CHAPTER
EIGHTEEN

LOCAL AREA NETWORKS

Synergy means behavior of whole systems unpredicted by the behavior of their parts.

—Richard Buckminster Fuller

Chapter Highlights

As control systems become more complex, they require more effective communication schemes between the system components. Some machine and process control systems require that programmable controllers be interconnected, so that data can be passed among them easily to accomplish the control task. Other systems require a plantwide communication system that centralizes functions, such as data acquisition, system monitoring, maintenance diagnostics, and management production reporting, thus providing maximum efficiency and productivity. This chapter presents one type of PLC communication scheme—the local area network—and the role it plays in achieving factory integration. The next chapter will discuss I/O bus networks, a type of communication scheme in which I/O field devices are connected directly to a network.

18-1 History of Local Area Networks

The proliferation of electronic and computer technologies in the 1970s made it feasible to place small personal computers at locations where users needed them. Before this, computational tasks had been performed by large computers in centralized locations. The widespread use of personal computers prompted the need for a communication method that could link this equipment. This led to the creation of **local area networks (LANs)**. These networks facilitated the decentralization of computing tasks by allowing network-connected computers to exchange information among themselves, without having to go through a central location.

Local area networks soon made their way to the industrial arena, where control had previously been exercised through a central PLC or main control system. LANs allowed many PLCs to be placed at different locations, each having its own intelligence to implement control. They also allowed PLCs to communicate system information with other PLCs performing other control tasks throughout the plant. This wave of industrial technology created further networking developments, including a special type of network—the I/O bus network—which allows intelligent field devices to communicate information to PLCs without standard PLC input/output interfaces. The next chapter explains I/O bus networks in detail.

18-2 Principles of Local Area Networks

Definition

A local area network is a high-speed, medium-distance communication system. For most LANs, the maximum distance between two nodes in the network is at least one mile, and the transmission speed ranges from 1 to 20 megabaud. Also, most local networks support at least 100 stations, or nodes. A special type of local area network, the industrial network, is one which meets the following criteria:

- capable of supporting real-time control
- high data integrity (error detection)
- high noise immunity
- high reliability in harsh environments
- suitable for large installations

Two other common types of local area networks are business system networks (e.g., Ethernet) and parallel-bus networks (e.g., Cluster/One). Business networks do not require as much noise immunity as industrial networks, since they are used in office environments. They also have less stringent access time requirements. The user of a business work station can wait a few seconds for information without problem, but a machine being controlled by a PLC may require information within milliseconds to operate correctly. Parallel-bus networks have requirements similar to business networks and are intended for microcomputers and minicomputers used in office environments over short distances.

Different types of networks have different allowable distances between connected devices. Figure 18-1 illustrates the distances at which different types of networks and buses can be used. Note that long-distance communication still relies on public networks, such as telephone systems, which have long-range data-channeling capabilities. However, developments in cable TV data transmission are enabling data exchange of information via TV cables at distances of up to 200 miles. Figure 18-2 illustrates a cable TV network, developed by LANcity (Cable Modem Division of Bay Networks), that allows connection between manufacturing plants and other locations.

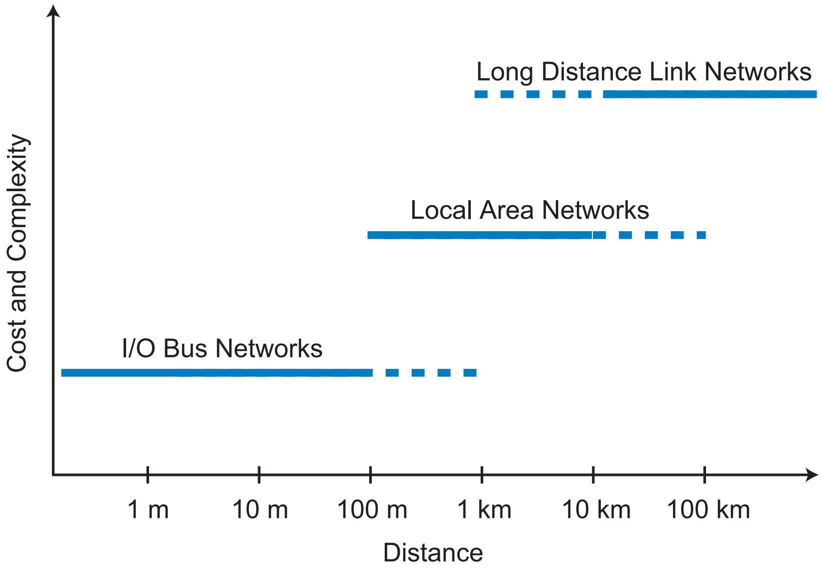
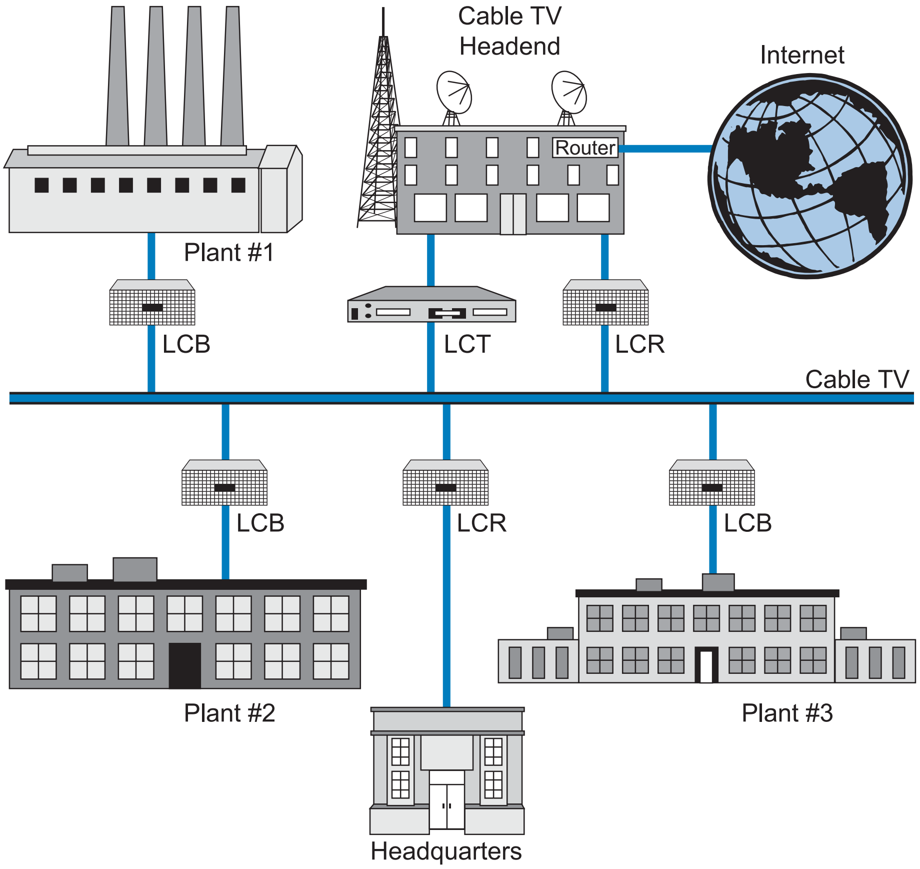


Figure 18-1. Network distance ranges.



LCT–Transmaster: single-channel translator
LCB–Bridge: Ethernet bridge to cable TV
LCR–Router: Internet via cable TV

Courtesy of LANcity—Cable Modem Division of Bay Networks, Andover, MA

Figure 18-2. LANcity cable TV network.

ADVANTAGES OF LANs

Before local area networks came into use, two other methods were employed to implement communication between PLCs. The first method used a pair of wires to connect the output card of one PLC to the input card of a second PLC. This method, which transmitted only one bit of information per pair of wires, was expensive to install and very cumbersome to use. In the second method, PLCs communicated through their programming ports via a central computer, which was customer-supplied and programmed. The disadvantages of this method were that it limited the data throughput rate to the baud rate of the PLC's programming port and that the network became unusable if the central computer failed due to the system's star topology.

The local area network offers distinct advantages over its predecessors because it greatly reduces the cost of wiring for large installations. It also uses a dedicated communication link to efficiently exchange large amounts of usable data among PLCs and other hosts. Moreover, because each PLC in the network can communicate independently with the others (without the use of a central computer), a LAN does not have the disadvantage of depending solely on one computer.

LAN Applications of the PLC

Centralized data acquisition and distributed control are the most common applications of local area networks. Data collection and processing, when performed by an individual controller, can burden the processor's scan time, consume large amounts of memory, and complicate the control logic program. A data highway configuration, in which all data is passed to a host computer that performs all data processing, eliminates these problems. Also, distributed control applications allocate control functions, once performed by a single controller, among several controllers. This eliminates dependence on a single controller and improves performance and reliability. To use the distributed processing approach, a local area network and the PLCs attached to it must provide the following functions:

- communication between programmable controllers
- upload capability to a host computer from any PLC
- download capability from a host computer to any PLC
- reading/writing of I/O values and registers to any PLC
- monitoring of PLC status and control of PLC operation

18-3 Network Topologies

The *topology* of a local area network is the geometry of the network, or how individual nodes are connected to it. A network's topology greatly affects its throughput rate, implementation cost, and reliability. The basic network topologies used today are star*,* common bus*,* and ring (see Figure 18-3). We should note, however, that a large network, such as the one shown in Figure 18-4, may consist of a number of interconnected topologies.

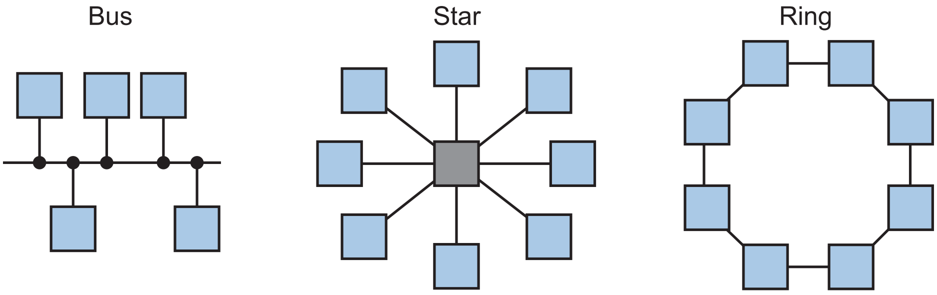


Figure 18-3. Bus, star, and ring topologies.

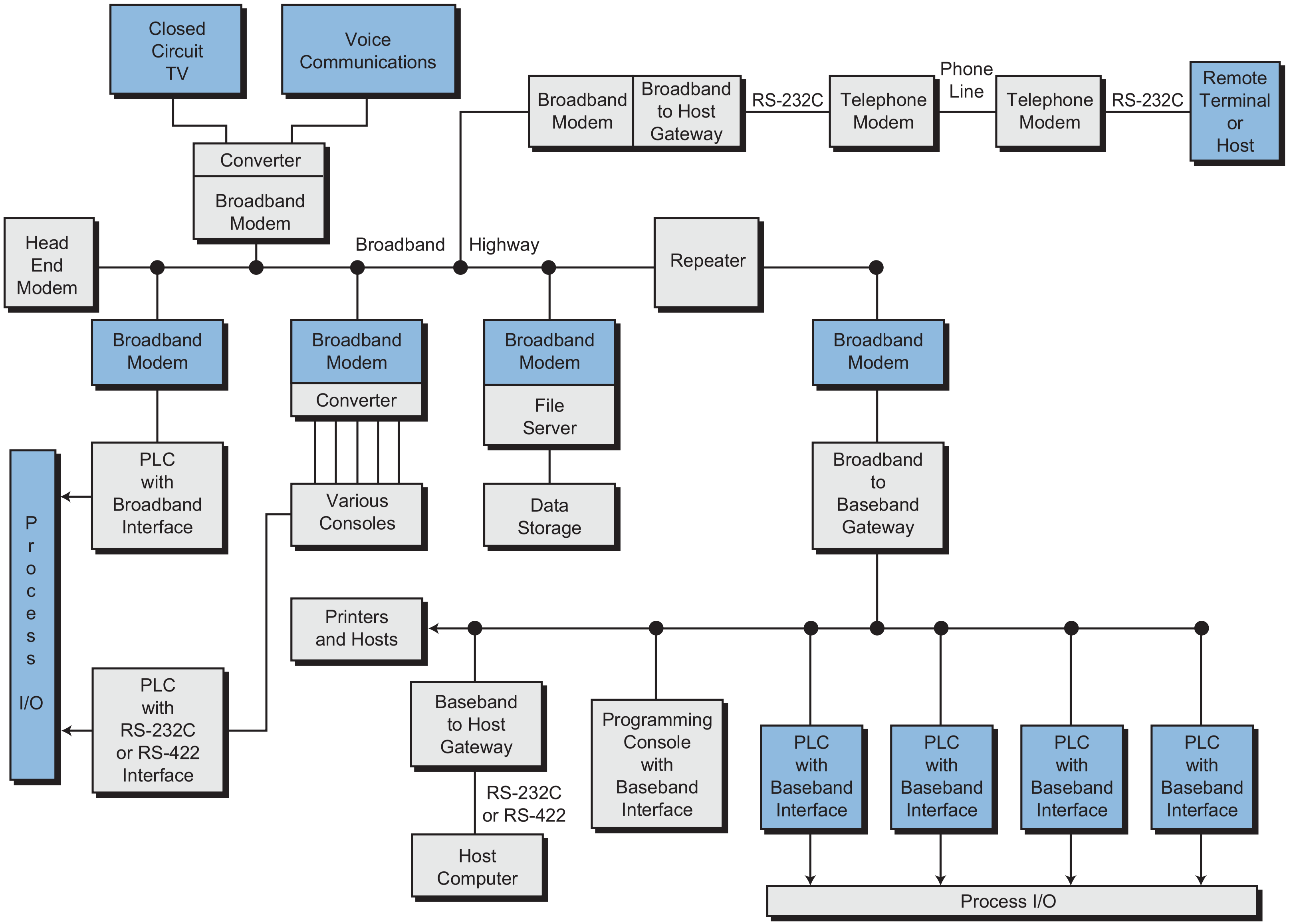


Figure 18-4. Large network using many different topologies.

Star

As mentioned previously, the first PLC networks consisted of a multiport host computer with each port connected to the programming port of a PLC. Figure 18-5 shows this arrangement, known as **star topology**. The network controller can be either a computer, a PLC, or another intelligent host.

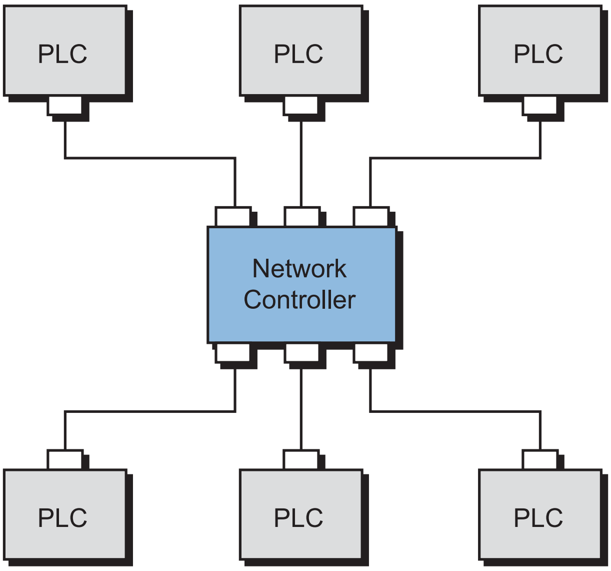


Figure 18-5. Star topology.

Most commercial computer installations are star networks, in which many terminals are tied to a central computer. This star topology is the same as the one used in telephone networks, where the central node has the task of establishing connections between the various network stations. The main advantage of this topology is that it can be implemented with a simple point-to-point protocol—that is, each node can transmit whenever necessary. If error checking is not required or if a simple parity bit per character check will suffice, then a *dumb terminal*, a terminal without network intelligence (e.g., a display monitor), can be a node. Star topology, however, has the following disadvantages:

- It does not lend itself to distributed processing due to its dependence on a central node.
- The wiring costs are high for large installations.
- Messages between two nodes must pass through the central node, resulting in low throughput.
- There is no broadcast mode, which lowers throughput even more.
- Failure of the central node will crash the network.

COMMON BUS

The **common bus topology** has a main trunkline to which individual PLC nodes are connected in a multidrop fashion (see Figure 18-6). A coaxial cable with proper terminators is typically the communication medium for the trunkline. In contrast to the star topology, communication in a common bus network can occur between any two nodes without passing information through a network controller. An inherent problem of this scheme, however, is determining which node may transmit at which time, to avoid data collision. Several communication access methods have been developed to solve this problem. We will discuss these later.

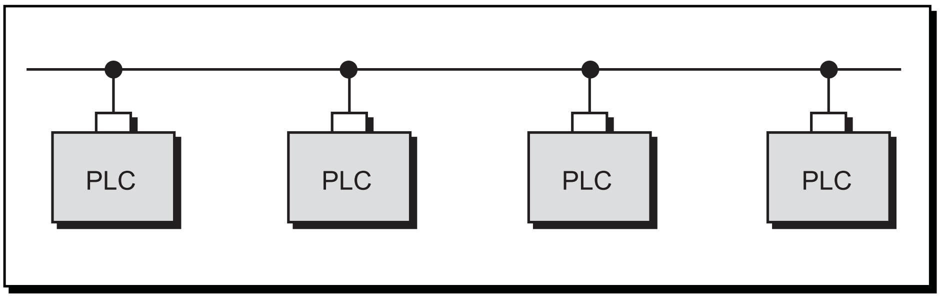


Figure 18-6. Common bus topology.

Common bus topologies are very useful in distributed control applications, since each station has equal independent control capability and can exchange information at any given time. Also, this topology requires little reconfiguration to add or remove stations from the network. The main disadvantage of this topology is that all of the nodes depend on a common bus trunkline. A break in this trunkline can affect many nodes.

Another configuration of the bus topology is the **master/slave bus topology**, consisting of several slave controllers and one master network controller (see Figure 18-7). In this configuration, the master sends data to the slaves; if the master needs data from a slave, it will *poll* (address) the slave and wait for a response. No communication takes place without the master initiating it. The implementation of a master/slave bus topology uses two pairs of wires. Through one pair of wires, the master transmits data and the slaves receive it. Through the other pair of wires, the slaves transmit data and the master receives it.

RING

Ring topology, shown in Figure 18-8, is not used in industrial environments because failure of any node (not just the master) will crash the network, unless the failed node is bypassed. We mention it here because it does not require multidropping due to its point-to-point connection restriction (see

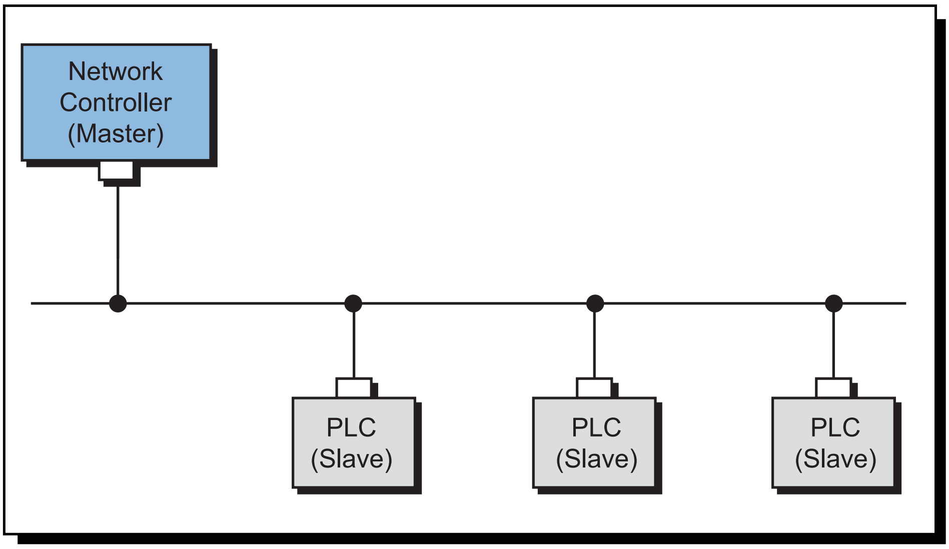


Figure 18-7. Master/slave bus topology.

Section 18-5). Thus, it is a good candidate for fiber-optic networks, since fiber-optic transmission media allows fast communication speed and long-distance connectivity.

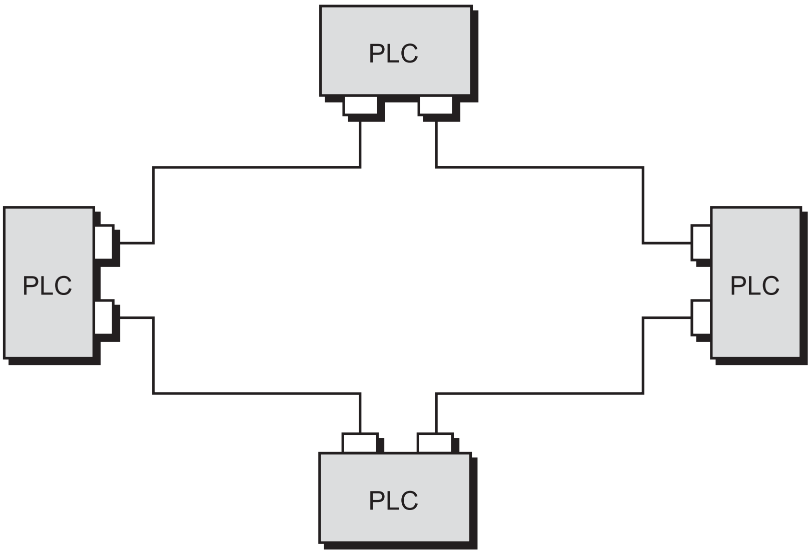


Figure 18-8. Ring topology.

Some LAN manufacturers have overcome the problem of node failure in a ring topology by using a wire center. The wire center, shown in Figure 18-9, automatically bypasses failed nodes in the ring. This **star-shaped ring topology**, however, requires twice as much wire as standard ring topology. Therefore, it must offer some other significant advantage (such as use in fiber optics) to be practical for large installations.

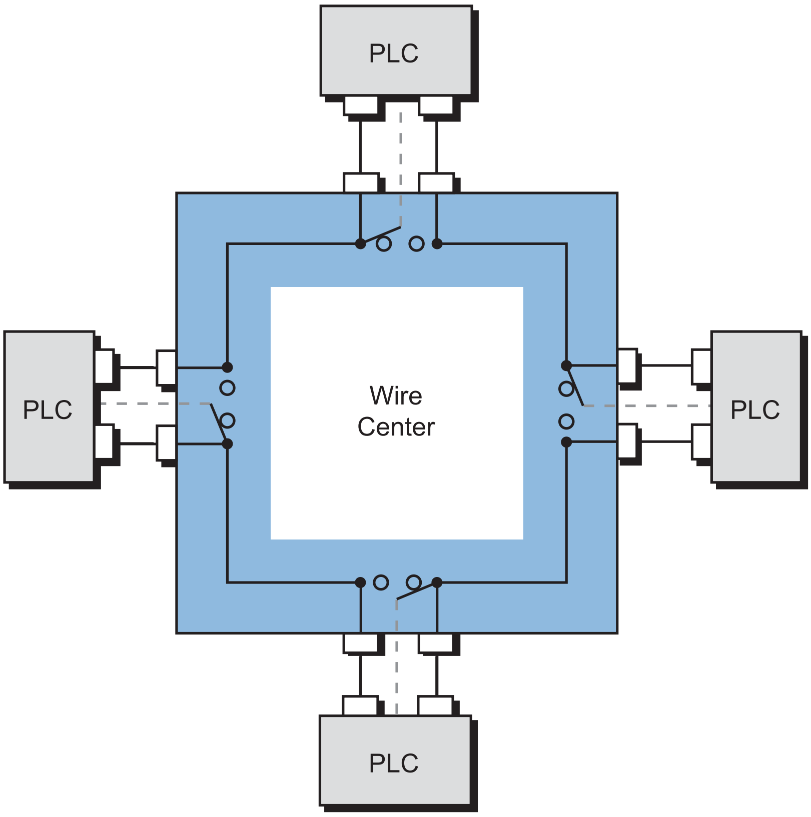


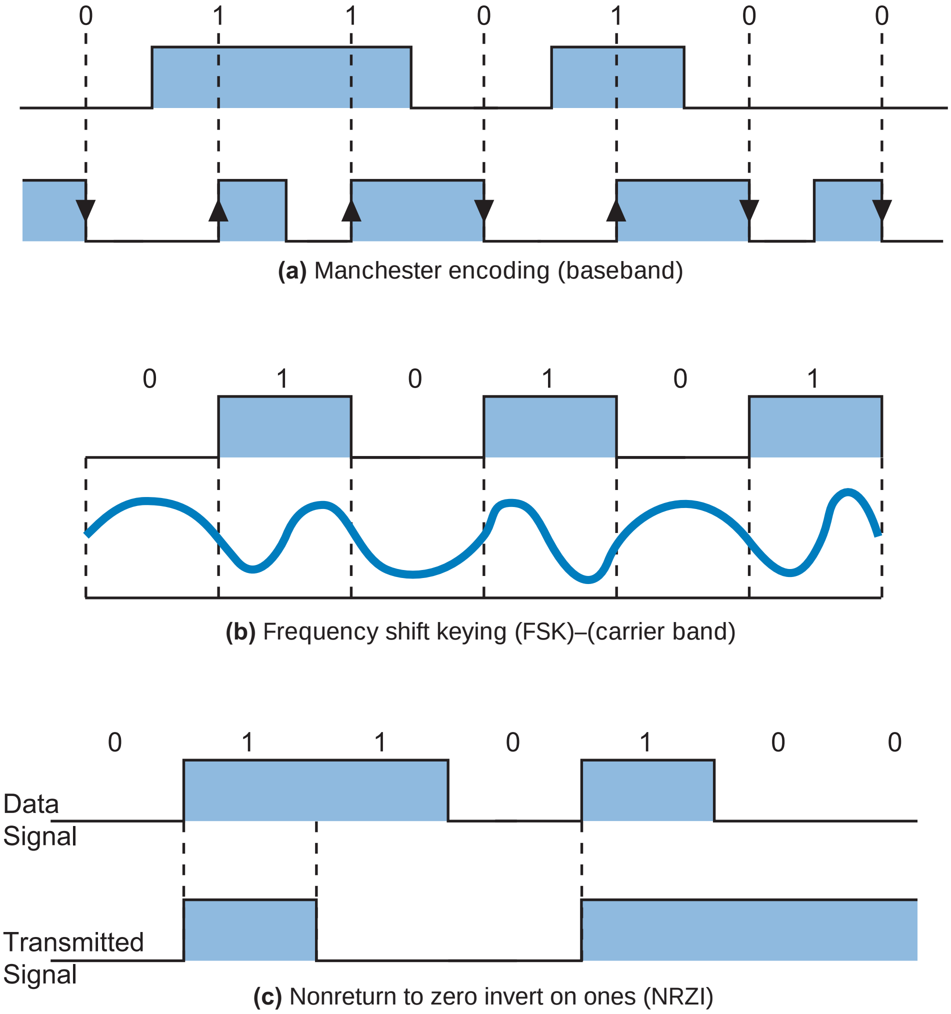
Figure 18-9. Star-shaped ring topology with a wire center.

DATA TRANSMISSION TECHNIQUES

Several transmission techniques are used to send data through a network (see Figure 18-10). Among the most common are:

- Manchester encoding
- frequency shift keying (FSK)
- nonreturn to zero invert on ones (NRZI)

Manchester encoding, also referred to as *baseband transmission encoding*, changes the signal polarity to positive for every logic 1 and to negative for every logic 0. During normal operation, the DC voltage on the cable is zero. *Frequency shift keying* (FSK) utilizes two frequencies to transmit logical values of 1 and 0. The *nonreturn to zero invert on ones* (NRZI) transmission technique involves a signal change whenever the next transmitted value is a 1. Ethernet networks use Manchester coding as their data transmission method.



(a) Manchester encoding (baseband)

(b) Frequency shift keying (FSK)–(carrier band)

(c) Nonreturn to zero invert on ones (NRZI)

Figure 18-10. Data transmission techniques: **(a)** Manchester encoding, **(b)** frequency shift keying, and **(c)** nonreturn to zero invert on ones.

18-4 NETWORK ACCESS METHODS

An access method is the manner in which a PLC accesses the network to transmit information. In other words, it defines the method used by the node to talk through the network. As mentioned in the previous section, a bus topology requires that the nodes take turns transmitting on the medium. This process requires that each node be able to shut down its transmitter without interfering with the network's operation. This can be done in one of the following ways:

- with a modem that can turn off its carrier

- with a transmitter that can be set to a high independence state
- with a passive current-loop transmitter, wired in series with the other transmitters, that shorts when inactive

Although many access methods exist, the most commonly used ones are polling*,* collision detection*,* and token passing.

POLLING

The access method most often used in master/slave protocols is **polling**. In polling, the master interrogates, or polls, each station (slave) in sequence to see if it has data to transmit. The master sends a message to a specific slave and waits a fixed amount of time for the slave to respond. The slave should respond by sending either data or a short message saying that it has no data to send. If the slave does not respond within the allotted time, the master assumes that the slave is dead and continues polling the other slaves. Interslave communication in a master/slave configuration is inefficient, since polling requires that data first be sent to the master and then to the receiving slave. Since master/slave configurations use this technique, polling is often referred to as the *master/slave access method.*

COLLISION DETECTION

Collision detection is generally referred to as CSMA/CD (carrier sense multiple access with collision detection). In this access method, each node with a message to send waits until there is no traffic on the network and then transmits. While the node is transmitting, its collision detection circuitry checks for the presence of another transmitter. If the circuit detects a collision (two nodes transmitting at the same time), the node disables its transmitter and waits a random amount of time before trying again. This method works well as long as the network does not have an excessive amount of traffic.

Each collision and retry uses time that cannot be used for transmission of data; therefore, the network's throughput decreases and access time increases as traffic increases. For this reason, collision detection is not popular in control networks, but it is popular in business applications. In industrial applications, collision detection can be used for data gathering and program maintenance in large systems and real-time distributed control applications with a relatively small number of nodes.

TOKEN PASSING

Token passing is an access technique that eliminates contention among the PLC stations trying to gain access to the network. In this technique, the PLCs pass a token, which is a message granting a polled station the exclusive, but temporary, right to control the network (i.e., transmit information). The station with the token has the exclusive right to transmit on the network; however, it must relinquish this right to the next designated node upon termination of transmission. Thus, token passing is actually a distributed form of polling. The token-passing access method is preferred in distributed control applications that have many nodes or stringent response time requirements.

In a common bus network configuration using the token-passing technique, each station is identified by an address. During operation, the token passes from one station to the next sequentially. The node that is transmitting the token also knows the address of the next station that will receive the token. The network circulates transmitted data in one or more information packets containing source, destination, and control data. Each node receives this information and uses it, if needed. If the node has information to send, it sends it in a new packet.

In the token-passing scenario shown in Figure 18-11, station 10 passes the token to station 15 (the next address), which in turn passes the token to station 18 (the next address after 15). If the next station does not transmit the token to its successor within a fixed amount of time (token pass timeout), then the token-passing station assumes that the receiving station has failed. In this case, the originating station starts polling addresses until it finds a station that will accept the token. For instance, if station 15 fails, station 10 will poll stations 16 and 17 without response, since they are not present in the network, and then poll station 18, which will respond to the token. This receiving station will become the new successor and the failed station will be removed from, or patched out of, the network (i.e., station 18 will become station 10's next address). The time required to pass the token around the entire network depends on the number of nodes in the network. This time can be approximated by multiplying the token holding time by the number of nodes in the network.

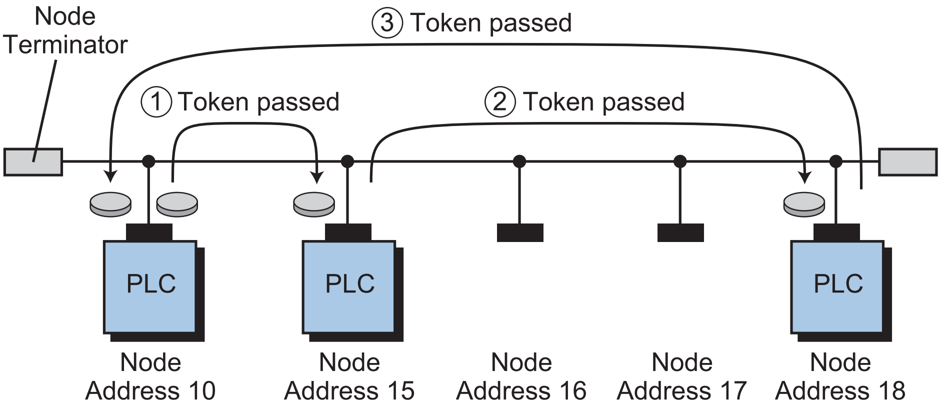


Figure 18-11. Example of token passing.

18-5 Communication Media

This section discusses the communication media (i.e., cables) used to implement local area networks. If installed properly, most local area networks can interface using any of these media. Proper installation includes the appropriate physical connectors and the correct electrical terminations. Media types commonly used for PLC networks include twisted-pair conductors, coaxial cables, and fiber optics. The type of media used and the number of nodes installed will affect the performance of the network (i.e., speed and distance). Figure 18-12 shows a comparison of different communication methods used with these media.

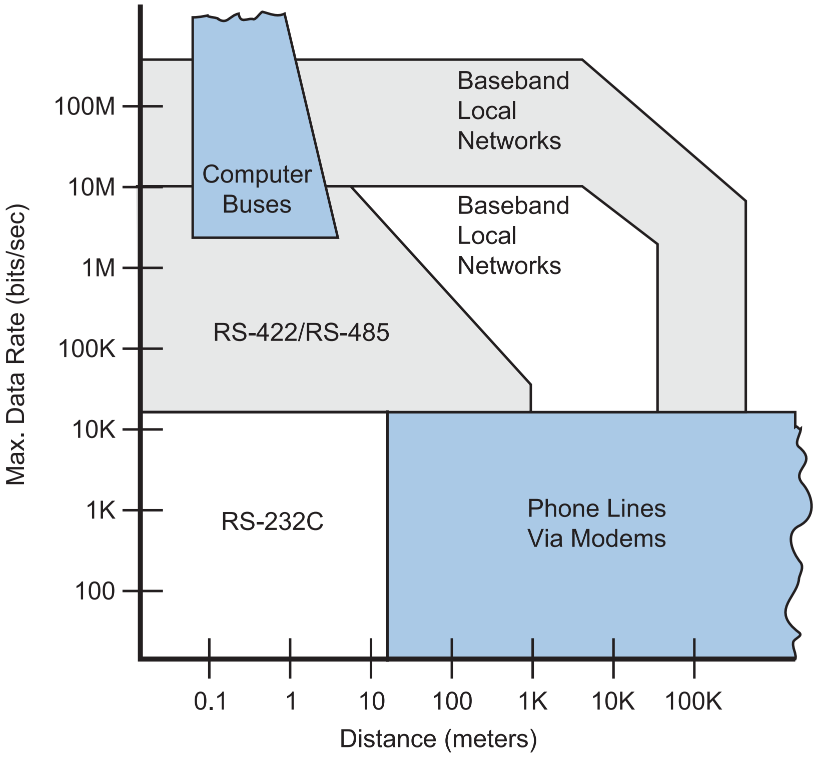


Figure 18-12. Comparison of the data transmission speeds and distances of various communication methods.

Twisted-Pair Conductors

Twisted-pair conductors are used extensively in industry for point-to-point applications at distances of up to 4000 feet and at transmission rates as high as 250 kilobaud. Twisted-pair conductors are relatively inexpensive and have fair noise immunity, which is improved when shielded. Performance, however, drops off rapidly as nodes are added to a twisted-pair bus. Moreover, nonuniformity also compromises the performance of these conductors. Characteristic impedance varies throughout the cable, making reflections difficult to reduce because there is no "right" value for termination resistance.

Baseband Coaxial Cable

Baseband coaxial cable, which can send one signal at a time at its original frequency, can transmit data in a local area network at speeds of up to 2 megabaud and distances of up to 18,000 feet. Unlike twisted-pair conductors, coaxial cable is extremely uniform, thus eliminating problematic reflections. The limiting factor for this type of cable is capacitive and resistive loss. Baseband cable is usually 3/8 inches in diameter.

Broadband Coaxial Cable

Broadband coaxial cable is thicker than baseband cable, ranging from 1/2 to 1 inch in diameter. Broadband cable, which has been used for years to carry cable television signals, can support a transmission rate of up to 150 megabaud. Although this type of coaxial cable can be used to increase distance in a baseband network, it is intended for use with a broadband network. Baseband networks use frequency division multiplexing to provide many simultaneous channels, each with a different RF carrier frequency. Broadband networks, on the other hand, use just one of these channels and one of the access methods previously discussed. The transmission rate on the channel is typically 1, 5, or 10 megabaud. Broadband local area networks can support thousands of nodes and are capable of spanning many miles through the use of bidirectional repeaters. One advantage of using broadband cable is that network communication can be implemented with just one of the broadband channels. The other channels can be used for video, computer access, and various monitoring and control functions.

Each broadband channel consists of two channels—a high-frequency forward channel and a low-frequency return channel. If only two nodes need to communicate, one can transmit on the forward channel and the other can transmit on the return channel. In a multidrop network, a head-end modem is required to retransmit the return channel signal on its corresponding forward channel in order for proper transmission and propagation to occur. The repeaters amplify the forward channel signals in one direction and the return channel signals in the other direction. Figure 18-4 presented an example of a broadband network with a baseband subnetwork.

Fiber-Optic Cable

Fiber-optic cable consists of thin fibers of glass or plastic enclosed in a material with low refraction. This type of cable transmits signals through pulses of reflected light. The main shortcoming of fiber optics is that a low-loss terminal access point, also called a *tap* or *T-connector*, has yet to be perfected. Currently, T-connectors in fiber-optic cable only pick up a small percentage of the light energy that transmits the information through the cable. This deficiency eliminates fiber optics from use in large bus topologies, but not from use in star or ring topologies. In addition, fiber-optic cable is three to four times more expensive than baseband coaxial cable, and optical couplers are several times more expensive than strictly electrical interfaces.

Fiber optics does, however, have some impressive advantages. First, it is totally immune to all kinds of electrical interference. Second, it is small and lightweight. Finally, it can sustain transmission rates of up to 800 megabaud at distances of up to 30,000 feet. In light of these qualities, the use of fiber optics should increase in industrial applications as the technology develops.

18-6 Understanding Network Specifications

This section explains how to determine if a particular network can support a given application. The designer should examine all aspects of the network, including device specifications, response time, maximum length, throughput, and interface, when choosing a network for an application.

Device Specifications

When selecting a network, the system designer must analyze the application to determine how many nodes are required and what type of device—PLC, vendor-supplied network programmer, host computer, or intelligent terminal—will be used at each node. The designer must determine if the network will support each type of device used and examine how that device will interface with the network (hardware and software). For network PLCs, the designer must also choose the model, because some PLC models are not capable of interfacing with a network. The network must be capable of supporting the number of nodes required for the current application, plus a reasonable number of nodes for future expansion.

Maximum Length

The maximum length of a network consists of two parts: the maximum length of the main cable and the maximum length of each drop cable used between a node and the main cable. Maximum drop lengths usually range between 30 and 100 feet; however, drop lengths should be kept as short as possible, since drops introduce reflection into the network. The ideal case is to run the main cable straight to the device and back again, even though this procedure increases wiring costs.

Another important piece of information that the designer should obtain from the vendor is the type of cable that must be used to achieve the specified transmission distance. If the system requires the maximum network transmission distance, the designer must use the proper type of cable. If the system requires a much shorter transmission distance, the designer can save money by using a less expensive cable.

RESPONSE TIME

Response time (RT), as used in this book, is the time between an input transition at one node and the corresponding output transition at another node. Response time, then, is the sum of the time required to detect the input transition, transmit the information to the output node, and operate the output. It is expressed as:

$$RT = IT + 2ST_1 + PT_1 + AT + TT + PT_2 + 2ST_2 + OT$$

where:

IT = the input delay time (the electrical delay involved in detecting the input transmission)

ST_1 = the scan time for the sending node

ST_2 = the scan time for the receiving node

PT_1 = the processing time for the sending node (the time between solving the program logic and becoming ready to transmit the data)

PT_2 = the processing time for the receiving node (the time between receiving the data and having data ready to be operated on by the program logic)

AT = the access time (the time involved in both becoming ready to transmit and in transmission)

TT = the transmission time (the time required to transmit data—this is the only time that is directly proportional to baud rate)

OT = the output delay time (the electrical delay involved in creating the output transition)

The scan time includes the I/O update time and any other overhead time, as well as the program logic execution time. It can be defined as the time between I/O updates. In the previous equation, the scan time is doubled to include the case where the input signal changes just after the I/O update. In this case, the network first executes the logic with the old information, then performs an I/O update, and finally executes the logic with the new information. This causes a two-scan delay.

I/O delay times and scan times are readily available values. Transmission time can be determined once the data rate and frame length are known. The data rate is sometimes equal to the baud rate, but it is usually less. Synchronous systems, which use Manchester encoding, have a data rate that is half of the baud rate. These systems utilize a transmission method in which the data characters and bits are transmitted at a fixed rate with the transmitter and receiver in synchronization. The data rate of asynchronous systems is

80% of the baud rate due to the start and stop bits that accompany each 8 data bits. In these systems, the time intervals between transmitted characters may be unequal in length. Transmission in an asynchronous system is controlled by start and stop signals at the beginning and end of each character.

The access time and the two processing times depend on the particular installation and generally must be obtained from the manufacturer. If the equipment is available, it is much easier and more accurate to determine the overall response time through actual measurements than through specifications. Section 18-8 presents a procedure for performing this measurement.

The parameter that should be determined by the response time equation is not the average response time, but rather the maximum response time. Therefore, the designer should take steps to create a worst-case environment during response time measurements. Creating this scenario involves performing tasks such as downloading programs and monitoring points while taking the measurements, because this sort of activity increases PLC scan times and network access times.

THROUGHPUT

Some manufacturers specify the LAN throughput value. This value represents the number of I/O points that can be updated per second through the network. The throughput value does not provide enough information to derive actual values for access time and data rate, although it gives the system designer some idea of these values. In addition, throughput varies with system loading as a result of each node's processing time. Therefore, to obtain an accurate value for throughput, the designer must know the conditions under which the measurement was taken.

DEVICES SUPPORTED

When considering each device in the system, the designer must ask not only, Will the local area network support this device?, but also, What is involved in connecting the device to the network? For user-supplied devices, the designer must also determine what support software will be required.

Programmable Controllers. All of the standard networks support at least some PLCs. A separately purchased interface unit usually connects a PLC to a network. The interface unit is connected to the PLC through either a high-speed parallel bus or the PLC's serial programming port. In the latter case, two additional terms must be added to the response time equation: the programming port transmission time and the programming port processing time.

Programming Devices. Most manufacturers offer some type of personal computer as a programming device that can be connected to a network. A PC unit connected to a network provides centralized programming of any

PLC on the network, along with various monitoring and control functions, if available. If a network-compatible programming device is not available, all programming must be done through the programming port of the individual PLCs.

Hosts. Host support means that a user-supplied host computer can perform programming functions, provided that its programming conforms to the network manufacturer's protocol. The host computer is usually connected to the network through a device called a **gateway**. The gateway contains a network port and another port (usually RS-232), which is connected to the host. A gateway greatly simplifies the software that the user must write for the host, because a host-to-gateway link requires only a simple point-to-point protocol rather than a masterless multidrop protocol, as is required by a network. A gateway also provides the appropriate electrical interfaces for the network. Since most computers have an RS-232 port, additional hardware is seldom required.

Intelligent Terminals. The type of intelligent terminal referred to here is actually a small host computer complete with an operating system and mass storage. It can interface with the network in exactly the same way as a large host computer. Anyone considering using one of these terminals on a network should investigate the software requirements closely to determine if the terminal's operating system will support the network's requirements. Some operating systems, for instance, provide for the transmission of only ASCII data, not binary data.

Gateways. In addition to the host gateway mentioned previously, some manufacturers provide gateways to other multidrop networks. They also provide other types of host gateways, for example, a high-speed, RS-422, synchronous host interface. In this case, the gateway would use a protocol designed for synchronous use, such as HDLC.

Application Interface

When developing an application interface, the designer must determine how each PLC's application program allows it to share information with other PLCs. Most manufacturers provide at least one of the following methods:

- reading of registers in other PLCs
- writing to registers in other PLCs
- reading and writing of network points or registers

For example, a PLC can detect the input status of another PLC on the network through the use of a network coil and a network contact. Figure 18-13 illustrates this configuration. When the network coil (Net 200) in PLC #1 is energized, the network contact, Net 200 (⊣⊢), in PLC #2 will close. PLC #2 can use this contact like any other contact in its ladder program. The user, however, must ensure that only one PLC on its network uses each network coil.

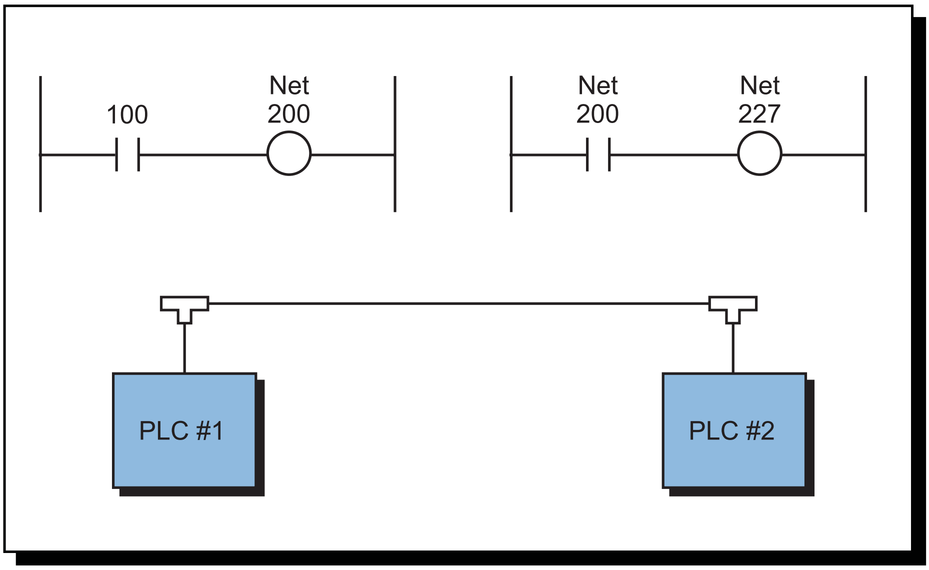


Figure 18-13. Network coils and contacts.

Network PLCs read to and write from registers through functional blocks. The designer must ensure that the capabilities of the network and PLCs are sufficient to support the communication needs of the application. Chapter 9 shows some of the typical network instructions found in PLCs.

18-7 Network Protocols

A protocol is a set of rules that two or more devices must follow if they are to communicate with each other. Protocol includes everything from the meaning of data to the voltage levels on connection wires. A network protocol defines how a network will handle the following problems and tasks:

- communication line errors
- flow control (to keep buffers from overflowing)
- access by multiple devices
- failure detection
- data translation
- interpretation of messages

OSI Reference Model

Networks follow a protocol to implement the transmission and reception of data over the network medium (e.g., coaxial cable). In 1979, the International Standards Organization (ISO) published the Open Systems Interconnection (OSI) reference model, also known as the ISO IS 7498, to provide guidelines for network protocols. This model divides the functions that protocols must perform into seven hierarchical layers (see Figure 18-14). Each layer interfaces only with its adjacent layers and is unaware of the existence of the other layers. Table 18-1 describes the seven layers of the OSI. The OSI model further subdivides the second layer into two sublayers, 2A and 2B, called *medium access control* (MAC) and *logical link control* (LLC), respectively. In network protocols, the physical layer (layer 1) and the medium access control sublayer (layer 2A) are usually implemented with hardware, while the remaining layers are implemented using software. The hardware components of layers 1 and 2A are generally referred to as modems (or transceivers) and drivers (or controllers), respectively.

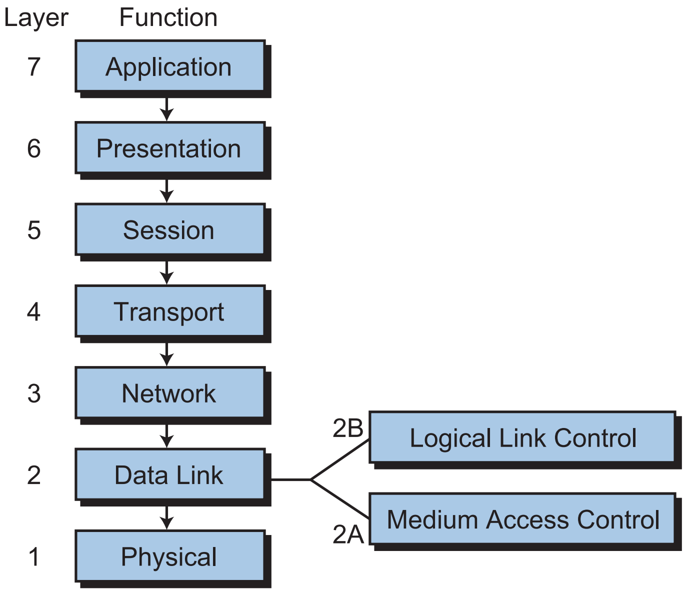


Figure 18-14. OSI reference model.

Strictly speaking, a network requires only layers 1, 2, and 7 of the protocol model to operate. In fact, many device bus networks, which we will cover in the next chapter, use only these three layers. The other layers are added only as more services are required (e.g., error-free delivery, routing, session control, data conversion, etc.). Most of today's local area networks contain all or most of the OSI layers to allow connection to other networks and devices.

Layer	Layer Name	Function
Layer 7	Application	The level seen by users; the user interface
Layer 6	Presentation	Control functions requested by the user; data is restructured from other standard formats; code and data conversion
Layer 5	Session	System-to-system connection; log-in and log-off controlled here; establishes connections and disconnections
Layer 4	Transport	Provides reliable data transfer between end devices; network connections for a given transmission are established by protocol
Layer 3	Network	Outgoing messages are divided into packets; incoming packets are assembled into messages for higher levels, establishing connections between equipment on the network
Layer 2	Data link	Outgoing messages are assembled into frame and acknowledgements; error detection or error correction is perfomed
Layer 1	Physical	Parameters, such as signal voltage swing, bit duration, and electrical connections, are established in this layer

Table 18-1. Seven layers of the OSI reference model.

To understand this seven-layer architecture, let's examine a familiar everyday example, an interoffice memo (see Figure 18-15). Imagine that two offices form two network nodes at two separate locations. If the manager of one office wants to send a memo to the manager of the other office, he/she must write the message with pencil and paper. After the message is written, the manager passes it to the secretary to be properly typed, addressed, stamped, and mailed. The pencil and paper corresponds to the seventh layer (application layer), which is the level that concerns the manager (i.e., the network user). He/she "applies" the pencil and paper to send the message. After that, it is no longer his/her responsibility; however, the memo remains in the system, meaning that the memo is still in the manager's office, having passed to the next steps that must occur before it enters the postal mail system. These other steps are the next six layers of the OSI model:

- The secretary types the memo and puts both the correct sender and receiver addresses on the envelope (layer 6—coding and conversion).
- He/she puts the memo in an envelope, affixes the correct amount of postage, and takes it to the mail room (layers 5, 4, and 3, respectively).

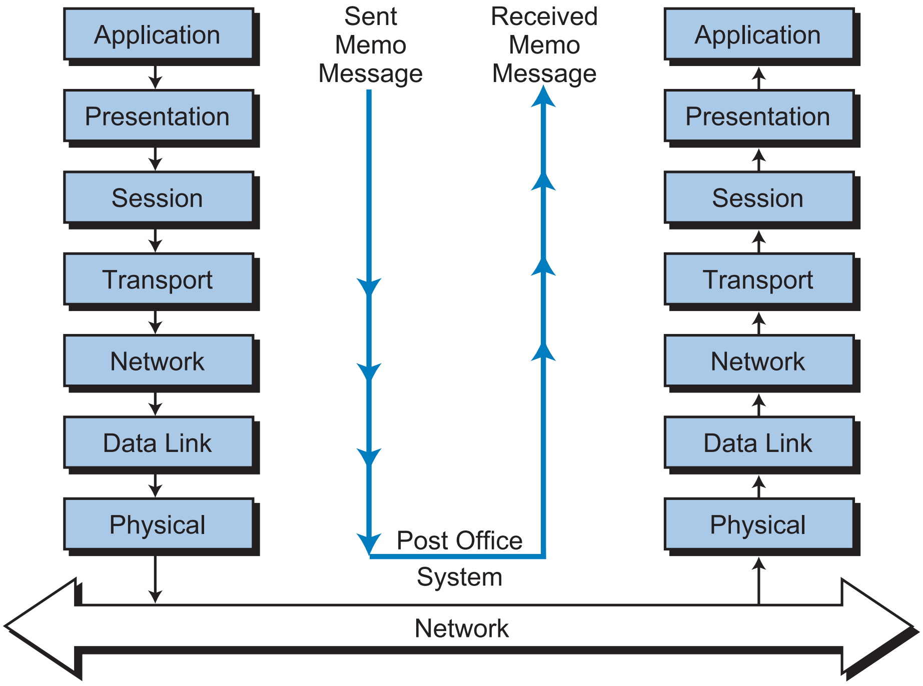


Figure 18-15. Seven-layer architecture.

- The mail room clerk takes the memo, makes sure that it has the right postage and address, and puts it in the outgoing mail basket with the other mail (layer 2).
- The mail carrier then physically picks up the memo (layer 1) and sends it through the postal mail system, or in other words, through the network.

After a couple of days, the other office receives the memo and a similar operation takes place, but in reverse order. The mail carrier delivers the memo, the clerk checks to see if the receiver works there and in which department. Then, the clerk sends the memo through the internal company delivery system and it arrives at the receiving manager’s secretary. The secretary passes the memo to the manager, who reads it and interprets the message. This seven-step method ensures proper creation, implementation, and delivery of the message, since a protocol of orderly operations takes place.

The ISO’s OSI model embraces an architecture that is followed by most protocol standards. Each standard is intended to be open so that network devices from different manufacturers can be interconnected. Specialized technical organizations, as opposed to standards committees such as the ISO, have made the largest efforts towards the standardization of network protocols. The ISO, however, will accept and validate a network standard as long as it complies with the protocol architecture defined by the OSI model.

IEEE STANDARDS

The Institute of Electrical and Electronic Engineers (IEEE) computer society established the Standards Project 802 in 1980 for the purpose of developing a local area network standard that would allow equipment from different manufacturers to communicate through a local area network. After studying all the users' and manufacturers' requirements, the committee developed standards that define several types of local networks.

IEEE 802.3. The IEEE, in accordance with the ISO, agreed to be responsible for the specifications of local area networks whose transmission speeds range between 1 and 20 megabaud (megabits/sec). The IEEE 802.3 standard, which the ISO accepted as its own standard (ISO 8802), regulates layers 1 and 2A of the OSI model. Figure 18-16 illustrates the different parts of the IEEE 802 standard and its relationship to the OSI model.

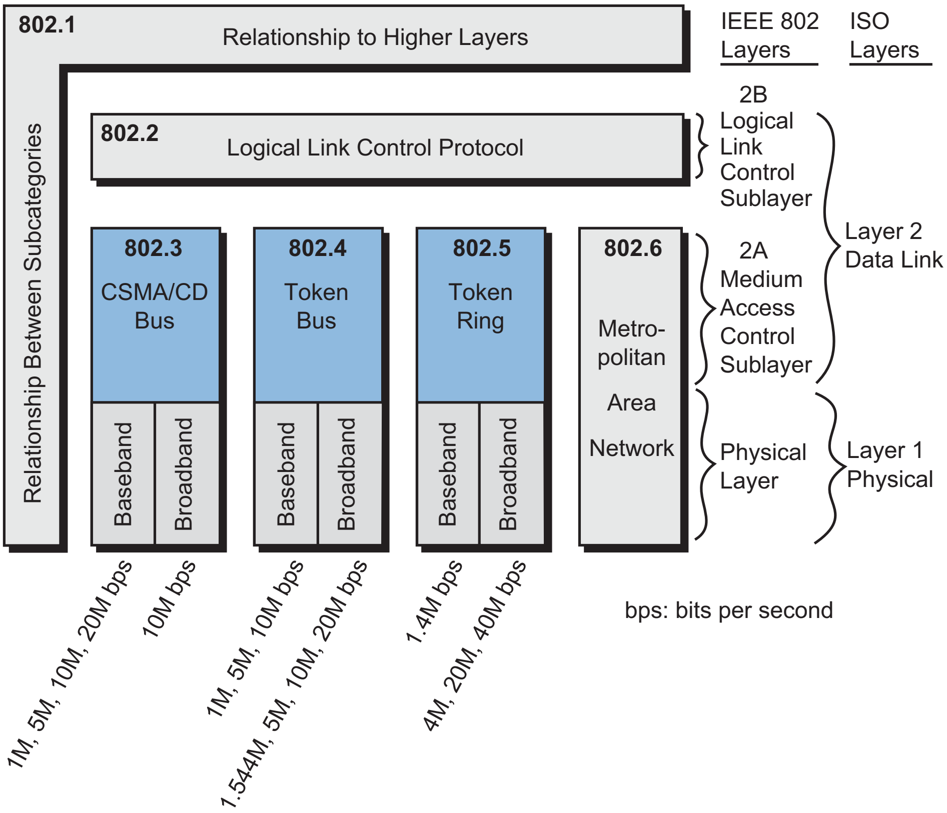
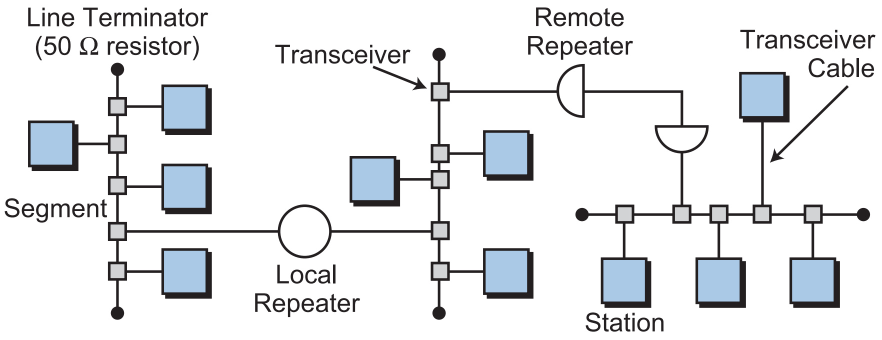


Figure 18-16. IEEE 802 standard.

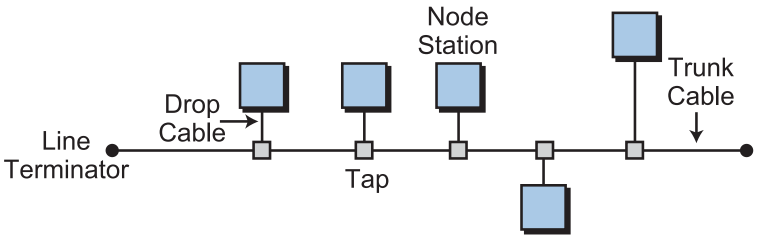
The IEEE 802.3 standard specifies that network access should occur through CSMA/CD using a bus topology at a rate of 1 to 20 Mbaud (baseband) or 10 Mbaud (broadband). The widely used Ethernet network complies with the IEEE 802.3 standard. In fact, when Ethernet was first developed in the early 1980s through a joint effort of Digital Equipment Corporation (DEC), Xerox, and Intel, the IEEE accepted it with only a few modifications to make it comply with the 802.3 (CSMA/CD bus). The ISO has also taken Ethernet as a standard, the ISO 8802.3. In control systems, the Ethernet (802.3) network is primarily suited for noncritical applications, such as supervisory monitoring and PLC program management.

IEEE 802.4 and 802.5. The IEEE 802.4 standard specifies a token bus network at different baseband and broadband transmission rates than the IEEE 802.3 standard. The 802.4 standard is used by many PLC manufacturers as the protocol structure of the lower layers of their local area networks. Furthermore, another IEEE standard, the IEEE 802.5, specifies a token ring network with lower transmission rates for baseband cables (1.4 Mbaud). IBM adopted the 802.5 standard for their token-passing protocol with ring topology. Figures 18-17a, b, and c illustrate the general characteristics of the IEEE 802.3, 802.4, and 802.5 standards, respectively.



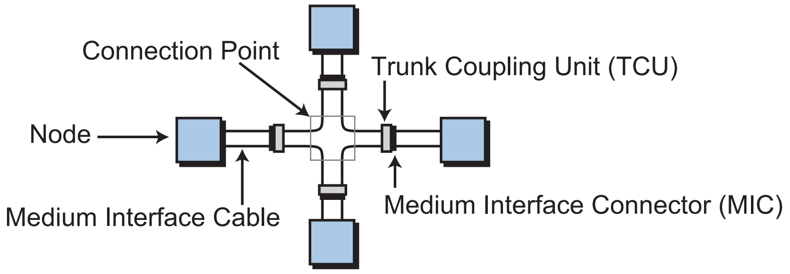
Topology:	extended bus (tree structure)
Method of transmission:	baseband, broadband
Data rate:	10 Mbit/sec
Coding:	Manchester
Access method:	CSMA/CD
Transmission media:	special coaxial cable
Max. distance between two nodes:	2.8 km

Figure 18-17a. Characteristics of the IEEE 802.3 standard (Ethernet).



Topology:	physical bus, logical ring structure
Method of transmission:	carrier band, broadband
Data rate:	1 to 20 Mbit/sec
Coding:	FSK, PSK
Access method:	token passing
Transmission media:	coaxial cable, fiber optics cable
Max. distance between two nodes:	800 m

Figure 18-17b. Characteristics of the IEEE 802.4 standard (token bus).



Topology:	physical and logical ring
Method of transmission:	baseband
Data rate:	1, 4, 16 Mbit/sec
Coding:	Manchester
Access method:	token passing
Transmission media:	twisted-pair cable
Max. distance between two nodes:	100 m

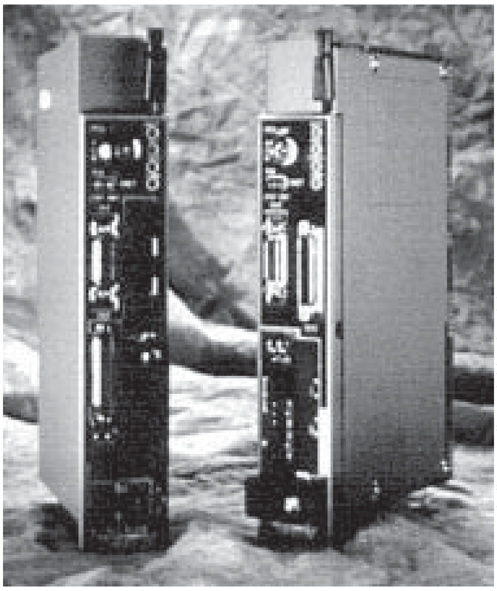
Figure 18-17c. Characteristics of the IEEE 802.5 standard (token ring network).

TCP/IP PROTOCOL

Most manufacturers who offer Ethernet compatibility to implement supervisory functions over equipment controlling plant floor functions use a TCP/IP protocol for layers 3 and 4 of the OSI model. The **transmission control protocol/internet protocol (TCP/IP)** was initially developed for Arpanet, a computer network created in the early 1970s in the United States. The U.S. Department of Defense established this protocol to communicate information in a reliable manner from one computer to another over the Arpanet network. Nowadays, the TCP/IP protocol is utilized in the Internet data network.

In the TCP/IP protocol, the TCP guarantees control of end-to-end connections. The TCP makes several services available to the user, such as the establishment of network connections and disconnections, guaranteed data sequencing, protection against loss of sequence, connection time control, and transparent multiplexing and transport of data. The IP (internet protocol) performs complementary functions such as addressing network data, distributing data packages, and routing data in multinetwork systems.

Some PLC manufacturers offer programmable controllers with TCP/IP-over-Ethernet protocol built into the PLC processor (see Figure 18-18). This allows the PLC to connect directly to a supervisory Ethernet network (see Figure 18-19). Note that the PLC in Figure 18-19 can also have a control network with other PLCs. Sometimes, the TCP/IP section in a supervisory network is replaced by another protocol, the *manufacturing message specification* (MMS) protocol, which is used by plant floor devices to communicate through 802.3 networks (see Figure 18-20). In this configuration, a PLC can communicate with other intelligent systems, such as robots and CNC machining centers.



Courtesy of Allen-Bradley, Highland Heights, OH

Figure 18-18. Allen-Bradley's PLC-5 controllers with built-in TCP/IP-over-Ethernet protocol.

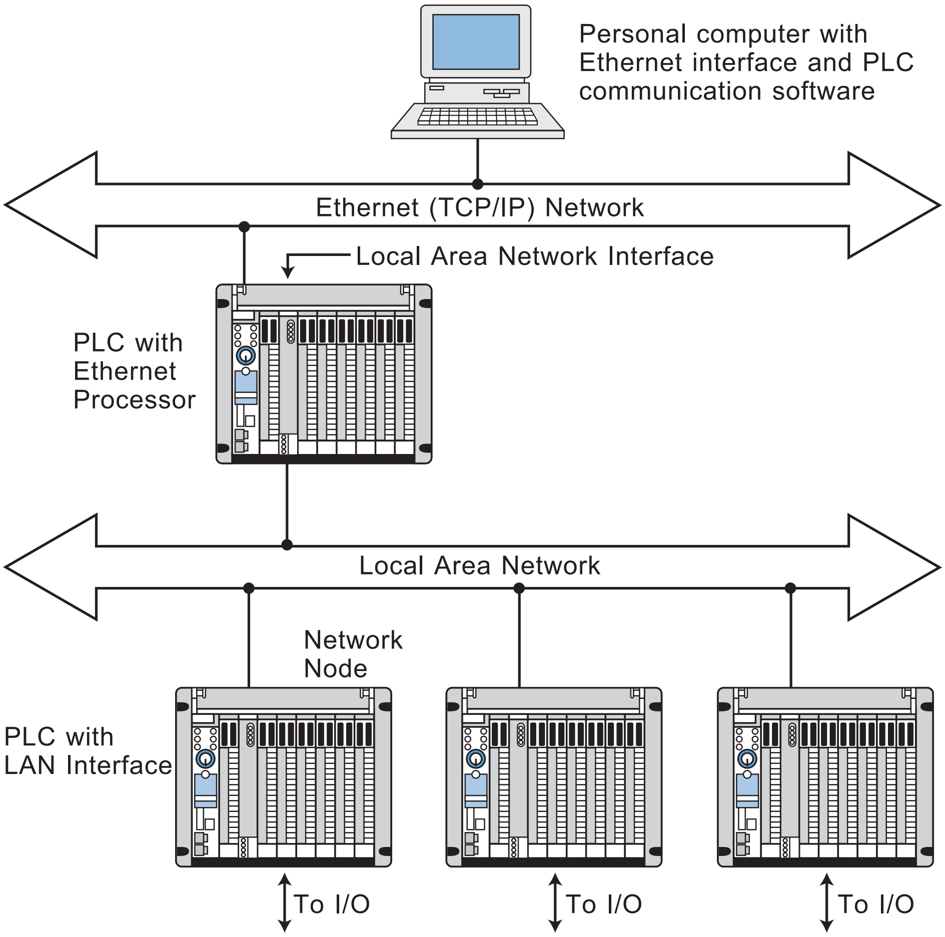

Personal computer with Ethernet interface and PLC communication software
Ethernet (TCP/IP) Network
Local Area Network Interface
PLC with Ethernet Processor
Local Area Network
Network Node
PLC with LAN Interface
To I/O
To I/O
To I/O

Figure 18-19. PLC connected directly to an Ethernet network.

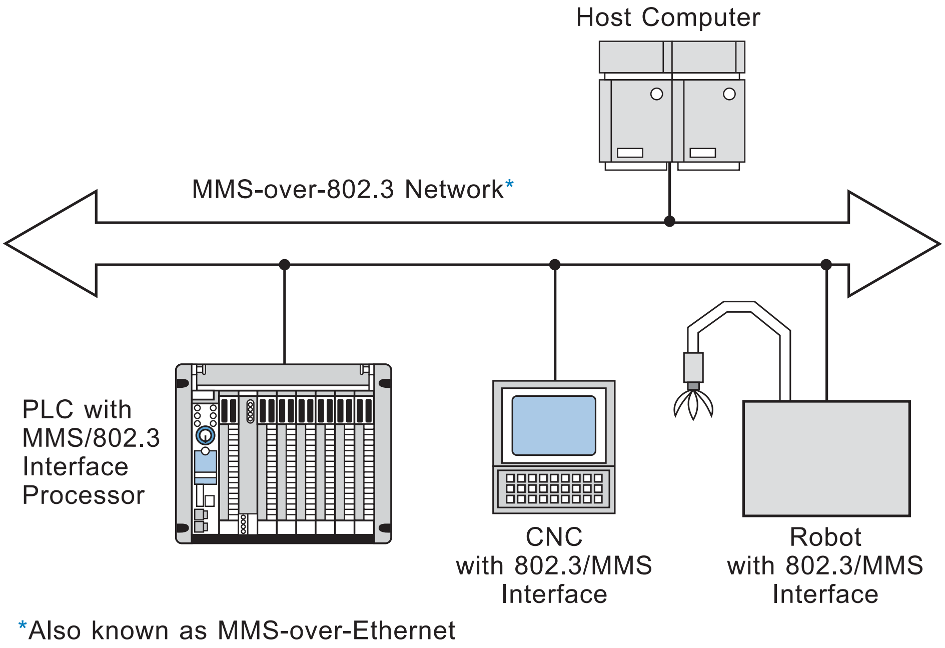

Host Computer
MMS-over-802.3 Network*
PLC with MMS/802.3 Interface Processor
CNC with 802.3/MMS Interface
Robot with 802.3/MMS Interface
*Also known as MMS-over-Ethernet

Figure 18-20. MMS protocol.

18-8 NETWORK TESTING AND TROUBLESHOOTING

Before a local area network is installed, the designer should test it to ensure that it not only performs the desired function, but also provides the required response time. The application program should continuously monitor the response time and take appropriate action if it exceeds the maximum time that the process will tolerate. A programmed buzzer circuit, which passes the contact closure through every critical node in the network before it is returned, can test the response time. Using this process, the pulse width of the created pulse is equal to the response time. This pulse width can be applied to a timer, which is set to the maximum allowable response time. When the timer times out, the circuit knows that the response time has been exceeded.

Troubleshooting networks can be quite difficult unless both the manufacturer and the user take steps to simplify the task. The manufacturer can provide error counts and a self-test for each node, while the user can provide application programming to detect the failure of a node. An extreme case of this would be to provide a buzzer and timer between each node and every other node. Thus, if the entire network goes down, it is probably due to a node with a short or a constantly transmitting transmitter. The user can determine which node is faulty by disconnecting each node one at a time and observing if communication is restored. Some manufacturers provide a network monitor that can detect a failed node, an open cable, or excessive electrical interference.

18-9 Network Comparison and Selection Criteria

Network Comparison

The most distinctive differences among local area networks are the transmission or communication medium and the network access method. Table 18-2 shows the advantages and disadvantages of each type of communication medium and access method. The communication medium directly affects the cost of a LAN installation from the outset due to the price difference between the types of network cables. For instance, baseband cable is cheaper to install and maintain, as well as troubleshoot. Broadband cable is more expensive to install but has the capability for multiple transmission through the same cable, which is the case in cable TV (multiple channel transmission). Depending on the type of network, the troubleshooting of voice, process data, and other information parameters may be more difficult with broadband cable.

	Transmission Medium	
	Broadband	**Baseband**
Multiple transmission	+	–
Installation cost	–	+
Maintenance cost	–	+
Troubleshooting	–	+

	Medium Access	
	CSMA/CD (Ethernet, 802.3)	**Baseband (802.4)**
Response time	even	+
Operation with multiple nodes (50% of max)	–	+
Safety against failure	+	even
Network expandibilty	+	even

Table 18-2. Advantages and disadvantages of transmission media and access methods.

The network's access method also influences the manner in which nodes communicate with each other and the time required for that communication. CSMA/CD, for example, has the disadvantage of not being able to accurately predict the response time of a message transmission due to the delay caused by too many nodes trying to communicate at the same time. This short delay may be acceptable in an office environment using Ethernet (IEEE 802.3), where the information transfer speed is not of vital importance. However, in an industrial control environment, this type of delay could cause a major process breakdown. Token passing, on the other hand, has a predictable response time, even when the network has a large number of nodes.

SELECTION CRITERIA

Table 18-3 lists some of the criteria that should be evaluated during the selection of a local area network. These criteria cover four important areas: the speed and capacity of the network, the reliability of the network, the flexibility of the network, and the overall cost associated with network configuration.

Local Area Network Considerations	
Speed and capacity	• Data rate/throughput • Possible delays due to error transmission • Response time based on network load (number of nodes)
Reliability	• Safe transmission • Total failure protection • Data protection against unauthorized access
Flexibility	• Changes • Expansions • Compatibility with other networks
Costs	• Initial installation • Expansion • Maintenance • Network hardware/software cost

Table 18-3. Criteria to evaluate when choosing a LAN.

Most industrial networks can transfer information fast enough to suit the majority of applications; therefore, it is not necessary to obtain a very high-speed network unless the application specifically requires it. The processing speed of the PLCs connected to the network and the total scan requirements of the system determine the required network speed. If a supervisory system is being used to monitor a PLC network, however, speed may not be a factor. In this situation, an Ethernet or 802.3 network (CSMA/CD) may be appropriate because compatibility may already exist between the supervisory equipment (e.g., nonprocess automation computers) and the PLC network. A supervisory network like Ethernet ensures the support of many devices, since most PLC manufacturers can provide Ethernet compatibility either through a gateway or directly through the PLC using the local area network. In contrast, PLC manufacturers' proprietary networks may not have as many compatible peripherals and field equipment as an Ethernet network.

Reliability, flexibility, and cost are all as important as speed in network selection. Reliability of a network deals with the detection and correction of system errors. A network must have a reliable way of automatically detecting any system errors, and it must also provide a way for the user/programmer to shut down a machine or process. The flexibility of a network deals with the ease of adding a node to the network, as well as the addressability of each network node. Many manufacturers of PLC local area networks provide network management software that gives the user flexibility when programming the network. Finally, the cost of a network must be analyzed not only for the initial installation costs, but also for maintenance and expansion costs. A network that is initially inexpensive to implement may turn out to be expensive due to restrictions on the addition of nodes and the lack of flexibility for changes.

Key Terms

baseband coaxial cable
broadband coaxial cable
collision detection
common bus topology
fiber-optic cable
gateway
local area network (LAN)
master/slave bus topology
polling
response time
ring topology
star-shaped ring topology
star topology
token passing
transmission control protocol/internet protocol (TCP/IP)
twisted-pair conductor

This page intentionally left blank.