantages that networks provide to their users. Let's look at some of the major benefits of these systems.

One of the most important benefits of a network is that it allows individual users to share printers and other peripherals. Sharing these devices eliminates the need for mechanical switches to allow printer sharing, allows users to redirect output to a chosen device, and allows users to share expensive devices that they might not have access to in a stand-alone environment.

In a network, users aren't limited to the data on their individual PCs. Instead they can access, or share, data on other network computers. The ability to share data allows multiple users to access database files at the same time, to access common documents and forms used in the organization, to share files, and to collaborate on documents.

In addition to peripherals and data, network users can also share applications software. Here's how it works. One copy of the software is installed on a PC, called a *server*. When a user needs the particular software, he or she can simply access it from the server.

Sharing applications software has several advantages. For example, sharing applications helps to reduce the amount of time needed for software maintenance and installation, and also reduces the costs involved. Sharing applications also establishes a standardized software setup and prevents users from modifying software configurations. This saves time and money spent on support and maintenance. Finally, sharing applications prevents the illegal copying of software, because a software metering application tracks the number of users that open and close particular applications.

Another advantage is that networks can provide substantial communications benefits, such as electronic mail, scheduling, and access to remote host (mini or mainframe) computers. It can also provide access to larger networks like the Internet.

Finally, networks provide varying levels of security to their users. For example, all networks require users to input a login ID and a password before they can access the information on the network. Additionally, networks may limit the time of day at which users can access the network and the workstations from which users can access the network. They may also provide access limitations to certain files and even certain devices (disk drives) on the network. A stand-alone workstation provides virtually no security.

Note that in order to obtain maximum security benefits, the data on a network should be backed up on a regular schedule. In addition, backup data should be stored off-site, and a detailed disaster recovery plan should be implemented.

NETWORK HARDWARE COMPONENTS

A computer network consists of both hardware and software components. A network's *hardware components* usually include a server (unless the network is a peer-to-peer network), workstations, network interface cards, and a cable system. The *software components* of a network include the operating system that manages the network, device drivers, code that's used to tell the operating systems how to use specific peripheral devices, network client software, and applications software. The *network client software* is used to tell the workstations how to utilize the network as if they were an extension of that operating system. *Applications software* includes programs that are used for word processing, creating spreadsheets, managing databases, producing graphics, and so on. In this section of your study unit, we'll concentrate on the hardware components.

Servers

A *server* is a computer that's attached to a network for a specific purpose. It runs the network operating system and offers network services to users at their individual workstations. These services include file storage, user management, security, network commands, applications software storage, printing services, and other communication services. Network servers contain higher speed processors, larger hard drives, and more memory as compared to desktop personal computers. A server may also be a specialized computer such as a Sun Microsystems Netra Server or even a minicomputer such as an IBM AS/400. Typically, a LAN server is a high-end PC or specialized PC built to be a server, such as the Hewlett-Packard NetServer.

Workstations

A *workstation* is a computer that's attached to a network and operated by individual users. Workstations don't function as servers. Instead, the workstations (sometimes called *clients*) use the services that are offered by the server, such as file storage and printing services. The types of computers that are used as workstations vary depending on user needs and on the network's operating system and applications software. A workstation may be an MS-DOS-based PC, an Apple Macintosh, a Unix-based system, an OS/2-based system, or a PC running Microsoft Windows 3.x, Windows 95/98, or Windows NT.

Network Interface Cards

A *network interface card* is a specialized adapter card that fits into one of the bus slots on a computer's motherboard. Each computer attached to a network, whether it's a server or a workstation, requires an NIC (Figure 2). An NIC is an extension of the computer's bus and is used along with the cable system for communication between the server and network clients or between one network client and another.

The NIC contains some RAM that serves as a communications buffer, customized chips that are used to exchange data between computers, and other network circuitry. It also contains the connector that's used to join the cable to the client system.

FIGURE 2—Each computer in a LAN has a network interface card to communicate with other computers in the system.

ADAPTER CARD   CABLING
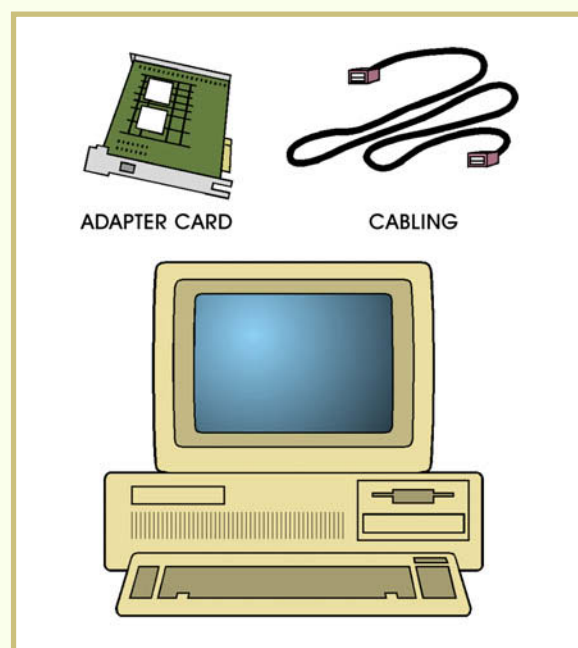
The two most popular types of NICs are Ethernet and token ring. Each of these comes with a different price tag and supports a different access method (networking scheme) and a different communication speed.

The type of NIC you select is based on the type of cable you decide to run. Ethernet NICs may support thick Ethernet cable, thin Ethernet (coaxial) cable, and unshielded twisted-pair (UTP) cable. Token ring NICs support shielded twisted-pair (STP) cable and UTP cable. We'll discuss cable types in the next section of the study unit.

Cable Systems

The *cable system* is the physical transmission medium that ties the various components of a network together. That is, the cable system provides the physical connections between the workstations and the server. The cables, however, are often the part of a network that receives the least amount of attention—and the least amount of money—during installation and maintenance.

Cable Types

Three major types of cable are used in LANs: twisted-pair cable, coaxial cable, and fiber-optic cable (Figure 3). Each type has specific properties that relate to their data-handling capacities, their immunities to electrical interference, the distances over which the data can travel, and installation costs.

Twisted-pair cable is the type that's used most often in LANs. It may be either *shielded twisted pair (STP)* cable or *unshielded twisted pair (UTP)* cable. Shielded cable offers more protection against electrical interference but is more expensive than UTP. UTP cable is one of the most popular types of cable, partly because it's commonly used in telephone installations and many buildings have an excess of it already installed. In some office environments, telephone wiring is run to centralized communications closets where telephone equipment is installed. These closets are ideal places to locate hubs or concentrators for a network. A *hub* or *concentrator* is a central location where cables that are connected to workstations can be attached.

UTP cable consists of at least two conductor wires that are twisted together and housed in a plastic sheathing. The number of twists per foot is standard in the United States and is used to offset electrical power interference. STP cable is essentially the same as UTP cable, except that the wire twists may be wrapped in an aluminum-backed plastic sheathing or a braided metal shield. The shields are grounded to drain off electrical interference. UTP cable should be used in situations where electromagnetic interference is low, because electromagnetic interference can disrupt the data signals.

COMPUTER CABLES			
	Twisted-Pair Cable	**Coaxial Cable**	**Fiber-Optic Cable**
Data Capacity	Medium to High	Medium to High	High
Distance Supported	Low	Medium	High
Interference Immunity	Low	Medium	High
Cost	Low to Medium	Medium to High	Medium to High

FIGURE 3—*The most popular means of linking computers in a LAN are twisted-pair, coaxial, and fiber-optic cables.*

Coaxial cable consists of shielding, a single conductor wrapped by insulation, and a second woven wire all contained in a plastic sheathing. This type of cable is used in cable TV lines. Coaxial cable is more expensive than twisted-pair cable, but it's capable of carrying data faster and farther.

Fiber-optic cable (also called *optical-fiber cable*) is even more popular for networks than coaxial or twisted-pair cable because of its ability to carry hundreds of times more information at faster speeds over longer distances. Fiber-optic cable is also immune to electrical interference, which means that it has a much lower data error rate at higher speeds. Fiber-optic cable consists of a thin strand of optical fiber protected by an inner layer of insulation called *cladding* and an outer layer of insulation called *sheathing*. Although the price of fiber-optic cable is dropping, a job using fiber-optic cable may cost as much as 30 percent more than a twisted-pair job.

Choosing Cable for a Network

Several factors must be considered in choosing a cable type. The first is the *bandwidth* of the cable, or the frequency with which data can be transmitted over the cable in a specific amount of time. Bandwidth is measured in *hertz* (cycles per second) or *bps* (bits per second). The higher the bandwidth of the cable, the higher the frequency and the amount of data that can be transmitted through the cable. Another factor to be considered is the environment in which the cable is to be installed. If the environment is electrically noisy (for example, if the workplace contains fluorescent lights, large motors, welding equipment, air compressors, or other industrial equipment), it will affect the type of cable you choose. Yet another factor is the distance from the workstation to the central wiring closet, or concentrator (hub).

The choice of cable affects the topology (physical layout) of a LAN, the types of network interface cards used, and other electronic components needed. Thus, when you're considering the design of a network, you should consider the amount of bandwidth you'll need in the future, not just the amount you need now.

The following are several factors to consider when you're choosing cable for a network:

- The physical layout of the workstations you're trying to network (the floor plan)

- The amount of electromagnetic interference (EMI) or radio frequency interference (RFI) that the network environment contains

- The number of workstations that will be connected to the network

- The distances between workstations and servers (the lengths of cable needed to make connections to and from the network)

If you're installing a network today, the chances are good that it will be Ethernet. The two types of Ethernet networks are 10-BaseT and 100-BaseT. The difference between these two types is the speed. The 10-BaseT network operates at 10 megabits per second, while the 100-BaseT network operates at 100 megabits per second. Network installations can be 10-BaseT, 100-BaseT, or even a combination of the two different speeds. However, a combination arrangement will require special hubs and switches to handle the different speeds.

The installation and maintenance costs for a token ring network are considerably higher than for an Ethernet network. Because there's no major advantage to justify the additional cost of the token ring network, this type isn't widely used today.

It's very important to design the cable layout of a network carefully. A cable plan that's improperly designed and installed will greatly increase the cost of maintaining a network because of the added time and expense for additions, changes, and moves. It's also harder and more time-consuming to troubleshoot cable-related problems in a system that lacks consistency and the proper documentation. When many different types of wire and connectors are used in a network, the inconsistency makes it difficult to maintain that system.

Wireless LANs

A *wireless LAN* is one that doesn't require cable. There are three types of wireless LANs: *infrared*, *single radio frequency*, and *spread spectrum radio frequency*. These types of transmission media are often just temporary solutions until permanent wired systems can be implemented, or they may be used where cable installation is impossible.

Backup Systems

A *backup system* is used to preserve data and applications that are critical to an organization's business in case the server's disk storage device fails. A backup system is composed of both software and hardware. LAN backup software is used to store both data and applications on another media, such as a tape or an optical disk, for archival purposes. Backup hardware consists of a tape drive and optical disk drives.

Some examples of tape drives are *digital audiotape (DAT)*, *4 mm*, *quarter-inch cartridge (QIC)*, and *8 mm*. Digital audiotape and 4 mm use CD-quality, digital recording technology with magnetic tape. Quarter-inch cartridge is a backup system that uses $\frac{1}{4}$-inch wide magnetic tape cartridges. 8 mm is used for backups in high-capacity tape drives. Some examples of optical disk drives are the *write once read many (WORM)* and *CD-recordable (CD-R).* The WORM system is an optical disk that can be recorded only once. The CD-R system is a recordable CD-ROM that can be written to only once.

Usually, a full server backup is performed when the server is first brought on-line (before any data is stored in it). After that, backups are performed at regular intervals (usually once a month, or whenever new applications software is installed). Data backups should be performed every day. Both server backups and data backups are the responsibility of the system administrator.

Another important network component that's related to the backup system is the uninterruptable power supply. An *uninterruptable power supply (UPS)* is used to provide battery backup power to a server when the power from the normal electrical system is lost. A sudden power interruption may not only shut down the server and make it inaccessible; it may also corrupt data and damage the server hardware. An uninterruptable power supply usually has a certain life in minutes or hours that's relative to the power requirements of the server. This amount of time should be sufficient to allow the system administrator to shut down the server in an orderly fashion if power is going to be out for an extended period of time. The UPS may have software that's run on the server to monitor the amount of time left until the power in the UPS battery is too low to support the power required by the server. A UPS may also protect a server from power fluctuations that can be harmful to the server's electronic components.

There are a host of other add-on components above and beyond those needed to set up a basic network. These can be added as the need arises. To keep up with the hardware and software offerings available and to stay abreast with new network technology, you can subscribe to trade newspapers, magazines, and journals.

ALTERNATIVE NETWORKS

LANs aren't the only way that computers can be linked together. Familiarity with the alternatives not only gives you a better understanding of LANs but also presents you with methods that may be employed in place of a LAN. Although a LAN may be the perfect solution to one person's problems, it may not benefit another person who really doesn't need what a LAN can offer. The important thing is to analyze the situation and then match the user's needs with the computing solution that's most appropriate. Let's examine some of these alternatives.

Manual Information Exchange

The most basic way to transfer information from one computer to another is through the process of *manual information exchange*. In this process, a user simply saves a file on a floppy disk, inserts the floppy disk into another computer, and retrieves the file into the second computer. Manual information exchange is sometimes jokingly referred to as *FootNet* or *SneakerNet*, since the user has to "walk" the disk from one computer to another (Figure 4). As primitive as this method sounds, it works almost flawlessly, it's inexpensive, and it meets the needs of a surprising number of users.

FIGURE 4—The easiest way to transfer information from one computer to another is through manual information exchange, sometimes called "FootNet" or "SneakerNet." Although it's not a very sophisticated method, it's still ideal in certain situations.

Naturally, manually exchanging disks between computers works best with computers that are compatible. However, several software programs are available that permit files to be exchanged between previously incompatible computers. For example, Apple File Exchange (a utility distributed by Apple Computers) allows a Macintosh to read and write files for both Apple and DOS-based (IBM-compatible) computers. This utility is ideal for transferring ASCII files from one computer to another. There's also a utility program called MAC-in-DOS that allows a DOS-based computer to read from and write to a Macintosh disk. On the hardware side, there are computers with the capability of accessing both DOS and Macintosh files. The Power PC is one such computer.

In some situations, a manual information exchange is ideal. For example, suppose you want to take a document file home to work on from your own PC. Saving the file to disk and carrying the disk home is probably the simplest way to transport the needed information. After you make the modifications at home, you can save the document to the same disk and carry it back to the office PC. The disk allows you to transport the file with the least amount of inconvenience.

File Transfer Programs

A step above FootNet is a *file transfer program* like LapLink from Traveling Software. This program comes with a special cable that allows a DOS-based computer to be connected through its serial port to another DOS-based computer or with a Macintosh. Part of the software is a set of translators that allows files created in one format to be transferred to the other computer in another format. For example, a WordPerfect file created on a PC can be converted to a Microsoft Word format and then transferred to a Macintosh. Because data is transferred through the serial port, the transmission speed is relatively slow as compared to the speed in a LAN (Figure 5).

The two computers involved in a file transfer program must be physically close together, since they must be connected by a cable. Perhaps the best use of a file transfer program is to transfer files from an office computer to a laptop computer that's being taken off-site. A salesperson leaving the office for a week on the road could use this technology to transfer the database of products and prices as well as client information to a laptop. Upon returning, the salesperson can transfer the file containing the orders to a PC in the office for processing.

Most major software vendors recognize that FootNet and file transfer programs are extremely popular, so they include a number of different formatting options in their programs. The best-selling spreadsheets, word processors, and databases give users the option of saving files in a number of formats. Other software developers have created translation programs that convert files from one format to another before they're exchanged. Soon, users will be able to change even the most complex documents from one format to another.

FIGURE 5—Specialized software allows files to be transferred from one computer to another through their serial ports.
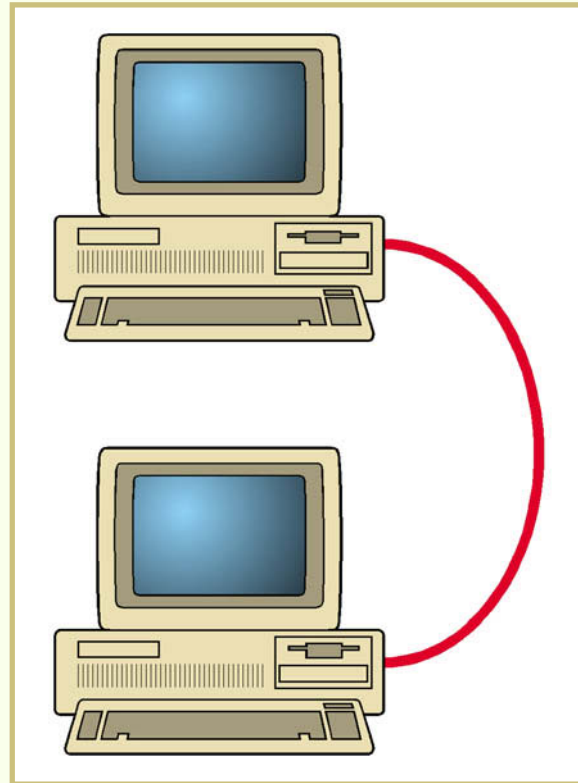
The format option is important because each software package saves files in a unique, proprietary format that often isn't readable to a different software package. For example, WordPerfect document files are saved in a particular way. If you try to access those files from another word processing package, you'll probably see strange symbols on the screen; and the text (if you see it) will be formatted incorrectly —with words running together and odd-looking characters interspersed throughout.

Many older versions of full-featured software allowed you to save in ASCII format. Saving in ASCII tended to remove most of the codes (such as double spacing, justification, italics, and so on), but retained the text in readable form. Then, you could retrieve the text into another word processing package intact.

Newer versions of full-featured software allow you to select several options when you save a document. For example, you can create a document in WordPerfect and save it in the proper format for Word, WordStar, AmiPro, or any of several other popular word processing packages. Then, you can use that word processing software to retrieve the document. This is very helpful when the computer you're using to open a file doesn't use the same software as the computer on which the file was created.

Printer Switch Boxes

Resources such as printers and hard disk drives can also be shared without using a network. Special cables, switch boxes, and other hardware solutions can be used to solve simple resource-sharing problems. For example, one popular printer-sharing system consists of hardware and software that allows up to six computers to share the same printer. Inexpensive switches can also be used to connect two, three, or four computers to one printer (Figure 6). Note that in this type of arrangement, the hardware must be within the physical reach of the switch so that cables can be connected to it.

Another type of printer-sharing system uses phone wire to connect devices. In these systems, the equipment can be located in different rooms as long as the phone wire can be run between them to make the necessary physical connections.
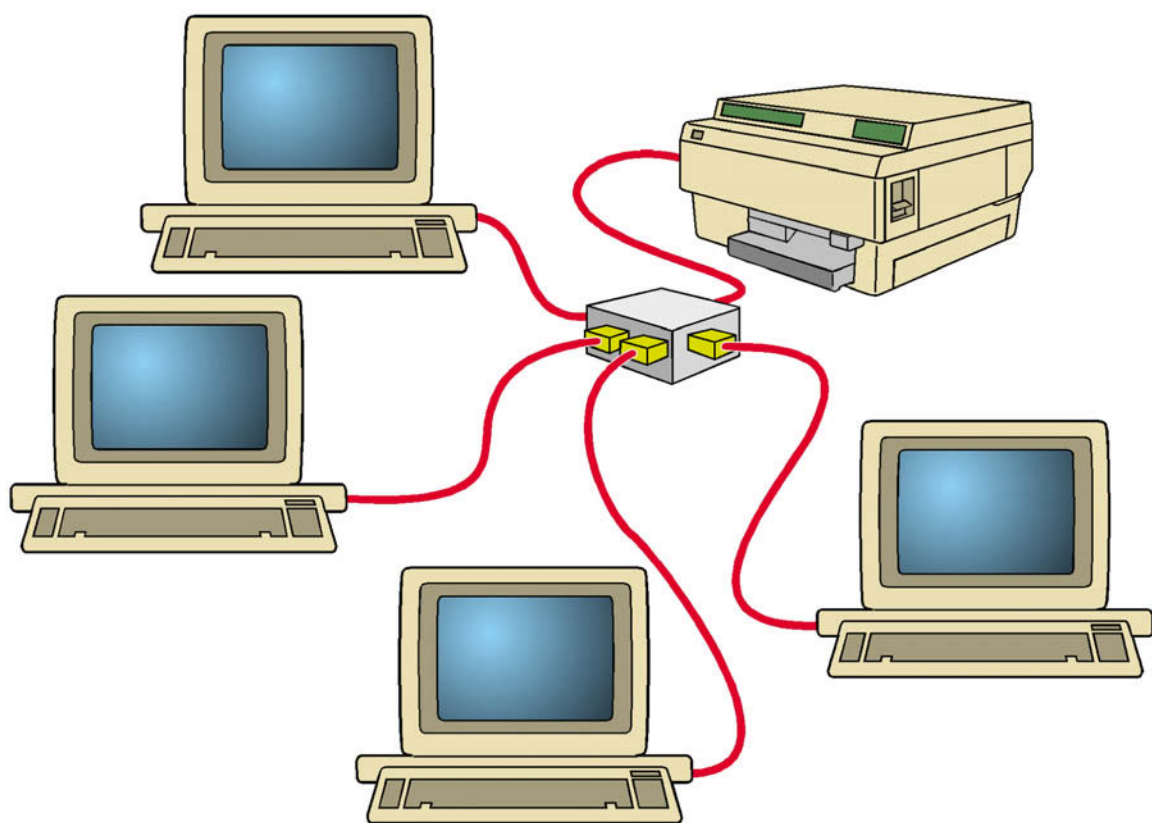

FIGURE 6—Special switches and cables allow users to connect several computers to one printer.

Multiuser Systems

A *multiuser system,* as its name implies, provides several users with computing resources that they can access at the same time, usually through a central processor and dumb terminals. A *dumb terminal* is a computer terminal that can display data, but not process data.

The central processor may be a minicomputer, a powerful PC, or even a dedicated "cabinet" unit that has computer capabilities (but lacks a keyboard or monitor). Multiuser systems are similar to LANs in many respects, but differ from them in the following ways:

- Multiuser systems generally support fewer users than LANs.

- Multiuser systems perform most processing functions at the central computer, rather than at the terminals.

- Multiuser systems are somewhat cheaper to install because the terminals are dumb rather than full-featured PCs.

- Multiuser systems are less easily expanded to service a large number of users.

- Multiuser systems are less likely to support hardware or software from multiple vendors.

- Multiuser systems are more likely to be supported by a vendor-affiliated technician than a general computer technician.

LANs and multiuser systems are becoming more and more alike. Most of the advantages of multiuser systems are duplicated by LANs. As the price of hardware comes down, the cost of full-featured PCs is approaching that of dumb terminals. The distinction between LANs and dedicated multiuser systems will blur in the coming years, just as the distinction between minicomputers and high-end PCs is now blurred. A few years from now, perhaps the only significant difference between a LAN and a multiuser system will be the name that a vendor chooses to assign to a product.

You've just gotten a taste of what LANs are all about and how they operate. The study unit this excerpt is based on continues with a description of network topologies— that is, the different physical layouts of computer networks.