Chapter 37

Manufacturing Networks

37.1 NETWORK APPLICATIONS

Manufacturing networks provide the infrastructure to transmit manufacturing and management data used to define and control computer-integrated manufacturing systems or components of computer-aided design (CAD) and computer-aided manufacturing (CAM). These data consist of CAD drawings, production schedules, inventory information, production information, production programs (for example, computer-numerical control [CNC] and programmable logic control [PLC] programs), production order releases, operation sheets, routing sheets, production order releases, inventory levels, and maintenance information. These data need to be transmitted to and from the production floor and within the corporate enterprise. The computer networks consist primarily of local area networks (LANs). LANs also can be joined to form enterprise-wide computing (EWC) or corporate intranets. An *intranet* is similar to the Internet except it can only be accessed by people within the company or organization.

Computer networks are specified by bandwidth architecture, access protocol, cable, distance, and cost. As computer network technology changes, the specifications for these terms will change, but the industry will continue to use them to describe the various networks for the foreseeable future. *Bandwidth* has become the focus for the computer communications industry with intranets and the internet becoming common information sources for manufacturing and corporations. Bandwidth refers to the number of signals that can be carried simultaneously on the same conductor.

There have been numerous types of LANs but ethernet is the primary network architecture for both office and plant floor. (*Architecture* refers to an organized combination of protocols and standards.)

37.2 NETWORK COMPONENTS

The four components of a network are:

1. servers (file, client, communications, print, and web);
2. transmission medium (cable or wireless);
3. network interface card (NIC), and
4. network operating system.

Application constraints, changes in networking technology, and costs affect the appropriate choices of the different types of available products. The use of different types of components has specific advantages and disadvantages in manufacturing environments. The migration from LANs to intranets also changes the types and numbers of servers and the network operating systems. The connectivity (cabling or wireless) technology is in most cases a very significant issue because manufacturing facilities are often much larger than office complexes. These longer distances require more careful planning of the connectivity system. The higher levels of electromagnetic radiation also need to be considered when planning the layout and choosing the type of conductor.

SERVERS

The file, client, and web servers are the most common servers and are important components for LANs and intranets. With the growth and implementation of technology that support the internet and intranets, web and communications servers will become more prevalent. However, print servers are becoming less common due to the availability of network boxes that interface printers to the network, and the lower cost of high-quality printers that connect directly to local computer ports.

The *file server*, the centerpiece of networks, stores program or data files for shared use. It also stores the network operating system, controls user access and security, provides redundancy in file or directory tables or registries, and performs periodic backup of data and program files. The *client server* (also called a *database server*) is important for real-time access by multiple users to any file, but most commonly databases or CAD documents. The major difference between file servers and client servers is in a user's access to a file. When a user requests a file from a file server, the entire file is downloaded to the client's workstation and only that user has access to it at that time. However, client servers retain the files and allow multiple users to access portions of the file simultaneously. This difference in access and control of files prohibits the file server from providing real-time access for multiple users. Enterprise resource planning (ERP) databases and CAD files are two examples of manufacturing files that engineers and production operations managers need to have access to in real time. Web servers, required for intranet or internet posting of an organization's web files, are a specific type of client server.

TRANSMISSION MEDIUM

Cabling was, and still is, the most common transmission medium, but wireless technology is available and appropriate for specific applications. Cabling has been made from a variety of copper conductors such as thick coaxial cable, thin coaxial cable, unshielded twisted pair (UTP) cable, and shielded twisted pair (STP) cable. Fiber-optic cable and wireless systems have been developed and have replaced some of the copper conductors. Fiber optics is the most secure medium, since the light does not have the electromagnetic fields inherent with wire or wireless communications, and the medium is the least susceptible to electromagnetic interference (EMI). UTP is the common media for local area networks in environments that are relatively free of EMI that comes from motors, transformers, and fluorescent lights. Fiber-optic or shielded cables are better for areas with high EMI. When describing the cabling for a network, the frequency is listed first as 10 or 100 baseband (unmodulated signal). For example, 10BaseT indicates a 10 megabit per second transmission rate, a twisted pair, and baseband transmission. Some devices may be used with dual frequencies and are listed as 10/100BaseT.

Twisted-pair cable capability is specified by the category of the cable. The category determines the bandwidth and distance the cable is capable of transmitting in addition to the number of twists per foot, capacitance, frequency, attenuation, and pair-to-pair near-end cross talk. *Cross talk* occurs when the signal from one wire in the twisted pair cable induces a random signal in an adjacent wire.

NETWORK INTERFACE CARD

The network interface card (NIC) connects the computer motherboard to the cabling.

Internal network interface cards are used with desktop computers while laptops use an NIC that connects to the laptop by the PCMCIA port. PCMCIA stands for Personal Computer Memory Card International Association, which promotes standards on integrated circuit cards for mobile computers. NICs have specific word lengths (16, 32, or 64 bits) and need to operate at the frequency designated by the network operating system and hardware. The network throughput increases proportionately to changes in the NIC word length and network frequency.

Network interface cards are not the only way to connect the motherboard to the cabling. Some laptops have built-in network capability. Also available are adapters that work on the universal serial bus (USB), parallel, or serial ports.

DATA TRANSMISSION

When a corporation wants remote access to its network, enterprise-wide computing, or to be connected to the internet, the local area networks need the ability to communicate beyond the network. At the least expensive and lowest performance level, plain old telephone system (POTS) lines and modems are used. This is still a prevalent technology for individual users contacting a network. While POTS lines may be used between networks or with the internet, the bandwidth is low.

Companies that use enterprise-wide computing often rely on T1 lines for data transmission. A *T1 line*, consisting of 24 channels, can transmit data at 1.544 Mbps (1.544×10^6 bits per second). While these lines are leased and costly, they provide the opportunity for greater exchanges of data, voice, and video conferencing. As corporations increase in size, have multiple geographical locations, and centralize their data processing, they tend to lease multiple T1 lines. While the T1 line is copper wire, the *T3 line* is fiber-optic cable and can support a transmission rate of 44.736 Mbps. T1 and T3 lines are expensive because of the cost of installation of cabling to the corporation by the telephone company and leasing 24-hour access. There are also less well known E1 and E3 lines, which are capable of sending data at 2.048 Mbps and 34.368 Mbps respectively.

Integrated services digital network lines (ISDN) were developed to provide an intermediate solution to the high performance and high cost of the T1 line and low performance of the modem on a POTS line. While T1 has been available wherever there were phone lines, ISDN lines have been available only in selected areas.

ISDN has never been universally available and its performance has been questioned. The standard calls for a switched line that uses a three-channel configuration of two full duplex 64 Kbps (64×10^3 bits per second) channels and one 16 Kbps channel for a total of 144 Kbps (basic rate interface or BRI). In reality, the channels are usually regulated by the providers to 56 Kbps and 16 Kbps. Divisions within the ISDN standard are BRI at 144 Kbps, primary rate interface (PRI) at 1.536 Mbps, and broadband ISDN (B-ISDN), which allows simultaneous transmission of voice, video, and data over fiber-optic lines at 155 Mbps. Dial-up ISDN voice calls, data transfer, and video conferencing are all possible over BRI with increasing capabilities available with PRI and B-ISDN. The lack of availability of the lines in many communities, their high line and supporting equipment costs, and the lower transmission rate of BRI and PRI, which has restricted their use for LAN-to-LAN connections, have minimized their implementation (Goldman 1995).

Digital subscriber lines (DSL) and digital data service (DDS) use conventional four-wire telephone lines in a digital mode. Since it is digital, a modem is not necessary. DSLs were intended to transmit data at high speed over low-cost telephone lines. DSL and DDS support speeds of 64 Kbps to 1.544 Mbps depending on the distance between the user and the provider.

Issues that determine the performance of a DSL include: (a) the distance from the telephone company's communications equipment to the user's local office or manufacturing plant; (b) the type of cable used between the communications equipment and the manufacturing plant; and (c) the services that have been sold to other subscribers running on adjacent lines.

Regardless of the technology, the central issues of how to transmit data reliably over a distance at the highest appropriate speed (bits per second or bps) and at an economical cost (communications lines, hardware, software, and support personnel) remain constant. As the technology changes from POTS to ISDN to DSL to T1 to T3 to the next levels, the central issues of communicating remotely with networks, between networks, and with the internet will also remain constant.

NETWORK OPERATING SYSTEM

An o*perating system* is the software that interfaces the user with the network and its components. Common operating systems that support ethernet architecture include Novell Netware, Windows NT, and Unix. Since each has different characteristics and applications, it is common to find at least two of them used in the same manufacturing facility.

37.3 OPEN-SYSTEMS INTERCONNECT MODEL

The open systems interconnect (OSI) seven-layer computer network model is an ideal model that provides a logical description of the various functions in computer networking. For any user, the layers should be transparent. However, a fundamental knowledge is helpful. The OSI model is illustrated in Figure 37-1.

The *physical layer* processes digital information into a form transmitted by the physical medium (wires, radio waves, or fibers). The EIA-232 C or D (RS-232C), which are cable standards, operate at the physical layer as does the network interface card when it generates the voltages and sends them over the transmission medium (cable, fiber, or radio wave). Ethernet uses baseband with the digital signal transmitted one signal at a time over the conductors. A second method, broadband, modulates the signal into a radio frequency and can handle multiplexed signals.

The *data-link layer* arranges the raw data bits of the physical layer into frames. These discrete frames are coded and form the building blocks for sending large volumes of data over the network. This level includes the access protocol such as token passing, polling, and carrier-sense multiple access with collision detection (CSMA/CD). The data-link layer provides error detection, transmits its frames to the physical layer for transmission, and receives data from the physical layer.

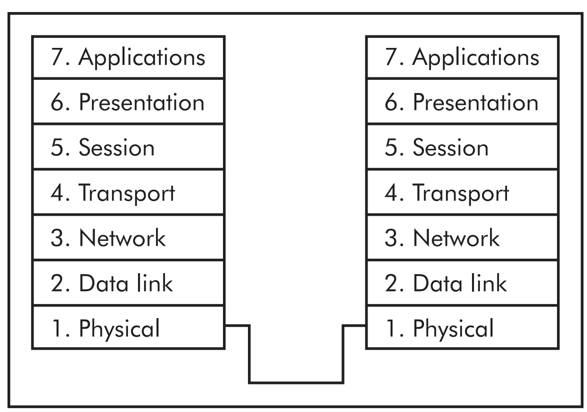

Figure 37-1. Open-systems interconnect (OSI) seven-layer model.

The *network layer* identifies the destination address of the frames and requests network facilities and priorities. This layer provides switching and routing. Addressing is of importance for computers on a network and for communication between multiple networks.

The *transport layer* verifies that data are sent and received correctly and in the correct order. A message may be routed over different paths when being transmitted across two or more networks. A portion of a message can arrive at a destination after a later portion arrives. The transport layer reads the code inserted on the frame by the data-link layer and reassembles the message in the correct order.

The *session layer* determines how two networks communicate, establishes communication, and monitors that communication.

The *presentation layer* is the interface between the application layer and the session layer. This layer has the capability to translate between different formats or codes. An example is sending a message from an IBM mainframe and receiving it on a PC over ethernet.

The *applications layer*, the level seen by users, exchanges information between the programs and the user interface.

37.4 REPEATERS, BRIDGES, ROUTERS, AND GATEWAYS

Repeaters, bridges, routers, and gateways all work at different levels of the OSI model to add capability to local area networks. *Repeaters* operate at level 1, the physical level, by receiving a signal and transmitting the same signal (repeating it). Repeaters are used to increase the overall transmission distance for the different conductors in a given network. They typically do not do error control, flow control, or address correction. Repeaters are reasonably fast because they do not process the signal. Repeaters and bridges are similar because they cannot change data or the form of the data.

Bridges enable computers on two similar but different networks to communicate with each other. Bridges transmit similar data from one network to another and filter out information that is not addressed for the other network. Bridges are used to link identical LANs to increase the range of user access. This linkage generally increases user access to file servers and application software, number of users, e-mail communications, and printing resources. Bridges store and forward frames at the data-link level (layer 2) of the OSI model.

Routers are protocol-sensitive units that support communication between dissimilar LANs (architectures) using the same protocol. Novell's SPX/IPX® or DEC's DECnet® are examples of common protocols for ethernet architecture. Routers operate at the third level of the OSI model (network layer) and communicate in packets. Routers are capable of modifying the network-specific information so that they can route a message from one type of network (for example, ethernet) to another (for example, token ring) if both are based on a common network operating system. If there are redundant routes for the flow of data from one network to another, a router is capable of selecting an appropriate path.

Gateways connect networks of different network operating systems, architectures, and protocols by translating the protocol from one to the other. They process bits at the physical layer all through error detection, framing, routing, flow control, etc., at the appropriate level from the physical through the application layers. The advantage of being able to translate and connect a network to any other network has the disadvantage of a time delay in the propagation of the message.

37.5 TOPOLOGIES

Network architecture also includes the topology of the network. LANs have both physical and logical topologies. The physical topology is the method of attaching PCs to a LAN. The three fundamental LAN physical topologies are star, ring, and bus as illustrated in Figure 37-2. The star layout is often preferred because it is often the easiest to troubleshoot if there is a failure in a cable.

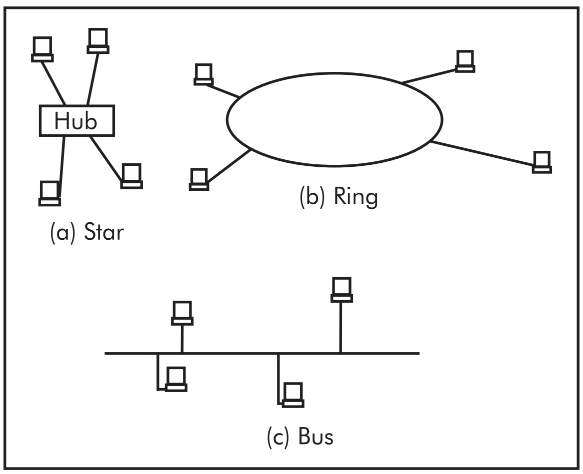

Figure 37-2. Fundamental network topologies.

Most networks today are a hybrid of at least two of the three fundamental topologies. Figure 37-3 illustrates two different hybrid topologies. Others topologies such as ring-star or bus-ring are also possible. The ease of network modification, cable installation, and cable troubleshooting makes the star-star or bus-star common configurations. A fundamental constraint of network cabling is that each type of cable has a maximum length for a given network system. While unshielded twisted pair may be used to connect hubs or hubs and a bus, greater distances can be gained by using fiber-optic cable, thinnet, or thicknet coaxial cables. Since manufacturing facilities are often very large, the design of the hybrid topology is very important for a cost-efficient installation.

37.6 PROTOCOLS

A *protocol* is the predefined manner or set of rules that a function or service is provided. Protocols regulate the data format for moving data between levels of the open-systems interconnect (OSI) model. Common protocols include network access, carrier-sense multiple access/collision detection, token passing, token-ring passing, and polling. Carrier-sense multiple access/collision detection (CSMA/CD) is used by ethernet.

The CSMA/CD protocol requires each user to wait until the line of channel is clear (idle) before he or she begins transmitting. If a data collision from two users is detected, the protocol requires that each user cease transmitting and wait a randomly determined period of time before checking for a clear line and transmitting again.

Token passing allows a workstation to transmit data (for example, save a file on the server) when the workstation holds the token. The token can be directed to the specific addresses of specific workstations more frequently than others. Token-ring messages pass through the multiple workstations, being received and re-transmitted, until the message or data arrive at the designated workstation.

Polling is the least common protocol. In polling, a central computer or host polls each specific workstation in some predetermined manner. Polling is most frequently used with host or mainframe-based systems.

The internet and intranet both require the transmission-control protocol/internet protocol (TCP/IP) suite. *Intranets* use the same technologies as the internet except they are restricted to a specific set of users. TCP/IP was originally developed by the Department of Defense (DoD) to allow different computing hardware and software to

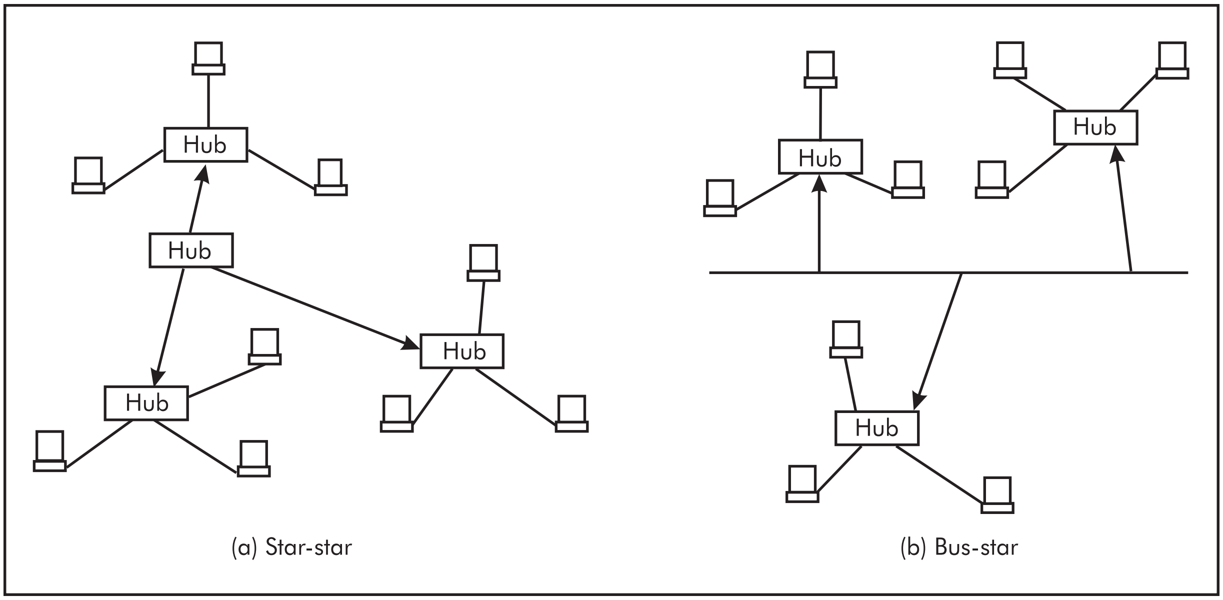

Figure 37-3. Common hybrid topologies.

communicate with each other and the DoD. TCP is used to transfer data between two internet devices. Virtual ports are used to make these connections and TCP monitors the flow of data. The *internet protocol* (IP) addresses the data and directs it to the appropriate destination. Each internet device has an IP number composed of four segments of one to three digits separated by decimal points (for example, 198.109.68.194). The *domain name system* (DNS) permits names to be coupled to the IP address. For example, www.sme.org may be used instead of 198.109.68.194 to locate the web page for the Society of Manufacturing Engineers. Since the internet has grown so rapidly, static IP addresses for specific computers are becoming a luxury. Dynamic IP addresses that are captured by a user at login to the network or internet reduce the total number of addresses required at a specific time. Dynamic IP addresses are managed by a dynamic host configuration protocol (DCHP) server. If the user wishes to upload or download a specific file to or from a server, file transfer protocol (FTP) is used. *Hypertext transfer protocol* (HTTP) is used to transfer information from web servers to web browsers.

Intranet software is required to operate an intranet. Common intranet suites are Novell® Intranetware®, Microsoft® Back Office®, and Lotus® Domino® (formerly Lotus® Notes®). The advantage of using an intranet instead of a LAN is multiple-user real-time access of multimedia, personal appointment data, e-mail, enterprise-wide computing information that is both text and graphic, access from the internet, and video conferencing. Intranets help share the corporate information in formats similar to the web. Groupware software on both the internet and intranets allow groups of people to work together.

The internet and intranets are key components in MEI wheel level 3 "shared knowledge systems (refer to Figure 36-1)." Each is instrumental in joining the customer (level 1) to the organization, to the people of the organization, and to enhance the teamwork within an organization (level 2). They are also significant in providing design and manufacturing information to level 4 for product design, manufacturing, and customer service.

REVIEW QUESTIONS

37.1) What term is used to describe the number of signals that can be carried simultaneously on the same conductor?

37.2) Which network component provides real-time access to database and CAD files?

37.3) Which type of cabling is least sensitive to electromagnetic radiation?

37.4) What piece of network hardware allows two similar but different networks to communicate with each other?

37.5) What type of fundamental LAN topology uses a central hub that each computer is connected to?

37.6) What protocol is used to transfer information from a web server to a web browser?

REFERENCE

Goldman, J.E. 1995. *Applied Data Communications*. New York: John Wiley & Sons, Inc.