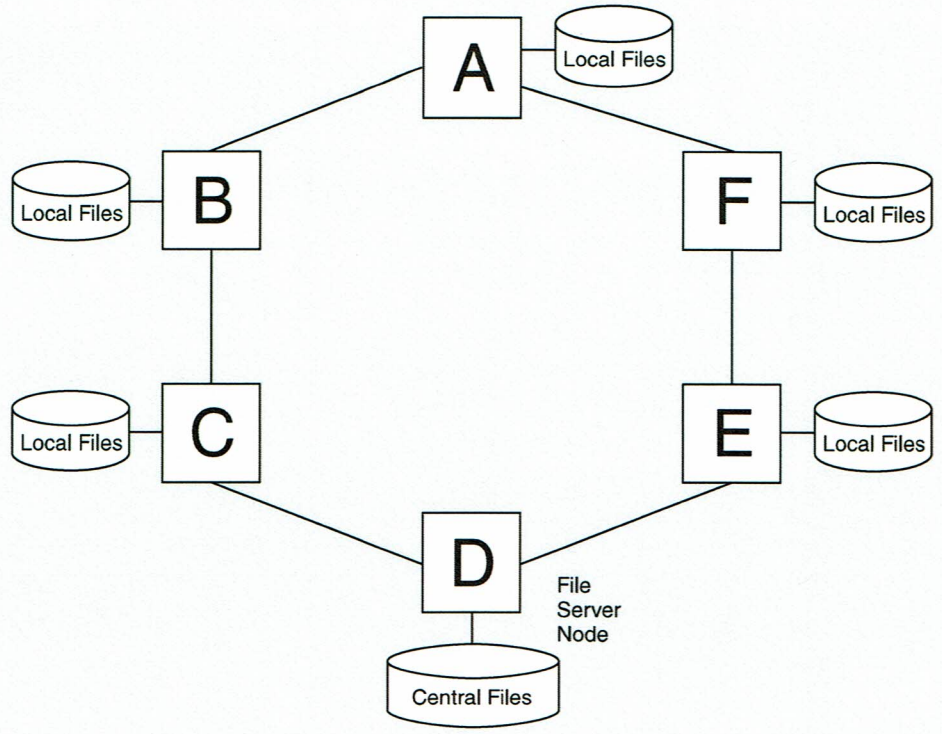
FIGURE 12-10 RING TOPOLOGY



different suppliers and customers, and each processing its own shipping and receiving transactions. In this case, where there are few common data, it is more efficient to distribute the database than to manage it centrally. However, when one warehouse has insufficient stock to fill an order, it can communicate through the network to locate the items at another warehouse.

BUS TOPOLOGY

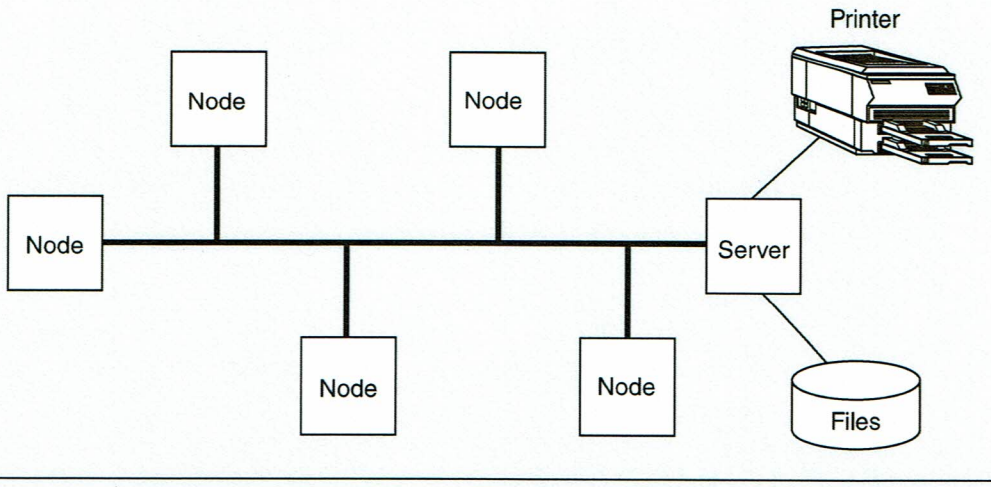
The bus topology illustrated in Figure 12-11 is the most popular LAN topology. It is so named because the nodes are all connected to a common cable—the bus. One or more servers centrally control communications and file transfers between workstations. As with the ring topology, each node on the bus has a unique address, and only one node may transmit at a time. The technique, which has been used for over two decades, is simple, reliable, and generally less costly to install than the ring topology.

CLIENT-SERVER TOPOLOGY

The term *client-server* is often misused to describe any type of network arrangement. In fact, the client-server topology has specific characteristics that distinguish it from the other topologies. Figure 12-12 illustrates the approach.

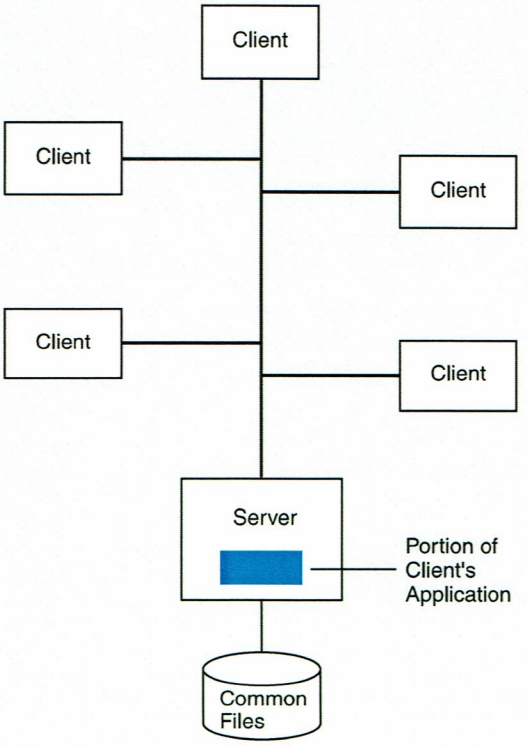
To explain the client-server difference, let's review the features of a traditional distributed data processing (DDP) system. DDP can result in considerable data traffic jams. Users competing for access to shared data files experience queues, delays, and lockouts. A factor influencing the severity of this problem is the structure of the database in use. For example, assume that User A requests a single record from a database table located at a central site. To meet this request, the file server at the central site must lock and transmit the entire table to User A. The user's application performs the search for the specific record at the remote site. When the record is updated, the entire file is then transmitted back to the central site.

FIGURE 12-11 **BUS TOPOLOGY**



The client-server model distributes the processing between User A's (client) computer and the central file server. Both computers are part of the network, but each is assigned functions that it performs best. For example, the record-searching portion of an application is placed at the server, and the data-manipulation portion is on the client computer. Thus, only a single record, rather than the entire file, must be locked and sent to the client for processing. After processing, the record is returned to the

FIGURE 12-12 **CLIENT-SERVER TOPOLOGY**



server, which restores it to the table and removes the lock. This approach reduces traffic and allows more efficient use of shared data. Distributing the record-searching logic of the client's application to the server permits other clients to access different records in the same file simultaneously. The client-server approach can be applied to any topology (e.g., ring, star, or bus). Figure 12-12 illustrates the client-server model applied to a bus topology.

Network Control

In this section, we examine methods for controlling communications between the physical devices connected to the network. Network control exists at several points in the network architecture. The majority of network control resides with software in the host computer, but control also resides in servers and terminals at the nodes and in switches located throughout the network. The purpose of network control is to perform the following tasks:

1. Establish a communications session between the sender and the receiver.
2. Manage the flow of data across the network.
3. Detect and resolve data collisions between competing nodes.
4. Detect errors in data that line failure or signal degeneration cause.

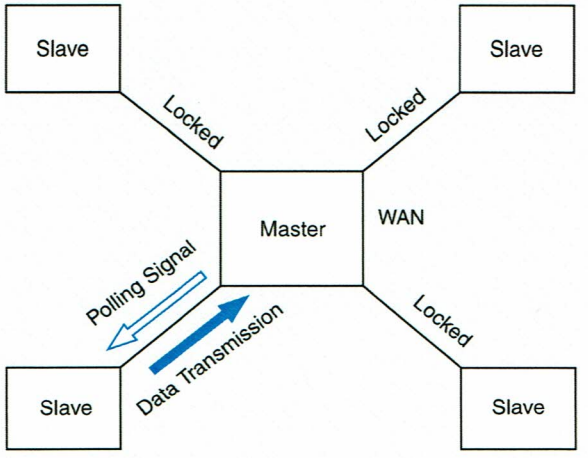
DATA COLLISION

To achieve effective network control, there must be an exclusive link or session established between a transmitting and a receiving node. Only one node at a time can transmit a message on a single line. Two or more signals transmitted simultaneously will result in a **data collision**, which destroys both messages. When this happens, the messages must be retransmitted. There are several techniques for managing sessions and controlling data collisions, but most of them are variants of three basic methods: polling, token passing, and carrier sensing.

Polling

Polling is the most popular technique for establishing a communications session in WANs. One site, designated the master, polls the slave sites to determine if they have data to transmit. If a slave responds in the affirmative, the master site locks the network while the data are transmitted. The remaining sites must wait until they are polled before they can transmit. The polling technique illustrated in Figure 12-13 is well suited to both the star and the hierarchical topologies.

FIGURE 12-13 POLLING METHOD OF CONTROLLING DATA COLLISIONS



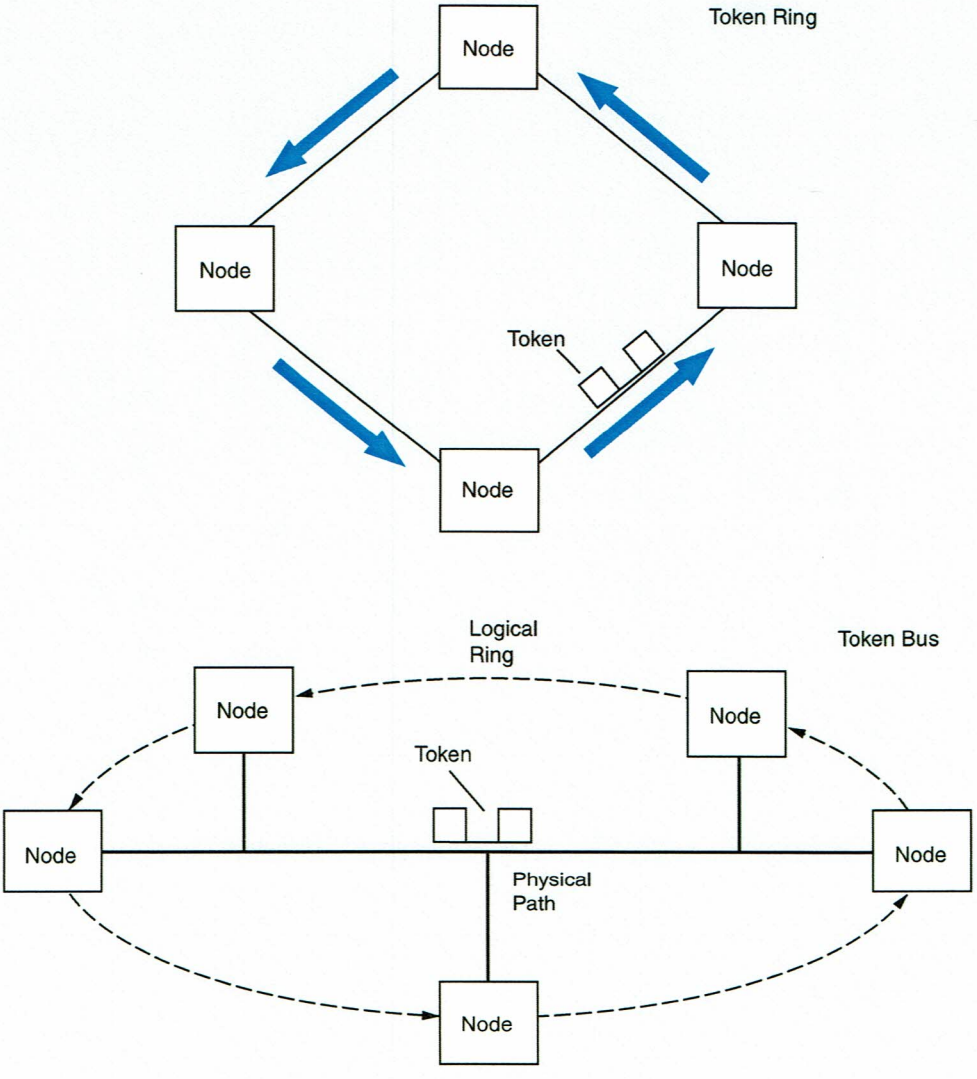
There are two primary advantages to polling. First, polling is noncontentious. Because nodes can send data only when the master node requests, two nodes can never access the network at the same time. Data collisions are, therefore, prevented. Second, an organization can set priorities for data communications across the network. Important nodes can be polled more often than less important nodes.

Token Passing

Token passing involves transmitting a special signal—the token—around the network from node to node in a specific sequence. Each node on the network receives the token, regenerates it, and passes it to the next node. Only the node possessing the token is allowed to transmit data.

Token passing can be used with either ring or bus topologies. On a ring topology, the order in which the nodes are physically connected determines the token-passing sequence. With a bus, the sequence is logical, not physical. The token is passed from node to node in a predetermined order to form a logical ring. Token bus and token ring configurations are illustrated in Figure 12-14.

FIGURE 12-14 TOKEN-PASSING APPROACH TO CONTROLLING DATA COLLISION



Because nodes are permitted to transmit only when they possess the token, the node wishing to send data across the network seizes the token upon receiving it. Holding the token blocks other nodes from transmitting and ensures that no data collisions will occur. After the transmitting node sends its message and receives an acknowledgment signal from the receiving node, it releases the token. The next node in sequence then has the option of either seizing the token and transmitting data or passing the token to the next node in the circuit.

A major advantage of token passing is its deterministic access method, which avoids data collisions. This is in contrast with the random access approach of carrier sensing (discussed in the following paragraphs). IBM's version of a token ring is emerging as an industry standard.

Carrier Sensing

Carrier sensing is a random access technique that detects collisions when they occur. This technique, which is formally labeled carrier-sensed multiple access with collision detection (CSMA7 CD), is used with the bus topology. The node wishing to transmit listens to the bus to determine if it is in use. If it senses no transmission in progress (no carrier), the node transmits its message to the receiving node. This approach is not as fail-safe as token passing. Collisions can occur when two or more nodes, unaware of each other's intent to transmit, do so simultaneously when they independently perceive the line to be clear. When this happens, the network server directs each node to wait a unique and random period of time and then retransmit the message. In a busy network, data collisions are more likely to occur; thus, it results in delays while the nodes retransmit their messages. Proponents of the token-passing approach point to its collision-avoidance characteristic as a major advantage over the CSMA/CD model.

Ethernet is the best-known LAN software that uses the CSMA/CD standard. Xerox Corporation developed the Ethernet model in the 1970s. In 1980, Digital Equipment Corporation, in a joint venture with Intel Corporation, published the specifications for a LAN based on the Ethernet model. The greatest advantage of Ethernet is that it is established and reliable, and network specialists understand it well. Ethernet also has a number of economic advantages over token ring: (1) the technology, being relatively simple, is well suited to the less costly twisted-pair cabling, whereas token ring works best with more expensive coaxial cable; (2) the network interface cards Ethernet uses are much less expensive than those used in the token ring topology; and (3) Ethernet uses a bus topology, which is easier to expand.

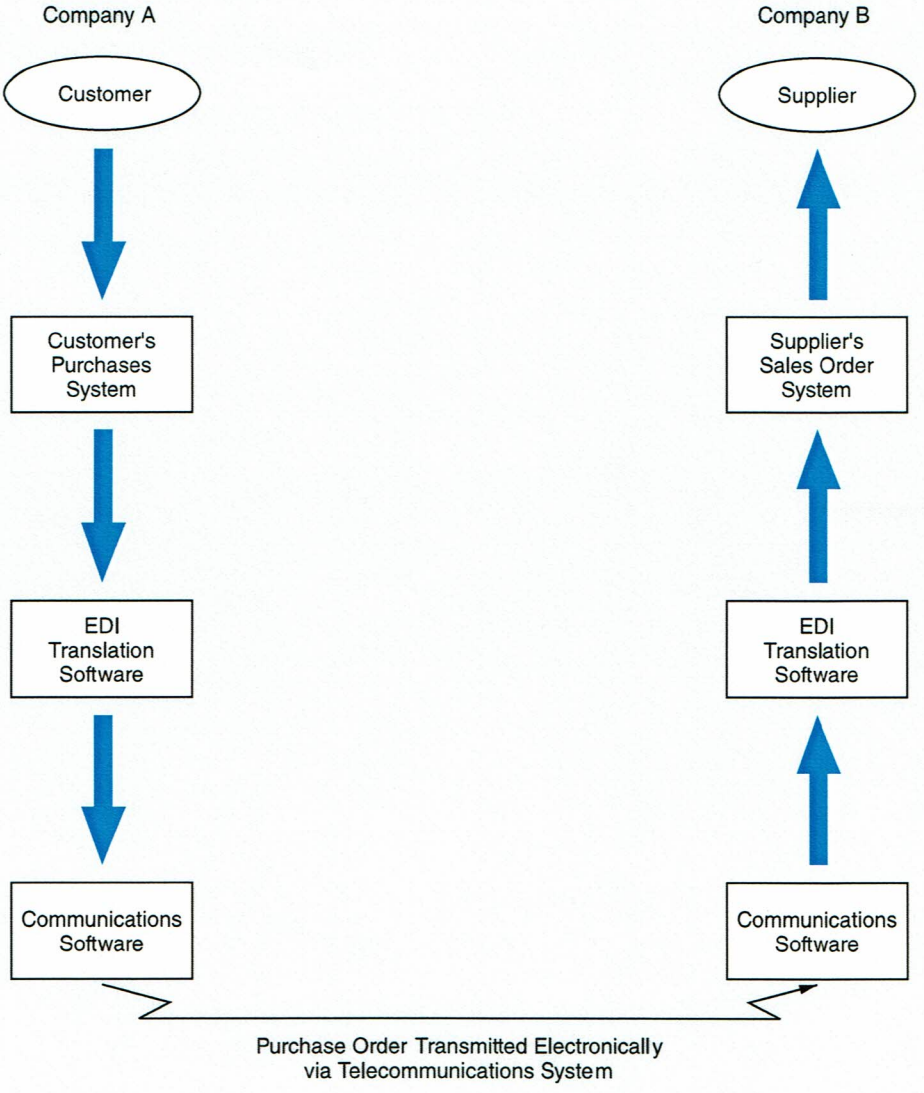
Electronic Data Interchange (EDI)

To coordinate sales and production operations and to maintain an uninterrupted flow of raw materials, many organizations enter into a trading partner agreement with their suppliers and customers. This agreement is the foundation for a fully automated business process called **Electronic Data Interchange (EDI).** A general definition of EDI is:

The intercompany exchange of computer-processible business information in standard format.

The definition reveals several important features of EDI. First, EDI is an inter-organization endeavor. A firm does not engage in EDI on its own. Second, the information systems of the trading partners automatically process the transaction. In a pure EDI environment, there are no human intermediaries to approve or authorize transactions. Authorizations, mutual obligations, and business practices that apply to transactions are all specified in advance under the trading partner agreement. Third, transaction information is transmitted in a standardized format. Therefore, firms with different internal systems can exchange information and do business. Figure 12-15 shows an overview of an EDI connection between two companies. Assume that the transaction in Figure 12-15 is the customer's (Company A) inventory purchase from the supplier (Company B). Company A's purchases system automatically creates an electronic purchase order (PO), which it sends to its translation software. Here, the PO is converted to a standard format electronic message

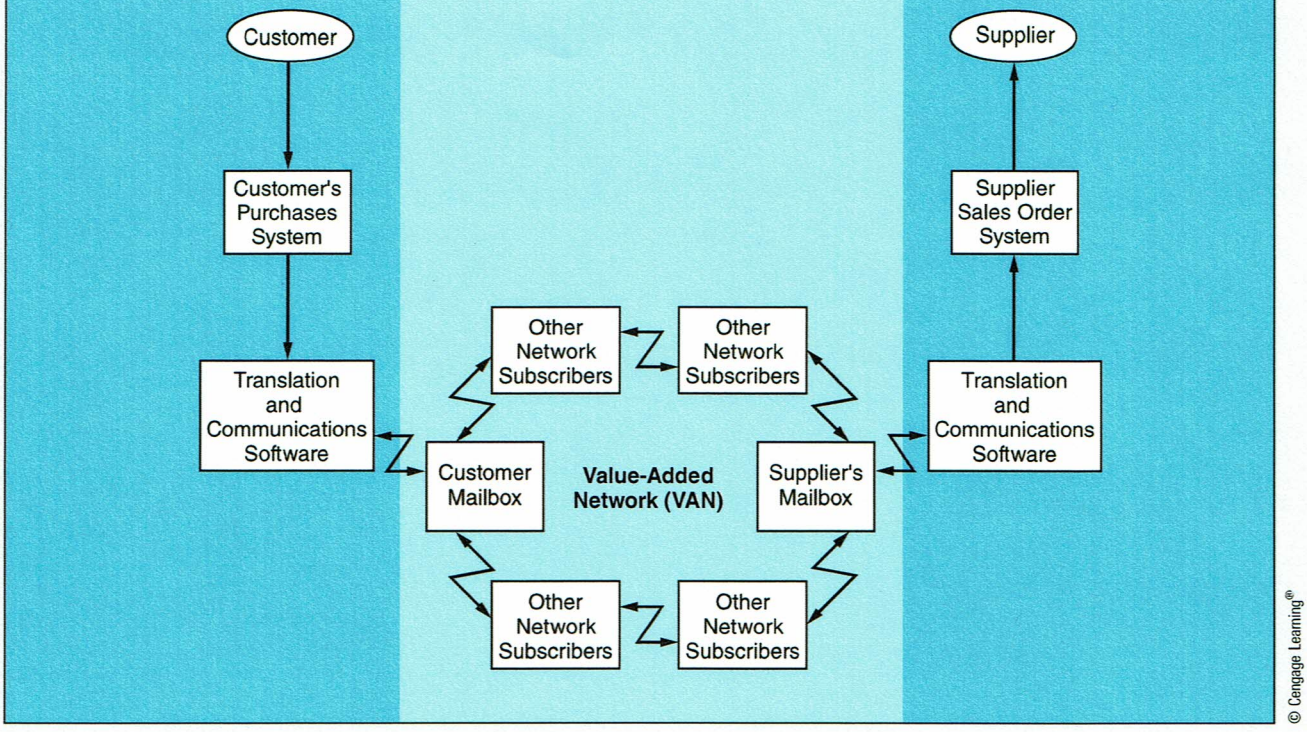
FIGURE 12-15 OVERVIEW OF EDI



ready for transmission. The message is transmitted to Company B's translation software, where it is converted to the supplier's internal format. Company B's sales order processing system receives the customer order, which it processes automatically.

Figure 12-15 shows a direct communications link between companies. But many companies choose to use a third-party VAN to connect to their trading partners. Figure 12-16 illustrates this arrangement. The originating company transmits its EDI messages to the network rather than directly to the trading partner's computer. The network directs each EDI transmission to its destination and deposits the message in the appropriate electronic mailbox. The messages stay in the mailboxes until the receiving companies' systems retrieve them. The network is a VAN because it provides service by managing the distribution of the messages between trading partners. VANs can also provide an important degree of control over EDI transactions. We examine EDI control issues in Chapter 16.

FIGURE 12-16 VALUE-ADDED NETWORK AND EDI



EDI STANDARDS

Key to EDI success is the use of a standard format for messaging between dissimilar systems. Over the years, both in the United States and internationally, a number of formats have been proposed. The standard in the United States is the American National Standards Institute (ANSI) X.12 format. The standard used internationally is the EDI For Administration, Commerce, and Transport (EDIFACT) format. Figure 12-17 illustrates the X.12 format.

The electronic envelope contains the electronic address of the receiver, communications protocols, and control information. This is the electronic equivalent of a traditional paper envelope. A functional group is a collection of transaction sets (electronic documents) for a particular business application, such as a group of sales invoices or purchase orders. The transaction set is the electronic document and is composed of data segments and data elements. Figure 12-18 relates these terms to a conventional document.

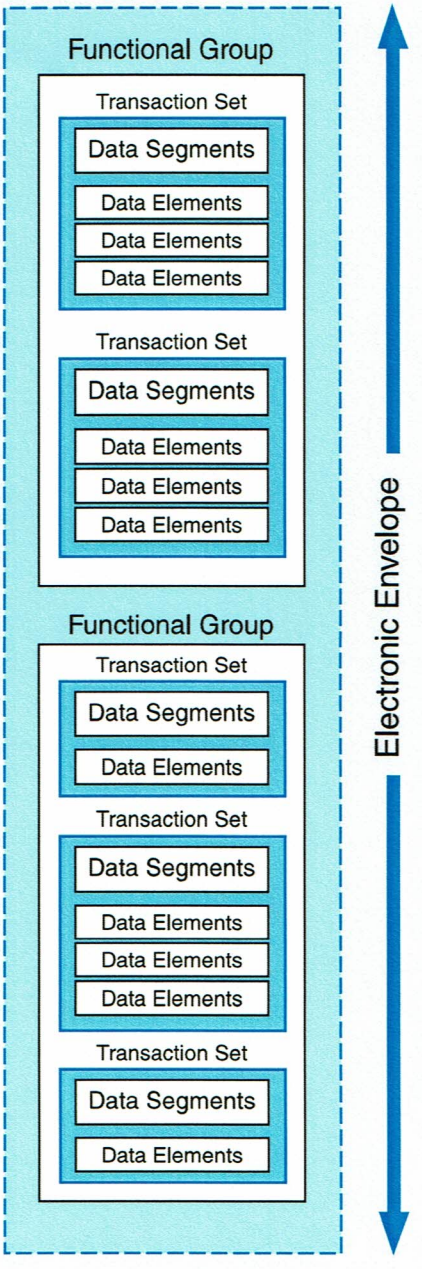
Each data segment is an information category on the document, such as part number, unit price, or vendor name. The data elements are specific items of data related to a segment. In the example in Figure 12-18, these include such items as REX-446, $127.86, and Ozment Supply.

BENEFITS OF EDI

EDI has made considerable inroads in a number of industries, including automotive, groceries, retail, health care, and electronics. The following are some common EDI cost savings that justify the approach.

- *Data keying*. EDI reduces or even eliminates the need for data entry.
- *Error reduction*. Firms using EDI see reductions in data keying errors, human interpretation and classification errors, and filing (lost document) errors.

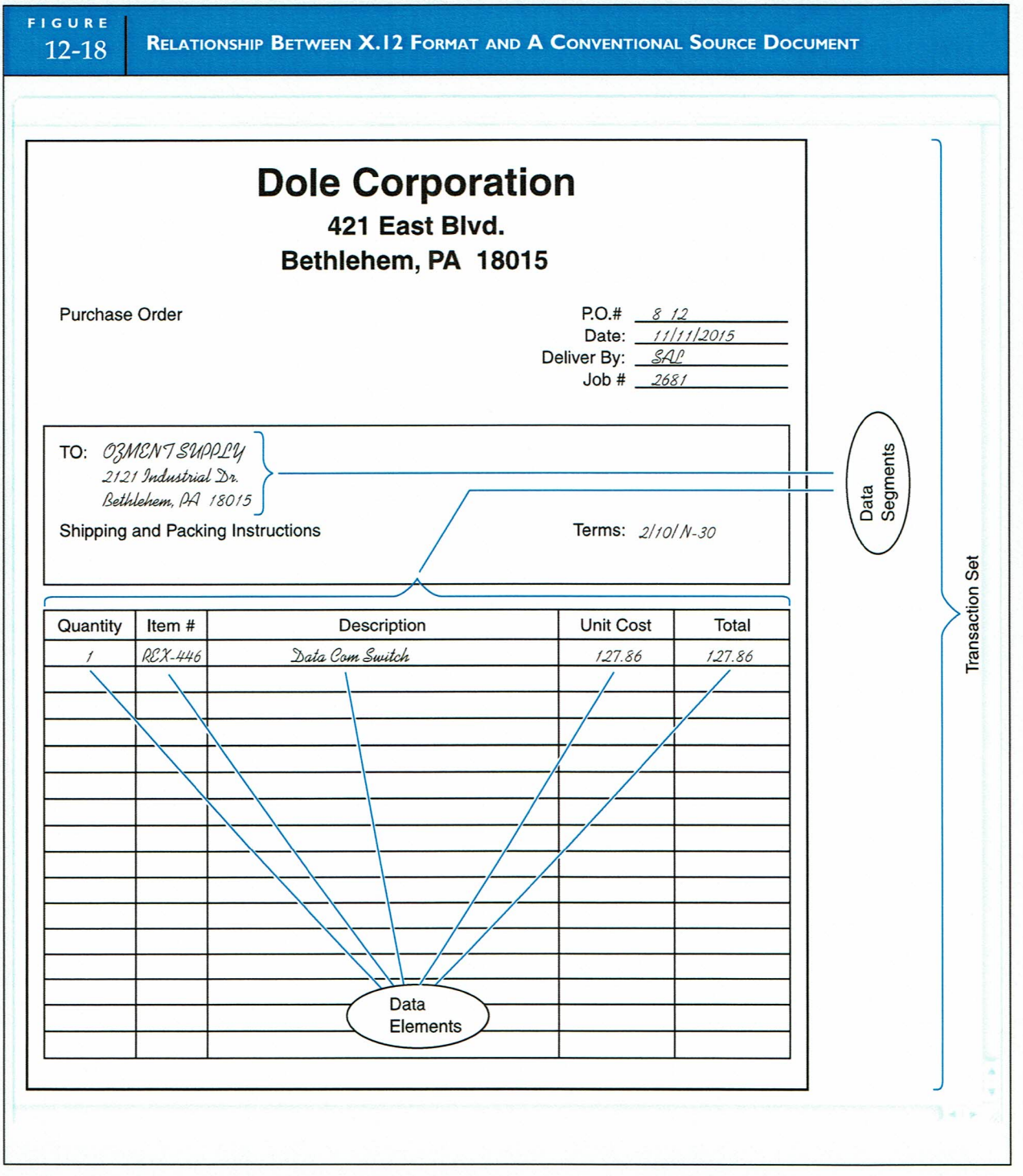
FIGURE 12-17 THE X.12 FORMAT



Source: *B. K. Stone, One to Get Ready: How to Prepare Your Company for EDI* (CoreStates, 1988): 1212.

- *Reduction of paper*. The use of electronic envelopes and documents reduces drastically the paper forms in the system.
- *Postage*. Mailed documents are replaced with much cheaper data transmissions.
- *Automated procedures*. EDI automates manual activities associated with purchasing, sales order processing, cash disbursements, and cash receipts.
- *Inventory reduction*. By ordering directly as needed from vendors, EDI reduces the lag time that promotes inventory accumulation.

FIGURE 12-18 RELATIONSHIP BETWEEN X.12 FORMAT AND A CONVENTIONAL SOURCE DOCUMENT

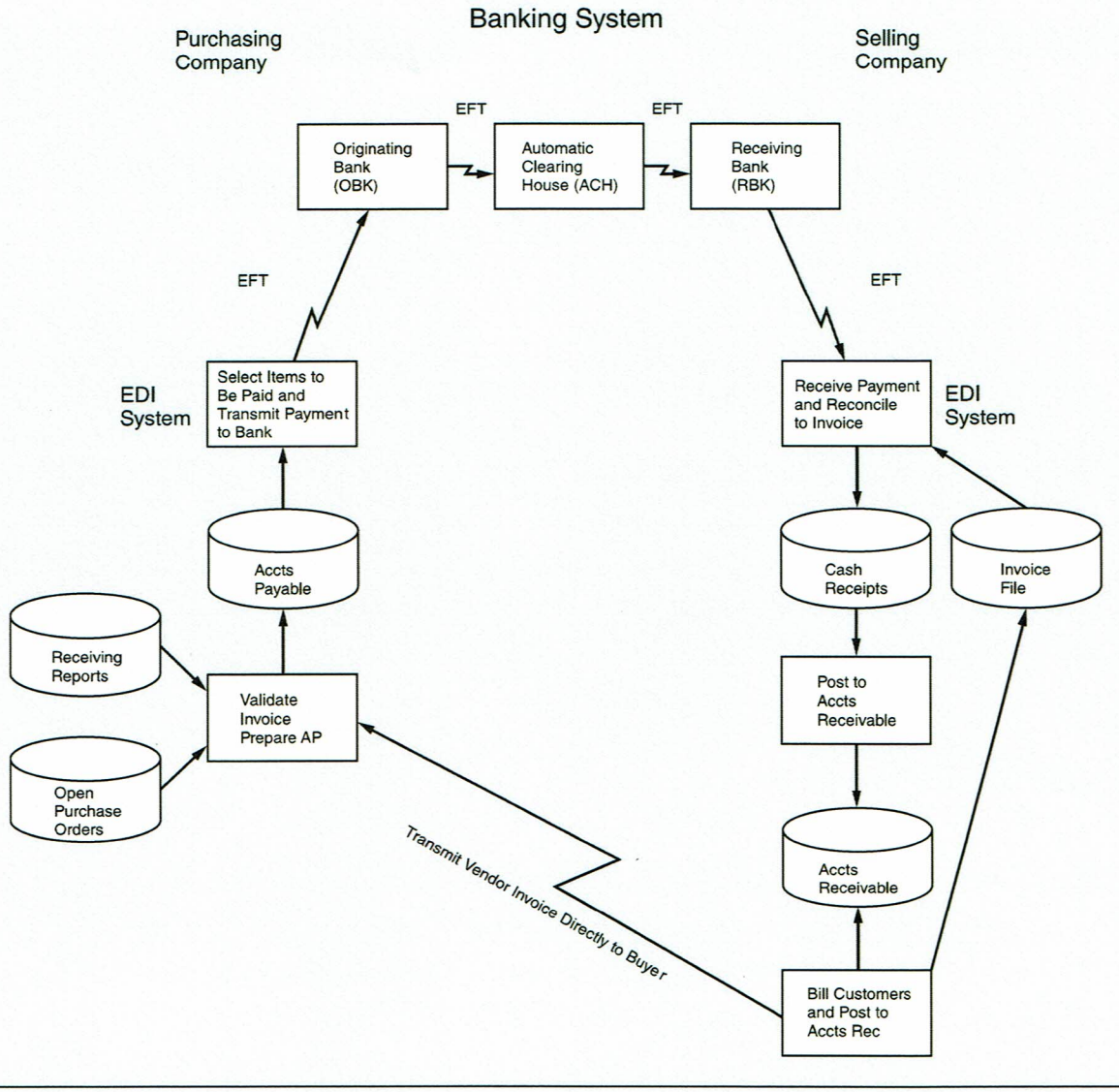


Source: J. M. Cathey, "Electronic Data Interchange: What the Controller Should Know," *Management Accounting* (November 1991): 4.

FINANCIAL EDI

Using electronic funds transfer (EFT) for cash disbursement and cash receipts processing is more complicated than using EDI for purchasing and selling activities. EFT requires intermediary banks between trading partners. This arrangement is shown in Figure 12-19. The buyer's EDI system receives the purchase invoices and automatically approves them for payment. On the payment date, the buyer's system automatically makes an EFT to its originating bank (OBK). The OBK

FIGURE 12-19 **EFT Transactions between Trading Partners**



removes funds from the buyer's account and transmits them electronically to the automatic clearing house (ACH) bank. The ACH is a central bank that carries accounts for its member banks. The ACH transfers the funds from the OBK to the receiving bank (RBK), which in turn applies the funds to the seller's account.

Transferring funds by EFT poses no special problem. A check can easily be represented within the X.12 format. The problem arises with the remittance advice information that accompanies the check. Remittance advice information is often quite extensive because of complexities in the transaction. The check may be in payment of multiple invoices or only a partial invoice. There may be disputed amounts because of price disagreements, damaged goods, or incomplete deliveries. In traditional systems, modifying the remittance advice and/or attaching a letter explaining the payment resolves these disputes.

Converting remittance information to electronic form can result in very large records. Members of the ACH system are required to accept and process only EFT formats limited to 94 characters of data—a record size sufficient for only very basic messages. Not all banks in the ACH system support the ANSI standard format for remittances, ANSI 820. In such cases, remittance information must be sent to the seller by separate EDI transmission or conventional mail. The seller must

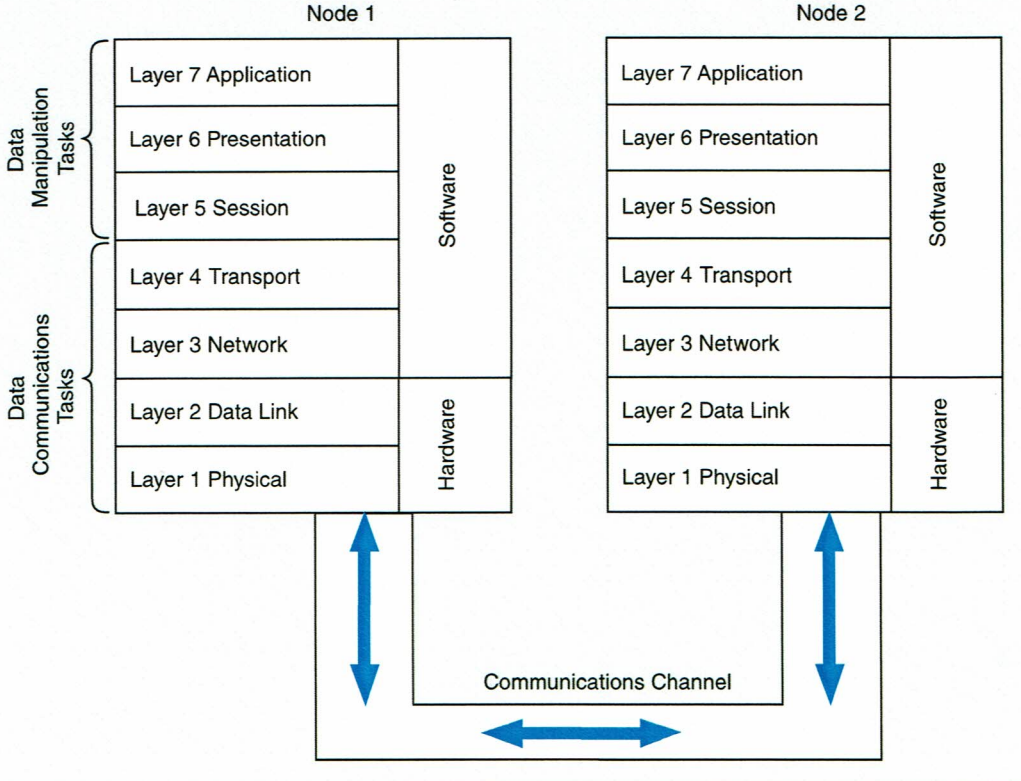
then implement separate procedures to match bank and customer EDI transmissions in applying payments to customer accounts.

Recognizing the void between services demanded and those the ACH system supplies, many banks have established themselves as value-added banks (VABs) to compete for this market. A VAB can accept electronic disbursements and remittance advices from its clients in any format. It converts EDI transactions to the ANSI X.12 and 820 formats for electronic processing. In the case of non-EDI transactions, the VAB writes traditional checks to the creditor. The services VABs offer allow their clients to employ a single cash disbursement system that can accommodate both EDI and non-EDI customers.

Open System Interface (OSI) Network Protocol

The OSI model provides standards by which the products of different manufacturers can interface with one another in a seamless interconnection at the user level. Figure 12-20 shows the seven-layer OSI model. The OSI standard has the following general features. First, each layer in the model is independent, which allows the development of separate protocols specifically for each layer. Second, the layers at each node communicate logically with their counterpart layers across nodes. The physical flow of data and parameters pass between layers. Each layer performs specific subtasks that support the layer above it and are in turn supported by the layer below it. Third, the model distinguishes between the tasks of data communications and data manipulation. The first four layers are dedicated to data communications tasks, which are a function of hardware devices and special software. The last three layers support data manipulation, which is a function of user applications and operating systems. The specific function of each layer is described in the following paragraphs.

FIGURE 12-20 THE OSI PROTOCOL



LAYER FUNCTIONS

Physical Layer

The physical layer, the first and lowest level in the protocol, defines standards for the physical interconnection of devices to the electronic circuit. This level is concerned with pin connections to devices, the wiring of workstations, and cabling standards. An example of a standard at this layer is the RS-232 connector cable that virtually all microcomputer manufacturers use.

Data Link Layer

Data link layer protocols are concerned with the transmission of packets of data from node to node based on the workstation address. This includes message origination, acknowledgment of message receipt, and error detection and retransmission.

Network Layer

Network layer protocols deal with the routing and relaying of data to different LANs and WANs based on the network address. They specify how to identify nodes on a network and regulate the sequencing of messages to the nodes. In addition, this third layer describes how packet data are transferred between networks with different architectures, which permits the synchronization of data.

Transport Layer

The purpose of the transport layer is to ensure delivery of the entire file or message across individual networks and multiple networks, regardless of the number and type of dissimilar devices involved. If a transmission error is detected, this layer defines the retransmission methods to ensure the complete and accurate delivery of the message.

In addition, the transport layer seeks the connection between users that best meets the users' needs for message packeting and multiplexing messages. These protocols provide the logic for segmenting long messages into smaller units and, at the receiving end, reassembling the packets into the original message.

Session Layer

A session layer is a specific connection between two users or entities on the network. The purpose of this layer is to guarantee a correct and synchronized connection. At this level, the protocols for starting a session may require a user password to establish the legitimacy of the connection. Protocols may also determine priorities of sessions and rules for interrupting and reestablishing the session. For example, a transmission of higher priority may interrupt the transmission of a large document. Session protocols define the rules for such interruptions and the procedures for resuming the original transmission.

Presentation Layer

In the presentation layer, data in transit are often in a format that is very different from what the user's application requires. During transmission, data may be compressed to increase transfer speeds, blocked for efficiency, and encrypted for security. Presentation protocols provide the rules for editing, formatting, converting, and displaying data to the user's system.

Application Layer

The application layer provides the overall environment for the user or the user's application to access the network. This layer provides what are called common application services. These services—common to all communicating applications—include protocols for network management, file transfer, and e-mail. The uniqueness of user applications makes this layer the least amenable

to general standards. By their very nature, protocols at this level impinge upon application structure and function. Consequently, these are the least rigorously defined rules. Most of the protocols here tend to be vendor defined. For example, an individual vendor's database management system may provide the application layer protocols for managing file transfers.

Key Terms

Advanced encryption standard (AES) (519)
algorithm (519)
application-level firewall (521)
botnets (515)
caesar cipher (519)
certification authorities (521)
cloud computing (508)
cookies (514)
data collision (532)
denial of service attack (DoS) (514)
digital certificate (521)
digital envelope (519)
digital signature (519)
distributed denial of service (DDoS) (515)
distribution level (508)
document name (504)
domain name (504)
dynamic virtual organization (510)
Electronic Data Interchange (EDI) (534)
extranet (503)
File Transfer Protocol (FTP) (506)
firewall (521)
home page (504)
HyperText Markup Language (HTML) (503)
HyperText Transfer Protocol (HTTP) (504)
HyperText Transport Protocol-Next Generation (HTTP-NG) (507)
information level (508)
Infrastructure-as-a-Service (IaaS) (509)
intelligent control agents (524)
International Standards Organization (506)
Internet Message Access Protocol (507)
Internet Relay Chat (IRC) (515)
IP broadcast address (515)
IP spoofing (514)
key (519)
Network News Transfer Protocol (NNTP) (507)
network virtualization (510)
network-level firewall (521)
Open System Interface (OSI) (506)
packet switching (502)
ping (515)
platform-as-a-Service (PaaS) (509)
polling (532)
Post Office Protocol (507)
privacy (523)
Privacy Enhanced Mail (PEM) (507)
Private Communications Technology (PCT) (507)
private key (519)
protocol (505)
protocol prefix (504)
public key encryption (519)
public key infrastructure (PKI) (521)
risk (512)
Rivest-Shamir-Adleman (RSA) (519)
Safe Harbor Agreement (523)
Secure Electronic Transmission (507)
Secure Sockets Layer (SSL) (507)
Simple Network Mail Protocol (SNMP) (507)
Smurf attack (515)
Software-as-a-Service (SaaS) (509)
storage virtualization (510)
Subdirectory name (504)
symmetric key (519)
SYN flood attack (515)
SYNchronize-ACKnowledge (SYN-ACK) (514)
TELNET (506)
transaction level (508)
Transfer Control Protocol/Internet Protocol (TCP/IP) (506)
Uniform Resource Locator (URL) (504)
value-added network (VAN) (524)
virtualization (509)
virtual private network (VPN) (503)
web page (503)
websites (504)
zombie (515)