Chapter 12

# Electronic Commerce Systems

**LEARNING OBJECTIVES**

*After studying this chapter, you should:*

- Be acquainted with the topologies that are employed to achieve connectivity across the Internet.
- Possess a conceptual appreciation of protocols and understand the specific purposes that several Internet protocols serve.
- Understand the business benefits associated with Internet commerce and be aware of several Internet business models.
- Be familiar with the risks associated with intranet and Internet electronic commerce.
- Understand issues of security, assurance, and trust pertaining to electronic commerce.
- Be familiar with the electronic commerce implications for the accounting profession.

Upon hearing the term *electronic commerce*, many people think of browsing an electronic catalog on the web or going Internet shopping at a virtual mall. While this may be the predominate component of electronic commerce, it is not the entire story.

Electronic commerce involves the electronic processing and transmission of data. This broad definition encompasses many diverse activities, including the electronic buying and selling of goods and services, online delivery of digital products, electronic funds transfer (EFT), electronic trading of stocks, and direct consumer marketing. Electronic commerce is not an entirely new phenomenon; many companies have engaged in electronic data interchange (EDI) over private networks for decades.

Driven by the Internet revolution, however, electronic commerce has dramatically expanded and undergone radical changes in recent years. This fast-moving environment has engendered an array of innovative markets and trading communities. While electronic commerce promises enormous opportunities for consumers and businesses, its effective implementation and control are urgent challenges facing organization management and accountants.

To properly evaluate the potential exposures and risks in this environment, the modern accountant must be familiar with the technologies and techniques that underlie electronic commerce. Hardware failures, software errors, and unauthorized access from remote locations can expose the organization's accounting system to unique threats. For example, transactions can be lost in transit and never processed, digitally altered to change their financial effect, corrupted by transient signals on transmission lines, and diverted to or initiated by the perpetrator of a fraud.

In this chapter and its appendix, we consider three aspects of electronic commerce: (1) the intra-organizational use of networks to support distributed data processing; (2) business-to-business transactions conducted via Electronic Data Interchange (EDI) systems; and (3) Internet-based commerce including business-to-consumer and business-to-business relationships. We examine the technologies, topologies, and applications of electronic commerce in each of these areas. We review the risks associated with electronic commerce, examine security and assurance techniques used to reduce risk and promote trust, and conclude with a discussion of electronic commerce's implications for the accounting profession.

# Intra-Organizational Networks and EDI

Local area networks (LANs), wide area networks (WANs), and EDI are electronic commerce technologies that have been with us for decades. As such, these topics are frequently found among the subject matter of introductory information technology courses. Because many accounting and information systems students become familiar with these topics before taking an AIS course, this material is covered in the chapter's appendix. The body of the chapter focuses on the salient issues pertaining to Internet-based electronic commerce. Students who have not been exposed to network and EDI topologies and technologies, however, should review the appendix before proceeding, as the treatment in the chapter presumes this background.

# Internet Commerce

Internet commerce has enabled thousands of business enterprises of all sizes, as well as millions of consumers, to congregate and interact in a worldwide virtual shopping mall. Along with enormous opportunities, however, the electronic marketplace has engendered unique risks. This section of the chapter examines the technologies, benefits, risks, and security issues associated with Internet commerce.

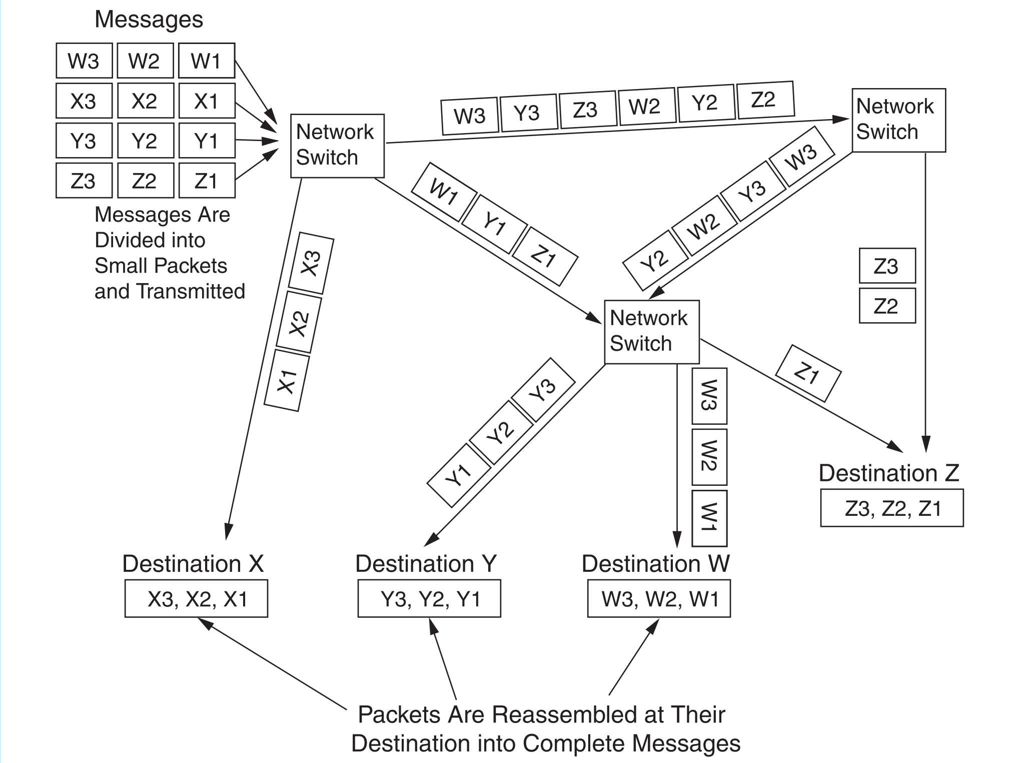
## Internet Technologies

The Internet was originally developed for the U.S. military and later became used widely for academic and government research. Over recent years, it has evolved into a worldwide information highway. This growth is attributed to three factors. First, in 1995, national commercial telecommunications companies such as MCI, Sprint, and UUNET took control of the backbone elements of the Internet and have continued to enhance their infrastructures. Large Internet service providers (ISPs) can link into these backbones to connect their subscribers, and smaller ISPs can connect directly to the national backbones or into one of the larger ISPs. Second, online services like CompuServe and AOL connect to the Internet for e-mail, which enables users of different services to communicate with each other. Third, the development of graphics-based web browsers, such as Microsoft's Internet Explorer, has made accessing the Internet a simple task. The Internet thus became the domain of everyday people with PCs rather than just scientists and computer hackers. As a result, the web has grown exponentially and continues to grow daily.

### *Packet Switching*

The Internet employs communications technologies based on **packet switching**. Figure 12-1 illustrates this technique, whereby messages are divided into small packets for transmission.

FIGURE 12-1 Message Packet Switching



Individual packets of the same message may take different routes to their destinations. Each packet contains address and sequencing codes so they can be reassembled into the original complete message at the receiving end. The choice of transmission path is determined according to criteria that achieve optimum utilization of the long-distance lines, including the degree of traffic congestion on the line, the shortest path between the end points, and the line status of the path (that is, working, failed, or experiencing errors). Network switches provide a physical connection for the addressed packets only for the duration of the message; the line then becomes available to other users. The first international standard for wide area packet switching networks was X.25, which was defined when all circuits were analog and very susceptible to noise. Subsequent packet technologies, such as frame relay and SMDS (Switched Multimegabit Data Service) were designed for today's almost error-free digital lines.

## *Virtual Private Networks*

A **virtual private network** (VPN) is a private network within a public network. For years, common carriers have built VPNs, which are private from the client's perspective, but physically share backbone trunks with other users. VPNs have been built on X.25 and frame-relay technologies. Today, Internet-based VPNs are of great interest. Maintaining security and privacy in this setting, however, requires encryption and authentication controls discussed later in the chapter.

## *Extranets*

Another variant on Internet technology is the **extranet**. This is a password-controlled network for private users rather than the general public. Extranets are used to provide access between trading partner internal databases. Internet sites containing information intended for private consumption frequently use an extranet configuration.

## *World Wide Web*

The World Wide Web (web) is an Internet facility that links user sites locally and around the world. In 1989, Tim Berners-Lee of the European Center for Nuclear Research (CERN) in Geneva developed the web as a means of sharing nuclear research information over the Internet. The fundamental format for the web is a text document called a **web page** that has embedded HyperText Markup Language (HTML) codes that provide the formatting for the page as well as hypertext links to other pages. The linked pages may be stored on the same server or anywhere in the world. HTML codes are simple alphanumeric characters that can be typed with a text editor or word processor. Most word processors support web publishing features that allow text documents to be converted to HTML format.

Web pages are maintained at **websites**, which are computer servers that support **HyperText Transfer Protocol (HTTP).** The pages are accessed and read via a web browser such as Internet Explorer. To access a website, the user enters the **Uniform Resource Locator (URL)** address of the target site in the web browser. When an Internet user visits a website, his or her point of entry is typically the site's **home page**. This HTML document serves as a directory to the site's contents and other pages. Through browsers, the web provides point-and-click access to the largest collection of online information in the world. The web has also become a multimedia delivery system that supports audio, video, videoconferencing, and 3-D animation. The ease of web page creation and navigation via browsers has driven the unprecedented growth of the web. In 1994, there were approximately 500 websites in the world; today there are millions.

## *Internet Addresses*

The Internet uses three types of addresses for communications: (1) e-mail addresses, (2) website URL addresses, and (3) internet protocol (IP) addresses of individual computers attached to a network.

***E-mail Address.*** The format for an e-mail address is USER NAME@DOMAIN NAME. For example, the address of the author of this textbook is jah0@lehigh.edu. There are no spaces between any of the words. The user name (or in this case, the user ID) is jah0. A domain name is an organization's unique name combined with a top-level domain (TLD) name. In the example above, the unique name is lehigh and the TLD is edu. Following are examples of TLD names:

| | |
|---|---|
| .com | commercial |
| .net | network provider |
| .org | nonprofit organization |
| .edu | education and research |
| .gov | government |
| .mil | military agency |
| .int | international intergovernmental |

Outside of the United States, the TLD names consist of the country code, such as .uk for the United Kingdom and .es for Spain. The Internet Ad Hoc Committee (IAHC) has introduced a category called a generic top-level domain (gTLD), which includes the following:

| | |
|---|---|
| .firm | a business |
| .store | goods for sale |
| .web | WWW activities |
| .arts | culture/entertainment |

| | |
|---|---|
| .rec | recreation/entertainment |
| .info | information service |
| .nom | individual/personal |

The Internet e-mail addressing system allows the user to send e-mail directly to the mailboxes of users of all major online services, such as America Online and CompuServe.

***URL Address.*** The URL is the address that defines the path to a facility or file on the web. URLs are typed into the browser to access website home pages and individual web pages and can be embedded in web pages to provide hypertext links to other pages. The general format for a URL is **protocol prefix**, **domain name**, **subdirectory name**, and **document name**. The entire URL is not always needed. For example, to access the South-Western Publishing home page, only the following protocol and domain name are required:

http://www.academic.cengage.com

The protocol prefix is http:// and the domain name is www.academic.cengage.com. From this home page, the user can activate hyperlinks to other pages as desired. The user can go directly to a linked page by providing the complete address and separating the address components with slashes. For example,

http:// www.academic.cengage.com/accounting/hall

Subdirectories can be several levels deep. To reference them, each must be separated with a slash. For example, the elements of the following URL for a hypothetical sporting goods company are described below.

http://www.flyfish.com/equipment/rods/brand_name.html

| | |
|---|---|
| http:// | protocol prefix (most browsers default to HTTP if a prefix is not typed) |
| www.flyfish.com/ | domain name |
| equipment/ | subdirectory name |
| rods/ | subdirectory name |
| brand_name.html | document name (web page) |

***IP Address.*** Every computer node and host attached to the Internet must have a unique Internet protocol (IP) address. For a message to be sent, the IP addresses of both the sending and the recipient nodes must be provided. Currently, IP addresses are represented by a 32-bit data packet. The general format is four sets of numbers separated by periods. The decomposition of the code into its component parts varies depending on the class to which it is assigned. Class A, class B, and class C coding schemes are used for large, medium, and small networks, respectively. To illustrate the coding technique, the IP address 128.180.94.109 translates into:

| | |
|---|---|
| 128.180 | Lehigh University |
| 94 | Business Department faculty server |
| 109 | A faculty member's office computer (node) |

## Protocols

The word **protocol** has been used several times in this section. Let's now take a closer look at the meaning of this term. Protocols are the rules and standards governing the design of hardware and software that permit users of networks, which different vendors have manufactured, to communicate and share data. The general acceptance of protocols within the network community provides both standards and economic incentives for the manufacturers of hardware and software. Products that do not comply with prevailing protocols will have little value to prospective customers.

The data communications industry borrowed the term *protocol* from the diplomatic community. Diplomatic protocols define the rules by which the representatives of nations communicate and collaborate during social and official functions. These formal rules of conduct are intended to avoid international problems that could arise through the misinterpretation of ambiguous signals passed between diplomatic counterparts. The greatest potential for error naturally exists between nations with vastly dissimilar cultures and conventions for behavior. Establishing a standard of conduct through protocols, which all members of the diplomatic community understand and practice, minimizes the risk of miscommunications between nations of different cultures.

An analogy may be drawn to data communications. A communications network is a community of computer users who also must establish and maintain unambiguous lines of communication. If all network members had homogeneous needs and operated identical systems, this would not be much of a problem; however, networks are characterized by heterogeneous systems components. Typically, network users employ hardware devices (PC, printers, monitors, data storage devices, modems, and so on) and software (user applications, network control programs, and operating systems) that a variety of vendors produce. Passing messages effectively from device to device in such a multivendor environment requires ground rules or protocols.

## What Functions Do Protocols Perform?

Protocols serve network functions in several ways.[1] First, they facilitate the physical connection between the network devices. Through protocols, devices are able to identify themselves to other devices as legitimate network entities and initiate (or terminate) a communications session.

Second, protocols synchronize the transfer of data between physical devices. This involves defining the rules for initiating a message, determining the data transfer rate between devices, and acknowledging message receipt.

Third, protocols provide a basis for error checking and measuring network performance. This is done by comparing measured results against expectations. For example, performance measures pertaining to storage device access times, data transmission rates, and modulation frequencies are critical to controlling the network's function. Thus, the identification and correction of errors depends on protocol standards that define acceptable performance.

Fourth, protocols promote compatibility among network devices. To transmit and receive data successfully, the various devices involved in a particular session must conform to a mutually acceptable mode of operation, such as synchronous, asynchronous and duplex, or half-duplex. Without protocols to provide such conformity, messages sent between devices will be distorted and garbled.

Finally, protocols promote network designs that are flexible, expandable, and cost effective. Users are free to change and enhance their systems by selecting from the best offerings of a variety of vendors. Manufacturers must, of course, construct these products in accordance with established protocols.

[1] H. M. Kibirige, *Local Area Networks in Information Management* (Greenwood Press, 1989).

### *The Layered Approach to Network Protocol*

The first networks used several different protocols that emerged in a rather haphazard manner. These protocols often provided poor interfaces between devices that actually resulted in incompatibilities. Also, early protocols were structured and inflexible, thus limiting network growth by making system changes difficult. A change in the architecture at a node on the network could have an unpredictable effect on an unrelated device at another node. Technical problems such as these can translate into unrecorded transactions, destroyed audit trails, and corrupted databases. Out of this situation emerged the contemporary model of layered protocols. The purpose of a layered-protocol model is to create a modular environment that reduces complexity and permits changes to one layer without adversely affecting another.

The data communication community, through the **International Standards Organization**,[2] has developed a layered set of protocols called the **Open System Interface (OSI)**. 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. This seven-layer protocol model is discussed in detail in the appendix.

## Internet Protocols

**Transfer Control Protocol/Internet Protocol (TCP/IP)** is the basic protocol that permits communication between Internet sites. It was invented by Vinton Cerf and Bob Kah under contract from the U.S. Department of Defense to network dissimilar systems. This protocol controls how individual packets of data are formatted, transmitted, and received. This is known as a reliable protocol because delivery of all the packets to a destination is guaranteed. If delivery is interrupted by hardware or software failure, the packets are automatically retransmitted.

The TCP portion of the protocol ensures that the total number of data bytes transmitted was received. The IP component provides the routing mechanism. Every server and computer in a TCP/IP network requires an IP address, which is either permanently assigned or dynamically assigned at start-up. The IP part of the TCP/IP protocol contains a network address that is used to route messages to different networks.

While TCP/IP is the fundamental communications protocol for the Internet, the following are some of the more common protocols that are used for specific tasks.

### *File Transfer Protocols*

**File Transfer Protocol (FTP)** is used to transfer text files, programs, spreadsheets, and databases across the Internet. **TELNET** is a terminal emulation protocol used on TCP/IP-based networks. It allows users to run programs and review data from a remote terminal or computer. TELNET is an inherent part of the TCP/IP communications protocol. While both protocols deal with data transfer, FTP is useful for downloading entire files from the Internet; TELNET is useful for perusing a file of data as if the user were actually at the remote site.

### *Mail Protocols*

**Simple Network Mail Protocol (SNMP)** is the most popular protocol for transmitting e-mail messages. Other e-mail protocols are **Post Office Protocol (POP)** and **Internet Message Access Protocol (IMAP).**

[2] The International Standards Organization (ISO) is a voluntary group comprising representatives from the national standards organizations of its member countries. The ISO works toward the establishment of international standards for data encryption, data communication, and protocols.

## Security Protocols

**Secure Sockets Layer (SSL)** is a low-level encryption scheme used to secure transmissions in higher-level HTTP format. **Private Communications Technology (PCT)** is a security protocol that provides secure transactions over the web. PCT encrypts and decrypts a message for transmission. Most web browsers and servers support PCT and other popular security protocols such as SSL. **Secure Electronic Transmission (SET)** is an encryption scheme developed by a consortium of technology firms and banks (Netscape, Microsoft, IBM, Visa, MasterCard, etc.) to secure credit card transactions. Customers making credit card purchases over the Internet transmit their encrypted credit card number to the merchant, who then transmits the number to the bank. The bank returns an encrypted acknowledgment to the merchant. The customer need not worry about an unscrupulous merchant decrypting the customer's credit card number and misusing the information. **Privacy Enhanced Mail (PEM)** is a standard for secure e-mail on the Internet. It supports encryption, digital signatures, and digital certificates as well as both private and public key methods (which will be discussed later).

## Network News Transfer Protocol

**Network News Transfer Protocol (NNTP)** is used to connect to Usenet groups on the Internet. Usenet newsreader software supports the NNTP protocol.

## HTTP and HTTP-NG

HTTP controls web browsers that access the web. When the user clicks on a link to a web page, a connection is established and the web page is displayed, then the connection is broken. **HyperText Transport Protocol–Next Generation (HTTP-NG)** is an enhanced version of the HTTP protocol that maintains the simplicity of HTTP while adding important features such as security and authentication.

**HyperText Markup Language (HTML)** is the document format used to produce web pages. HTML defines the page layout, fonts, and graphic elements as well as hypertext links to other documents on the web. HTML is used to lay out information for display in an appealing manner such as one sees in magazines and newspapers. The ability to lay out text and graphics (including pictures) is important in terms of appeal to users in general. Even more pertinent is HTML's support for hypertext links in text and graphics that enable the reader to virtually jump to another document located anywhere on the World Wide Web.

With advances in Internet technology and connectivity, corporations have moved toward disclosure of corporate financial information in a form compatible with standard web-browsing tools. In this way, investors and analysts may have access to current corporate information. Dissemination of HTML-based financial reports, however, is limited to presentation only. HTML does not support the exchange of information in a relational form such as that commonly employed in EDI applications.[3]

## XML

**eXtensible Markup Language (XML)** is a metalanguage for describing markup languages. The term *extensible* means that any markup language can be created using XML. This

[3] Although EDI can employ the Internet, it is normally limited to specific trading partners in a precontracted trade agreement and is focused on a relatively narrow aspect of overall business operations (for example, exchange of purchase orders and subsequent payment in electronic form).

includes the creation of markup languages capable of storing data in relational form in which tags (or formatting commands) are mapped to data values. Thus, XML can be used to model the data structure of an organization's internal database.

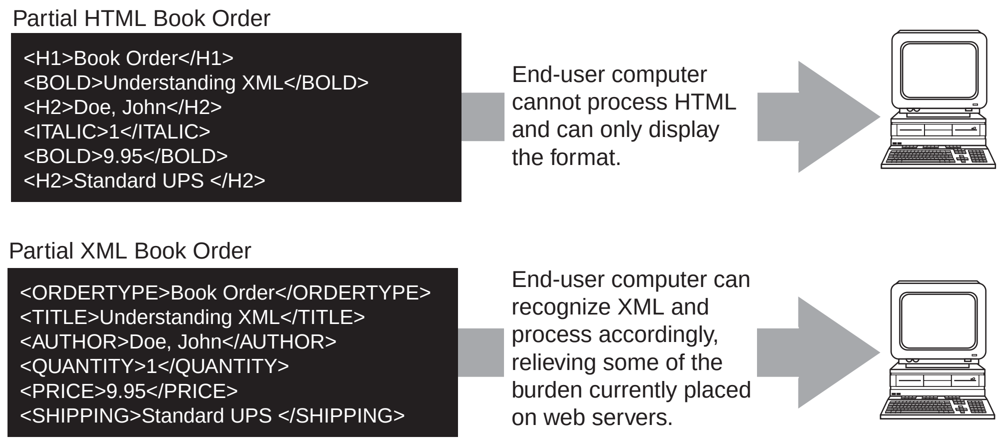
The examples illustrated in Figure 12-2 serve to distinguish HTML from XML using a bookstore order formatted in both languages.[4] Although essentially the same information is contained in both examples, and they look similar in structure, important differences exist between them. While both examples use tags (words that are bracketed by the symbols < and >) and attributes such as Doe, John, the way in which these tags and attributes are used differs. In the HTML example, the tags have predefined meaning that describes how the attributes will be presented in a document. The book order in this example can only be viewed (similar to a FAX) and must be manually entered into the bookstore's order entry system for processing. In the case of the XML order, the tags are customized to delimit the attributes. The application reads and interprets the data. Thus, the bookstore order prepared in XML presents order attributes in a relational form that can be automatically imported into a bookseller's internal database.

## XBRL

Recognizing the potential benefits of XML, the AICPA encouraged research into the creation of an accounting-specific markup language based on XML. **eXtensible Business Reporting Language (XBRL)** is an XML-based language that was designed to provide the financial community with a standardized method for preparing, publishing, and automatically exchanging financial information, including financial statements of publicly held companies. XBRL is typically used for reporting aggregated financial data, but can also be applied to communicating information pertaining to individual transactions.

**XBRL taxonomies** are classification schemes that are compliant with the XBRL specifications to accomplish a specific information exchange or reporting objective such as filing with the Securities and Exchanges Commission. XBRL-based taxonomies also allow business entities to provide expanded financial information instantaneously to interested parties. Furthermore, companies that use native-XBRL database technology[5]

**FIGURE 12-2 Comparison of HTML and XML Documents**



Partial HTML Book Order

```
<H1>Book Order</H1>
<BOLD>Understanding XML</BOLD>
<H2>Doe, John</H2>
<ITALIC>1</ITALIC>
<BOLD>9.95</BOLD>
<H2>Standard UPS </H2>
```

End-user computer cannot process HTML and can only display the format.

Partial XML Book Order

```
<ORDERTYPE>Book Order</ORDERTYPE>
<TITLE>Understanding XML</TITLE>
<AUTHOR>Doe, John</AUTHOR>
<QUANTITY>1</QUANTITY>
<PRICE>9.95</PRICE>
<SHIPPING>Standard UPS </SHIPPING>
```

End-user computer can recognize XML and process accordingly, relieving some of the burden currently placed on web servers.

[4] http://www.ebusinessforum.gr

[5] As opposed to the use of standard databases such as Oracle or Sybase.

internally, as their primary information storage platform, can further speed up the process of reporting. Consumers of such financial data (for example, investors and analysts) can readily import XBRL documents into internal databases and analysis tools to greatly facilitate their decision-making processes.

## *Creating an XBRL Report*

Figure 12-3 presents part of a hypothetical company's internal database.[6] This snapshot shows various general ledger accounts and their values. Currently, these data are organized and labeled according to the hypothetical company's internal needs and conventions. To make the data useful to outsiders and comparable with other firms, they need to be organized, labeled, and reported in a manner that all XBRL users generally accept. This involves mapping the organization's internal data to XBRL taxonomy elements to produce an **XBRL instance document**. The process for doing this is described below.[7]

The first step in the process is to select a taxonomy. In essence, the XBRL taxonomy specifies the data to be included in an exchange or report. The XBRL Standards Committee has created several taxonomies for widespread use. This illustration employs XBRL Taxonomy for Financial Reporting for Commercial and Industrial Companies, referred to as CI taxonomy.

The next step is to cross-reference each general ledger account to an appropriate XBRL taxonomy element (tag). This can be accomplished using a simple tool such as Taxonomy Mapper, pictured in Figure 12-4.[8] Note how the XBRL tag labeled Cash, Cash Equivalents, and Short Term Investments is mapped to the database account labeled Cash in Bank–Canada.

Once the mapping process is complete, each database record will contain a stored tag as depicted by the Taxonomy Element field in Figure 12-5. The data mapping need be done only once, but the tags are used whenever the data are placed in XBRL format for dissemination to outsiders.

From this new database structure, computer programs that recognize and interpret the tags associated with the data attributes can generate XBRL instance documents (the actual financial reports). Figure 12-6 presents an example of an instance document.[9]

The XBRL instance document can now be published to make it available to users. The document can be placed on an intranet server (see the appendix) for internal use; it can be placed on an extranet for limited dissemination to customers or trading partners; or it can be placed on the Internet for public dissemination. In its current state, the instance document is computer readable for analysis and processing. To make it more human readable, HTML layout rules can be provided in a separate style sheet that web browsers use to present the XBRL information in a visually appealing manner.

XBRL is an important technology that facilitates B2B information exchange while still supporting widespread dissemination via the World Wide Web. In addition, the use of XBRL will facilitate fulfillment of legal requirements stipulated in the Sarbanes-Oxley Act, which was passed in response to widespread concern and skepticism about financial

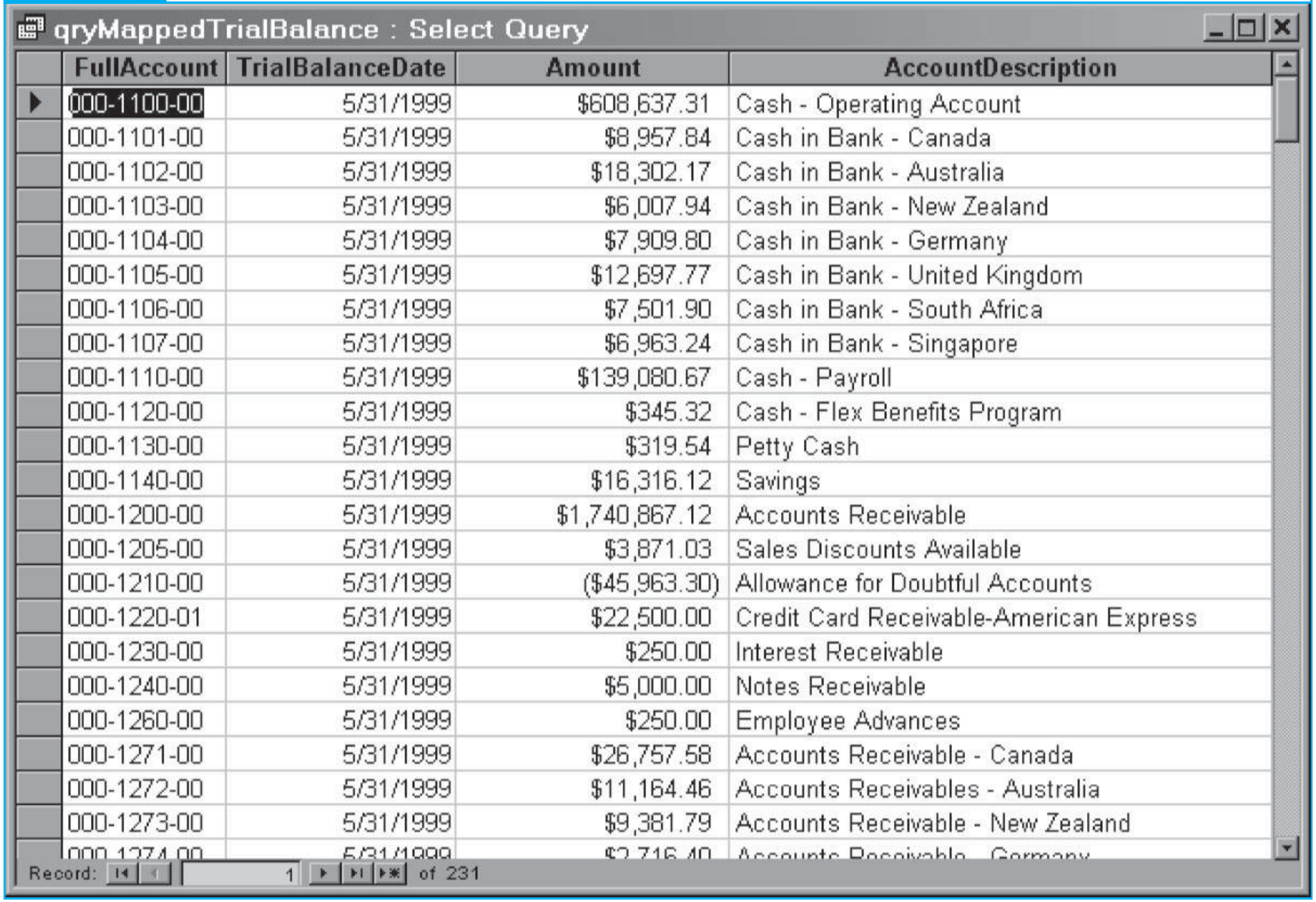
[6] http://www.xbrlsolutions.com

[7] This illustration is based on an example prepared by Charles Hoffman, member of the XBRL Steering Committee Specification Working Group with assistance from Neal Hannon, XBRL Steering Committee Education co-chair.

[8] Ibid.

[9] http://www.xbrlsolutions.com

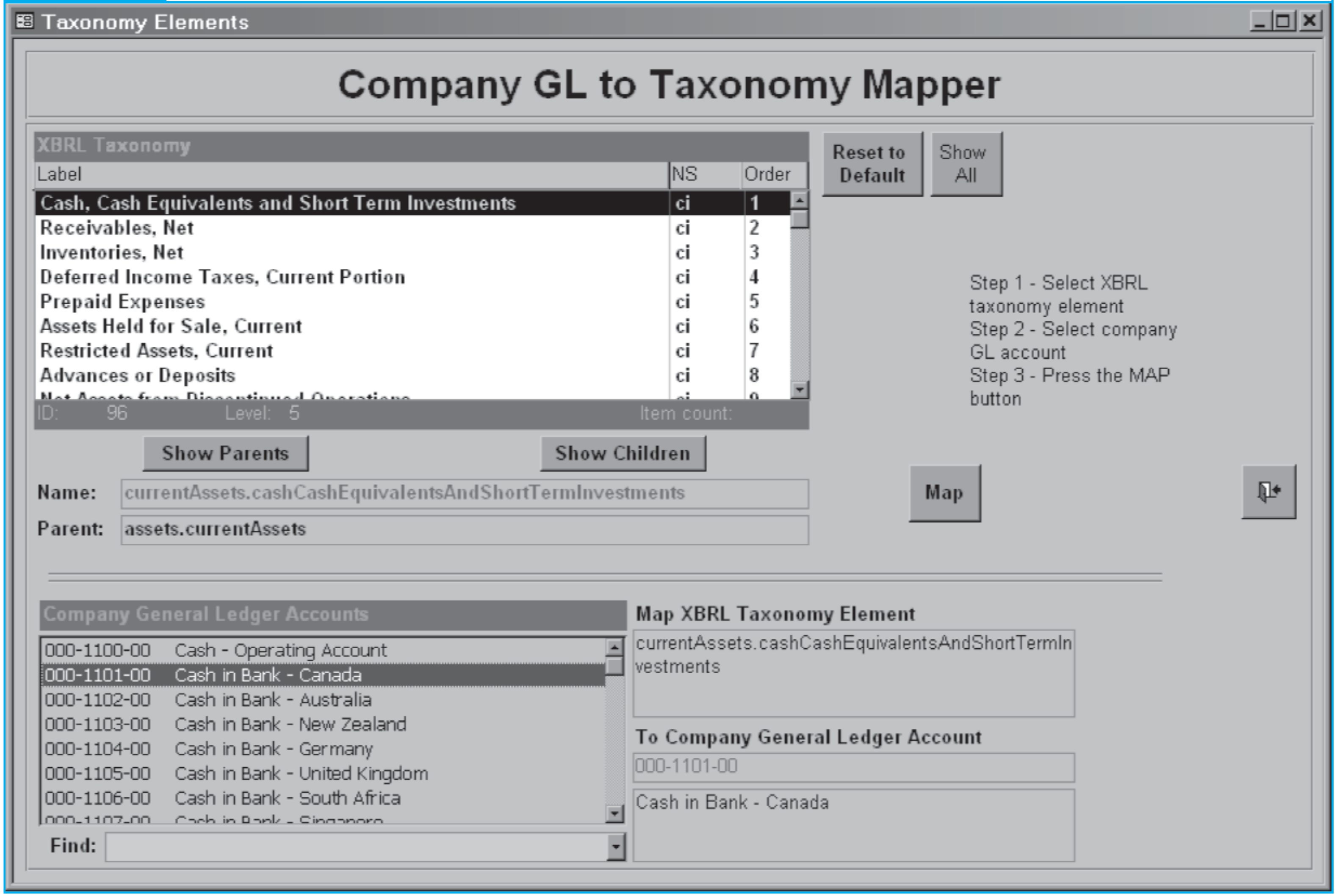
FIGURE 12-3 Internal Corporate Database



qryMappedTrialBalance : Select Query

| FullAccount | TrialBalanceDate | Amount | AccountDescription |
|---|---|---|---|
| 000-1100-00 | 5/31/1999 | $608,637.31 | Cash - Operating Account |
| 000-1101-00 | 5/31/1999 | $8,957.84 | Cash in Bank - Canada |
| 000-1102-00 | 5/31/1999 | $18,302.17 | Cash in Bank - Australia |
| 000-1103-00 | 5/31/1999 | $6,007.94 | Cash in Bank - New Zealand |
| 000-1104-00 | 5/31/1999 | $7,909.80 | Cash in Bank - Germany |
| 000-1105-00 | 5/31/1999 | $12,697.77 | Cash in Bank - United Kingdom |
| 000-1106-00 | 5/31/1999 | $7,501.90 | Cash in Bank - South Africa |
| 000-1107-00 | 5/31/1999 | $6,963.24 | Cash in Bank - Singapore |
| 000-1110-00 | 5/31/1999 | $139,080.67 | Cash - Payroll |
| 000-1120-00 | 5/31/1999 | $345.32 | Cash - Flex Benefits Program |
| 000-1130-00 | 5/31/1999 | $319.54 | Petty Cash |
| 000-1140-00 | 5/31/1999 | $16,316.12 | Savings |
| 000-1200-00 | 5/31/1999 | $1,740,867.12 | Accounts Receivable |
| 000-1205-00 | 5/31/1999 | $3,871.03 | Sales Discounts Available |
| 000-1210-00 | 5/31/1999 | ($45,963.30) | Allowance for Doubtful Accounts |
| 000-1220-01 | 5/31/1999 | $22,500.00 | Credit Card Receivable-American Express |
| 000-1230-00 | 5/31/1999 | $250.00 | Interest Receivable |
| 000-1240-00 | 5/31/1999 | $5,000.00 | Notes Receivable |
| 000-1260-00 | 5/31/1999 | $250.00 | Employee Advances |
| 000-1271-00 | 5/31/1999 | $26,757.58 | Accounts Receivable - Canada |
| 000-1272-00 | 5/31/1999 | $11,164.46 | Accounts Receivables - Australia |
| 000-1273-00 | 5/31/1999 | $9,381.79 | Accounts Receivable - New Zealand |
| 000-1274-00 | 5/31/1999 | $2,716.40 | Accounts Receivable - Germany |

FIGURE 12-4 GL to Taxonomy Mapper



Company GL to Taxonomy Mapper

XBRL Taxonomy

| Label | NS | Order |
|---|---|---|
| Cash, Cash Equivalents and Short Term Investments | ci | 1 |
| Receivables, Net | ci | 2 |
| Inventories, Net | ci | 3 |
| Deferred Income Taxes, Current Portion | ci | 4 |
| Prepaid Expenses | ci | 5 |
| Assets Held for Sale, Current | ci | 6 |
| Restricted Assets, Current | ci | 7 |
| Advances or Deposits | ci | 8 |
| Net Assets from Discontinued Operations | ci | 9 |

ID: 96 Level: 5 Item count:

Step 1 - Select XBRL taxonomy element
Step 2 - Select company GL account
Step 3 - Press the MAP button

Name: currentAssets.cashCashEquivalentsAndShortTermInvestments

Parent: assets.currentAssets

Company General Ledger Accounts

| | |
|---|---|
| 000-1100-00 | Cash - Operating Account |
| 000-1101-00 | Cash in Bank - Canada |
| 000-1102-00 | Cash in Bank - Australia |
| 000-1103-00 | Cash in Bank - New Zealand |
| 000-1104-00 | Cash in Bank - Germany |
| 000-1105-00 | Cash in Bank - United Kingdom |
| 000-1106-00 | Cash in Bank - South Africa |
| 000-1107-00 | Cash in Bank - Singapore |

Find:

Map XBRL Taxonomy Element

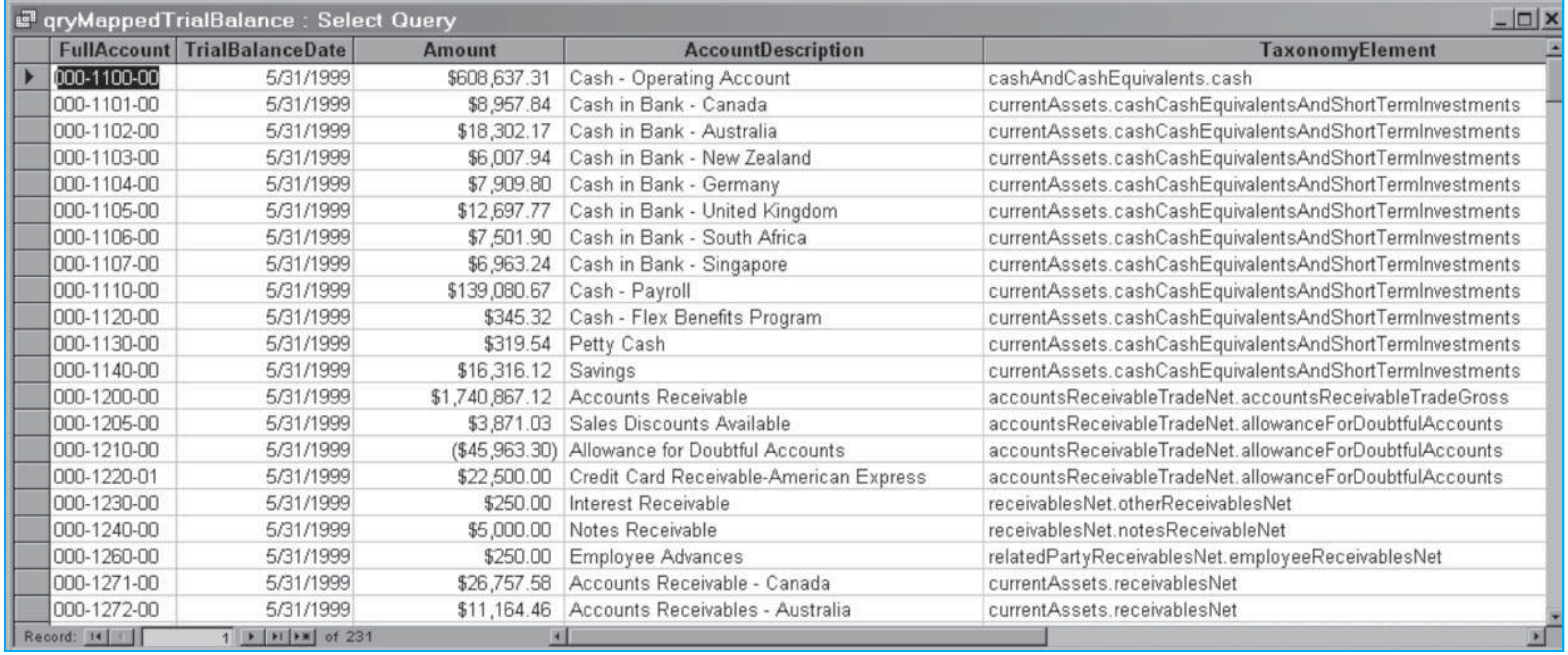
currentAssets.cashCashEquivalentsAndShortTermInvestments

To Company General Ledger Account

000-1101-00

Cash in Bank - Canada

FIGURE 12-5 Database Structure with XBRL Tag

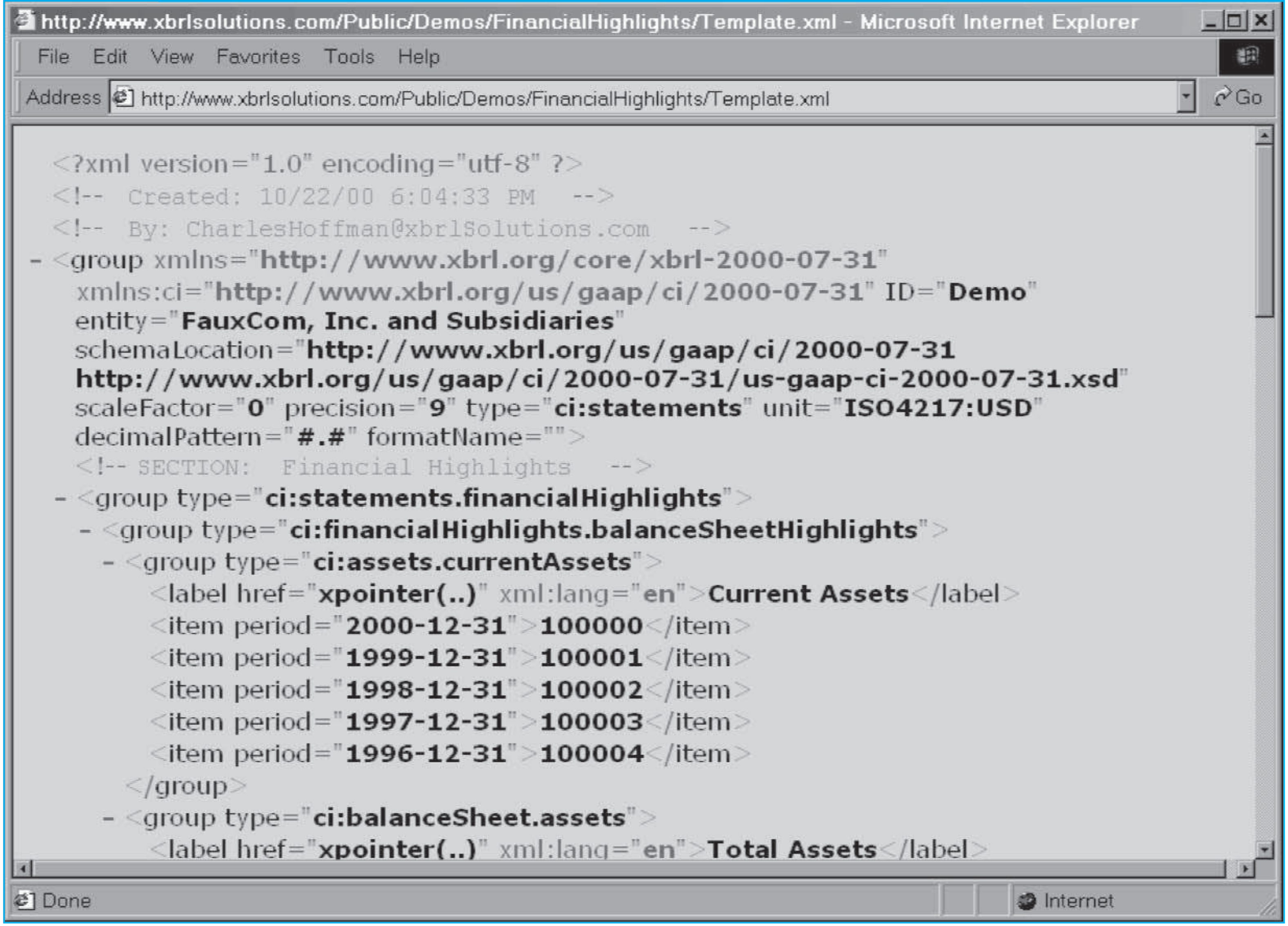


qryMappedTrialBalance : Select Query

| FullAccount | TrialBalanceDate | Amount | AccountDescription | TaxonomyElement |
|---|---|---|---|---|
| 000-1100-00 | 5/31/1999 | $608,637.31 | Cash - Operating Account | cashAndCashEquivalents.cash |
| 000-1101-00 | 5/31/1999 | $8,957.84 | Cash in Bank - Canada | currentAssets.cashCashEquivalentsAndShortTermInvestments |
| 000-1102-00 | 5/31/1999 | $18,302.17 | Cash in Bank - Australia | currentAssets.cashCashEquivalentsAndShortTermInvestments |
| 000-1103-00 | 5/31/1999 | $6,007.94 | Cash in Bank - New Zealand | currentAssets.cashCashEquivalentsAndShortTermInvestments |
| 000-1104-00 | 5/31/1999 | $7,909.80 | Cash in Bank - Germany | currentAssets.cashCashEquivalentsAndShortTermInvestments |
| 000-1105-00 | 5/31/1999 | $12,697.77 | Cash in Bank - United Kingdom | currentAssets.cashCashEquivalentsAndShortTermInvestments |
| 000-1106-00 | 5/31/1999 | $7,501.90 | Cash in Bank - South Africa | currentAssets.cashCashEquivalentsAndShortTermInvestments |
| 000-1107-00 | 5/31/1999 | $6,963.24 | Cash in Bank - Singapore | currentAssets.cashCashEquivalentsAndShortTermInvestments |
| 000-1110-00 | 5/31/1999 | $139,080.67 | Cash - Payroll | currentAssets.cashCashEquivalentsAndShortTermInvestments |
| 000-1120-00 | 5/31/1999 | $345.32 | Cash - Flex Benefits Program | currentAssets.cashCashEquivalentsAndShortTermInvestments |
| 000-1130-00 | 5/31/1999 | $319.54 | Petty Cash | currentAssets.cashCashEquivalentsAndShortTermInvestments |
| 000-1140-00 | 5/31/1999 | $16,316.12 | Savings | currentAssets.cashCashEquivalentsAndShortTermInvestments |
| 000-1200-00 | 5/31/1999 | $1,740,867.12 | Accounts Receivable | accountsReceivableTradeNet.accountsReceivableTradeGross |
| 000-1205-00 | 5/31/1999 | $3,871.03 | Sales Discounts Available | accountsReceivableTradeNet.allowanceForDoubtfulAccounts |
| 000-1210-00 | 5/31/1999 | ($45,963.30) | Allowance for Doubtful Accounts | accountsReceivableTradeNet.allowanceForDoubtfulAccounts |
| 000-1220-01 | 5/31/1999 | $22,500.00 | Credit Card Receivable-American Express | accountsReceivableTradeNet.allowanceForDoubtfulAccounts |
| 000-1230-00 | 5/31/1999 | $250.00 | Interest Receivable | receivablesNet.otherReceivablesNet |
| 000-1240-00 | 5/31/1999 | $5,000.00 | Notes Receivable | receivablesNet.notesReceivableNet |
| 000-1260-00 | 5/31/1999 | $250.00 | Employee Advances | relatedPartyReceivablesNet.employeeReceivablesNet |
| 000-1271-00 | 5/31/1999 | $26,757.58 | Accounts Receivable - Canada | currentAssets.receivablesNet |
| 000-1272-00 | 5/31/1999 | $11,164.46 | Accounts Receivables - Australia | currentAssets.receivablesNet |

Record: 1 of 231

FIGURE 12-6 XBRL Instance Document


http://www.xbrlsolutions.com/Public/Demos/FinancialHighlights/Template.xml - Microsoft Internet Explorer
File
Edit
View
Favorites
Tools
Help
Address
http://www.xbrlsolutions.com/Public/Demos/FinancialHighlights/Template.xml
Go
Done
Internet

```
  <?xml version="1.0" encoding="utf-8" ?>
  <!-- Created: 10/22/00 6:04:33 PM   -->
  <!-- By: CharlesHoffman@xbrlSolutions.com   -->
- <group xmlns="http://www.xbrl.org/core/xbrl-2000-07-31"
    xmlns:ci="http://www.xbrl.org/us/gaap/ci/2000-07-31" ID="Demo"
    entity="FauxCom, Inc. and Subsidiaries"
    schemaLocation="http://www.xbrl.org/us/gaap/ci/2000-07-31
    http://www.xbrl.org/us/gaap/ci/2000-07-31/us-gaap-ci-2000-07-31.xsd"
    scaleFactor="0" precision="9" type="ci:statements" unit="ISO4217:USD"
    decimalPattern="#.#" formatName="">
    <!-- SECTION: Financial Highlights   -->
  - <group type="ci:statements.financialHighlights">
    - <group type="ci:financialHighlights.balanceSheetHighlights">
      - <group type="ci:assets.currentAssets">
          <label href="xpointer(..)" xml:lang="en">Current Assets</label>
          <item period="2000-12-31">100000</item>
          <item period="1999-12-31">100001</item>
          <item period="1998-12-31">100002</item>
          <item period="1997-12-31">100003</item>
          <item period="1996-12-31">100004</item>
        </group>
      - <group type="ci:balanceSheet.assets">
          <label href="xpointer(..)" xml:lang="en">Total Assets</label>
```

reporting standards. XBRL can play a role in facilitating earlier reporting of financial statements required under Sarbanes-Oxley.

## Benefits from Internet Commerce

Virtually all types of businesses have benefited in some way from Internet commerce. Some potentially significant benefits include:

- Access to a worldwide customer and/or supplier base.
- Reductions in inventory investment and carrying costs.
- The rapid creation of business partnerships to fill market niches as they emerge.
- Reductions in retail prices through lower marketing costs.
- Reductions in procurement costs.
- Better customer service.

### *Internet Business Models*

Not all organizations enjoy all the benefits listed above. The benefits attained from electronic commerce will depend on the degree of organizational commitment to it as a business strategy. This can occur on three levels, discussed in the following section.

***Information Level.*** At the **information level** of activity, an organization uses the Internet to display information about the company, its products, services, and business policies. This level involves little more than creating a website, and it is the first step taken by most firms entering the Internet marketplace. When customers access the website, they generally first visit the home page. This is an index to the site's contents through other web pages. Large organizations often create and manage their websites internally. Smaller companies have their sites hosted on servers that an ISP maintains. To be successful at this level, the organization must ensure that: (1) information displayed on the website is current, complete, and accurate; (2) customers can find the site and successfully navigate through it; (3) an adequate hardware and software infrastructure exists to facilitate quick access during high usage periods; and (4) only authorized users access information on the site.

***Transaction Level.*** Organizations involved at the **transaction level** use the Internet to accept orders from customers and/or to place them with their suppliers. This involves engaging in business activities with total strangers from remote parts of the world. These may be customers, suppliers, or potential trading partners. Many of the risks that are discussed later in the chapter relate to this (and to the next) level of electronic commerce. Success in this domain involves creating an environment of trust by resolving the key concerns listed below:

- Ensure that data used in the transaction are protected from misuse.
- Verify the accuracy and integrity of business processes used by the potential customer, partner, or supplier.
- Verify the identity and physical existence of the potential customer, partner, or supplier.
- Establish the reputation of the potential customer, partner, or supplier.

***Distribution Level.*** Organizations operating on the **distribution level** use the Internet to sell and deliver digital products to customers. These include subscriptions to online news services, software products and upgrades, and music and video products. In addition to all the concerns identified at the transaction level, firms involved in this aspect of electronic commerce are concerned that products are delivered successfully and to only legitimate customers.

### *Dynamic Virtual Organizations*

Perhaps the greatest potential benefit to be derived from electronic commerce is the firm's ability to forge dynamic business alliances with other organizations to fill unique market niches as opportunities arise. These may be long-lasting partnerships or one-time ventures. Electronic partnering of business enterprises forms a **dynamic virtual organization** that benefits all parties involved.

For example, consider a company that markets millions of different products including books, music, software, and toys over the Internet. If this were a traditional organization created to serve walk-in customers, it would need a massive warehouse to store the extensive range of physical products that it sells. It must also make significant financial investments in inventory and personnel to maintain stock, fill customer orders, and control the environment. A virtual organization does not need this physical infrastructure. Figure 12-7 illustrates the partnering relationship possible in a virtual organization.

The selling organization maintains a website for advertising product offerings. The products themselves are not physically in the custody of the seller, but are stored at the trading partner's (for example, manufacturer, publisher, or distributor) facilities. The seller provides customers with product descriptions, consumer reports, prices, availability, and expected delivery times. This information comes from trading partners through an Internet connection. The seller validates customer orders placed through the website and automatically dispatches these to the trading partner firm, which actually ships the product.

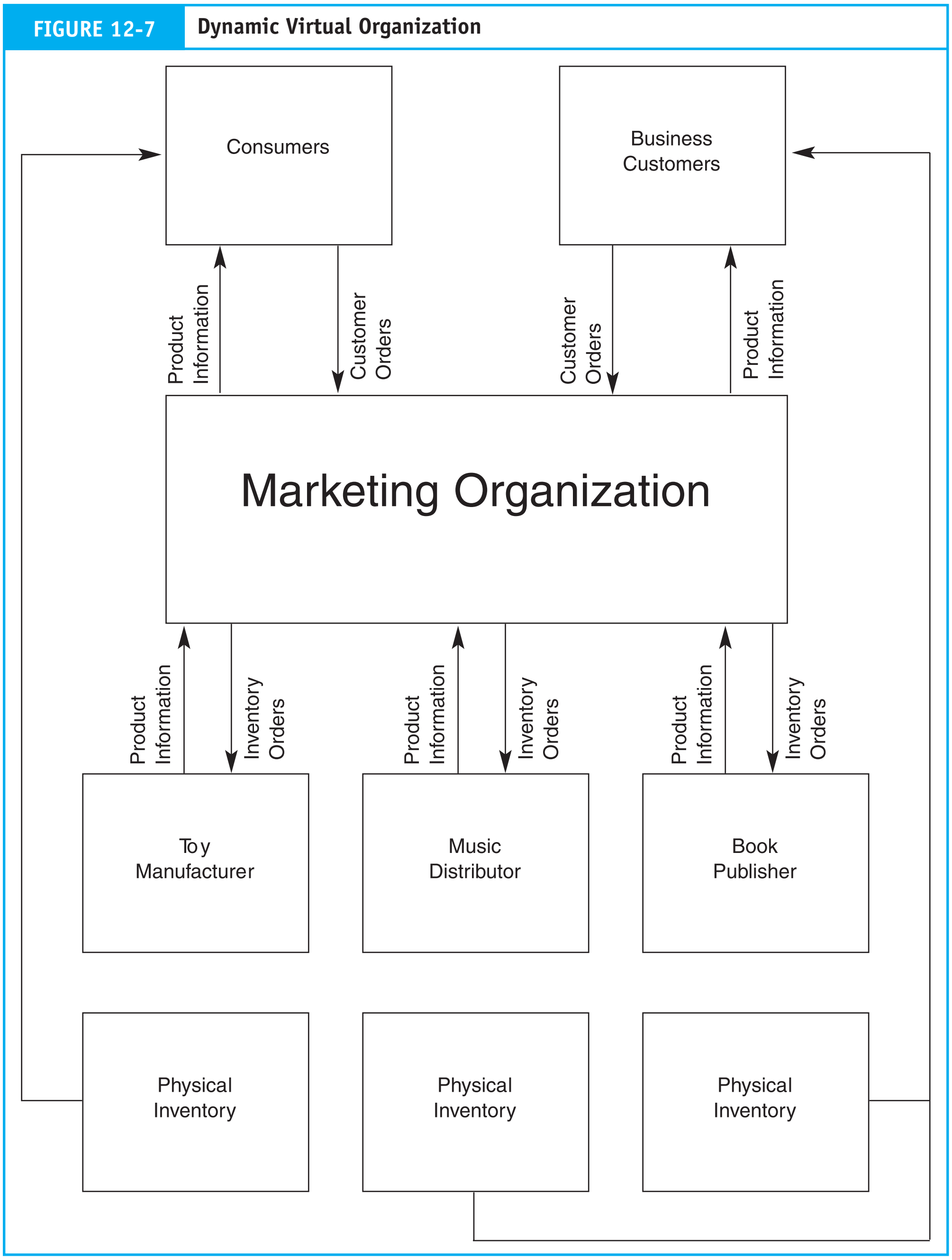
The virtual organization can expand, contract, or shift its product line and services by simply adding or eliminating trading partners. To fully exploit this flexibility, organizations often forge relationships with total strangers. Managers in both firms need to make quick determinations as to the competence, compatibility, and capacity of potential partners to discharge their responsibilities. These and other security-related risks are potential impediments to electronic commerce.

## Risks Associated with Electronic Commerce

Reliance on electronic commerce poses concern about unauthorized access to confidential information. As LANs become the platform for mission-critical applications and data, proprietary information, customer data, and financial records are at risk. Organizations connected to their customers and business partners via the Internet are particularly exposed. Without adequate protection, firms open their doors to computer hackers, vandals, thieves, and industrial spies both internally and from around the world.

The paradox of networking is that networks exist to provide user access to shared resources, yet the most important objective of any network is to control such access. Hence, for every productivity argument in favor of remote access, there is a security argument against it. Organization management constantly seeks balance between increased access and the associated business risks.

FIGURE 12-7 Dynamic Virtual Organization



In general, business **risk** is the possibility of loss or injury that can reduce or eliminate an organization's ability to achieve its objectives. In terms of electronic commerce, risk relates to the loss, theft, or destruction of data as well as the use of computer programs that financially or physically harm an organization. The following sections deal with various forms of such risk. This includes intranet risks posed by dishonest employees who have the technical knowledge and position to perpetrate frauds, and Internet risks that threaten both consumers and business entities.

## Intranet Risks

Intranets consist of small LANs and large WANs that may contain thousands of individual nodes.[10] Intranets are used to connect employees within a single building, between buildings on the same physical campus, and between geographically dispersed locations. Typical intranet activities include e-mail routing, transaction processing between business units, and linking to the outside Internet.

Unauthorized and illegal employee activities internally spawn intranet threats. Their motives for doing harm may be vengeance against the company, the challenge of breaking into unauthorized files, or to profit from selling trade secrets or embezzling assets. The threat from employees (both current and former) is significant because of their intimate knowledge of system controls and/or the lack of controls. Discharged employees, or those who leave under contentious circumstance, raise particular concerns. Trade secrets, operations data, accounting data, and confidential information to which the employee has access are at greatest risk.

### *Interception of Network Messages*

The individual nodes on most intranets are connected to a shared channel across which travel user IDs, passwords, confidential e-mails, and financial data files. The unauthorized interception of this information by a node on the network is called sniffing. The exposure is even greater when the intranet is connected to the Internet. Network administrators routinely use commercially available sniffer software to analyze network traffic and to detect bottlenecks. Sniffer software, however, can also be downloaded from the Internet. In the hands of a computer criminal, sniffer software can be used to intercept and view data sent across a shared intranet channel.

### *Access to Corporate Databases*

Intranets connected to central corporate databases increase the risk that an employee will view, corrupt, change, or copy data. Social security numbers, customer listings, credit card information, recipes, formulas, and design specifications may be downloaded and sold. Outsiders have bribed employees who have access privileges to financial accounts to electronically write off an account receivable or erase an outstanding tax bill. A Computer Security Institute (CSI) study reported that financial fraud losses of this sort averaged $500,000.[11] A previous CSI study found that the average loss from corporate espionage was more than $1 million. Total losses from insider trade secret theft have been estimated to exceed $24 billion per year.

### *Privileged Employees*

We know from earlier chapters that an organization's internal controls are typically aimed at lower-level employees. According to the CSI study, however, middle managers, who often possess access privileges that allow them to override controls, are most often prosecuted for insider crimes.[12] Information systems employees within the organization are another group empowered with override privileges that may permit access to mission-critical data.

[10] See the chapter appendix for a complete discussion of LANs and WANs.

[11] Association of Certified Fraud Examiners, "2002 Report to the Nation: Occupational Fraud and Abuse," (2002).

[12] Financial Executives Institute, "Safety Nets: Secrets of Effective Information Technology Controls, An Executive Report," (June 1997).

### *Reluctance to Prosecute*

A factor that contributes to computer crime is many organizations' reluctance to prosecute the criminals. According to the CSI study, this situation is improving. In 1996, only 17 percent of the firms that experienced an illegal intrusion reported it to a law enforcement agency. In 2002, 75 percent of such crimes were reported. Of the 25 percent that did not report the intrusions, fear of negative publicity was the most common cited justification for their silence.

Many computer criminals are repeat offenders. Performing background checks on prospective employees can significantly reduce an organization's hiring risk and avoid criminal acts. In the past, employee backgrounding was difficult to achieve because former employers, fearing legal action, were reluctant to disclose negative information to prospective employers. A no comment policy prevailed.

The relatively new legal doctrine of negligent hiring liability is changing this. This doctrine effectively requires employers to check into an employee's background. Increasingly, courts are holding employers responsible for criminal acts that employees, both on and off the job, perpetrated if a background check could have prevented crimes. Many states have passed laws that protect a former employer from legal action when providing work-related performance information about a former employee when (1) the inquiry comes from a prospective employer, (2) the information is based on credible facts, and (3) the information is given without malice.[13]

## Internet Risks

This section looks at some of the more significant risks associated with Internet commerce. First the risks related to consumer privacy and transaction security are examined. The risk to business entities from fraud and malicious acts are then reviewed.

## Risks to Consumers

As more and more people connect to the web, Internet fraud increases. Because of this, many consumers view the Internet as an unsafe place to do business. In particular, they worry about the security of credit card information left on websites and the confidentiality of their transactions. Some of the more common threats to consumers from cyber criminals are discussed below.

***Theft of Credit Card Numbers.*** The perception that the Internet is not secure for credit card purchases is considered to be the biggest barrier to electronic commerce. Some Internet companies are negligent or even fraudulent in the way they collect, use, and store credit card information. One hacker successfully stole 100,000 credit card numbers with a combined credit limit of $1 billion from an Internet service provider's customer files. He was arrested when he tried to sell the information to an undercover FBI agent.

Another fraud scheme involves establishing a fraudulent business operation that captures credit card information. For example, the company may take orders to deliver flowers on Mother's Day. When the day arrives, the company goes out of business and disappears from the web. Of course, the flowers are never delivered, and the perpetrator either sells or uses the credit card information.

[13] M. Greenstein and T. Fineman, *Electronic Commerce: Security, Risk Management and Control* (Irwin McGraw-Hill, 2000): 146.

***Theft of Passwords.*** One form of Internet fraud involves establishing a website to steal a visitor's password. To access the web page, the visitor is asked to register and provide an e-mail address and password. Many people use the same password for different applications such as ATM services, e-mail, and employer-network access. In the hopes that the website visitor falls into this pattern of behavior, the cyber criminal uses the captured password to break into the victim's accounts.

***Consumer Privacy.*** Concerns about the lack of privacy discourage consumers from engaging in Internet commerce. One poll revealed that:[14]

- Almost two-thirds of non-Internet users would start using the Internet if they could be assured that their personal information was protected.
- Privacy is the number one reason that individuals are avoiding Internet commerce.

Many coalitions have been formed to lobby for stronger privacy measures. The Center for Democracy and Technology (CDT), Electronic Frontier Foundation (EFF), and Electronic Privacy Information Center (EPIF) are three prominent groups. One aspect of privacy involves the way in which websites capture and use cookies.

**Cookies** are files containing user information that the web server of the site being visited creates. The cookies are then stored on the visitor's computer hard drive. They contain the URLs of visited sites. When the site is revisited, the user's browser sends the specific cookies to the web server. The original intent behind the cookie was to improve efficiency in processing return visits to sites where users are required to register for services. For example, on the user's first visit to a particular website, the URL and user ID may be stored as a cookie. On subsequent visits, the website retrieves the user ID, thus saving the visitor from rekeying the information.

Cookies allow websites to off-load the storage of routine information about vast numbers of visitors. It is far more efficient for a web server to retrieve this information from a cookie file stored on the user's computer than to search through millions of such records stored at the website. Most browsers have preference options to disable cookies or to warn the user before accepting one.

The privacy controversy over cookies relates to what information is captured and how it is used. For example, the cookie may be used to create a profile of user preferences for marketing purposes. The profile could be based on the pages accessed or the options selected during the site visit, the time of day or night of the visit, and the length of time spent at the site. The profile could also include the user's e-mail address, zip code, home phone number, and any other information the user is willing to provide to the website.

This type of information is useful to online marketing firms that sell advertising for thousands of Internet firms that sell goods and service. The user profile enables the marketing firm to customize ads and to target them to Internet consumers. To illustrate, let's assume a user visiting an online bookstore browses sports car and automobile racing listings. This information is stored in a cookie and transmitted to the online marketing firm, which then sends JavaScript ads for general automotive products to the bookstore's web page to entice the visitor to click on the ads. Each time the consumer visits the site, the contents of the cookie will be used to trigger the appropriate ads. User profile information can also be compiled into a mailing list, which is sold and used in the traditional way for solicitation.

[14] "Privacy . . . A Weak Link in the Cyber-Chain," PricewaterhouseCoopers E-Business Leaders Series, www.pwcglobal.com, 1999.

***Cookies and Consumer Security.*** Another concern over the use of cookies relates to security. Cookies are text (.txt) files that can be read with any text editor. Some websites may store user passwords in cookies. If the passwords are not encrypted (discussed later) before being stored, anyone with access to the computer can retrieve the cookies and the passwords. Thus, when multiple employees share a computer in the workplace, all users of the computer may review the cookies file, which is stored in a common directory.

A related form of risk comes from criminal or malicious websites. As the user browses the site, a JavaScript program may be uploaded to the user's computer. The program secretly scans the hard drive for the cookies file and copies it to the website, where it is reviewed for passwords and other personal data.

## *Risks to Businesses*

Business entities are also at risk from Internet commerce. IP spoofing, denial of service attacks, and malicious programs are three significant concerns.

***IP Spoofing.*** **IP spoofing** is a form of masquerading to gain unauthorized access to a web server and/or to perpetrate an unlawful act without revealing one's identity. To accomplish this, a perpetrator modifies the IP address of the originating computer to disguise his or her identity. A criminal may use IP spoofing to make a message appear to be coming from a trusted or authorized source and thus slip through control systems designed to accept transmissions from certain (trusted) host computers and block out others. This technique could be used to crack into corporate networks to perpetrate frauds, conduct acts of espionage, or destroy data. For example, a hacker may spoof a manufacturing firm with a false sales order that appears to come from a legitimate customer. If the spoof goes undetected, the manufacturer will incur the costs of producing and delivering a product that was never ordered.

***Denial of Service Attack.*** A **denial of service attacks (Dos)** is an assault on a web server to prevent it from servicing its legitimate users. While such attacks can be aimed at any type of website, they are particularly devastating to business entities that are prevented from receiving and processing business transactions from their customers. Three common types of Dos attacks are: SYN flood, smurf, and distributed denial of service (DDos).

***SYN Flood Attack.*** When a user establishes a connection on the Internet through TCP/IP, a three-way handshake takes place. The connecting server sends an initiation code called a SYN (SYNchronize) packet to the receiving server. The receiving server then acknowledges the request by returning a **SYNchronize–ACKnowledge (SYN-ACK)** packet. Finally, the initiating host machine responds with an ACK packet code. The **SYN flood attack** is accomplished by not sending the final acknowledgment to the server's SYN-ACK response, which causes the server to keep signaling for acknowledgement until the server times out.

The individual or organization perpetrating the SYN flood attack transmits hundreds of SYN packets to the targeted receiver, but never responds with an ACK to complete the connection. As a result, the ports of the receiver's server are clogged with incomplete communication requests that prevent legitimate transactions from being received and processed. Organizations under attack may, thus, be prevented from receiving Internet messages for days at a time.

If the target organization could identify the server that is launching the attack, a firewall (discussed later) could be programmed to ignore all communication from that site.

Such attacks, however, are difficult to prevent because they use IP spoofing to disguise the source of the messages. IP spoofing programs that randomize the source address of the attacker have been written and publicly distributed over the Internet. Therefore, to the receiving site, it appears that the transmissions are coming from all over the Internet.

***Smurf Attack.*** A **smurf attack** involves three parties: the perpetrator, the intermediary, and the victim. It is accomplished by exploiting an internet maintenance tool called a **ping,** which is used to test the state of network congestion and determine whether a particular host computer is connected and available on the network. The ping works by sending an echo request message (like a sonar ping) to the host computer and listening for a response message (echo reply). The ping signal is encapsulated in a message packet that also contains the return IP address of the sender. A functioning and available host must return an echo reply message that contains the exact data received in the echo request message packet.

The perpetrator of a smurf attack uses a program to create a ping message packet that contains the forged IP address of the victim's computer (IP spoofing) rather than that of the actual source computer. The ping message is then sent to the intermediary, which is actually an entire subnetwork of computers. By sending the ping to the network's **IP broadcast address,** the perpetrator ensures that each node on the intermediary network receives the echo request automatically. Consequently, each intermediary node sends echo responses to the ping message, which are returned to the victim's IP address, not the source computer's. The resulting flood echoes can overwhelm the victim's computer and cause network congestion that makes it unusable for legitimate traffic. Figure 12-8 illustrates a smurf attack.

The intermediary in a smurf attack is an unwilling and unaware party. Indeed, the intermediary is also a victim and to some extent suffers the same type of network congestion problems the target victim suffers. One method of defeating smurf attacks is to disable the IP broadcast addressing option at each network firewall and thus eliminate the intermediary's role. In response to this move, however, attackers have developed tools to search for networks that do not disable broadcast addressing. These networks may subsequently be used as intermediaries in smurf attacks. Also, perpetrators have developed tools that enable them to launch smurf attacks simultaneously from multiple intermediary networks for maximum effect on the victim.

***Distributed Denial of Service.*** A **distributed denial of service (DDos)** attack may take the form of a SYN flood or smurf attack. The distinguishing feature of the DDos is the sheer scope of the event. The perpetrator of a DDos attack may employ a virtual army of so-called **zombie** or bot (robot) computers to launch the attack. Since vast numbers of unsuspecting intermediaries are needed, the attack often involves one or more **Internet Relay Chat (IRC)** networks as a source of zombies. IRC is a popular interactive service on the Internet that lets thousands of people from around the world engage in real-time communications via their computers.

The problem with IRC networks is that they tend to have poor security. The perpetrator can thus easily access the IRC and upload a malicious program such as a Trojan horse (see the appendix in Chapter 16 for a definition), which contains DDos attack script. This program is subsequently downloaded to the PCs of the many thousands of people who visit the IRC site. The attack program runs in the background on the new zombie computers, which are now under the control of the perpetrator. These collections of compromised computers are known as **botnets**. Figure 12-9 illustrates this technique.

**FIGURE 12-8** Smurf Attack

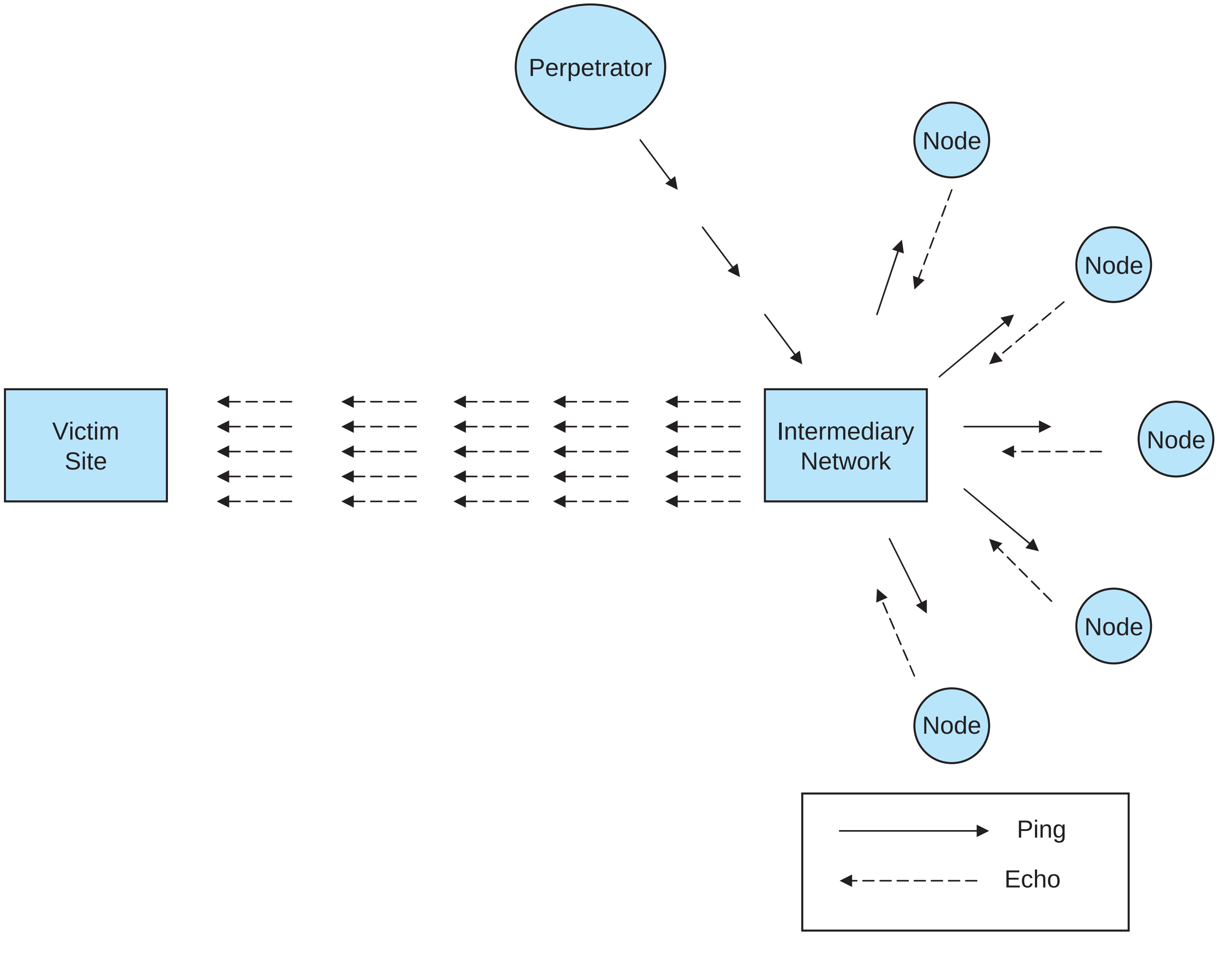
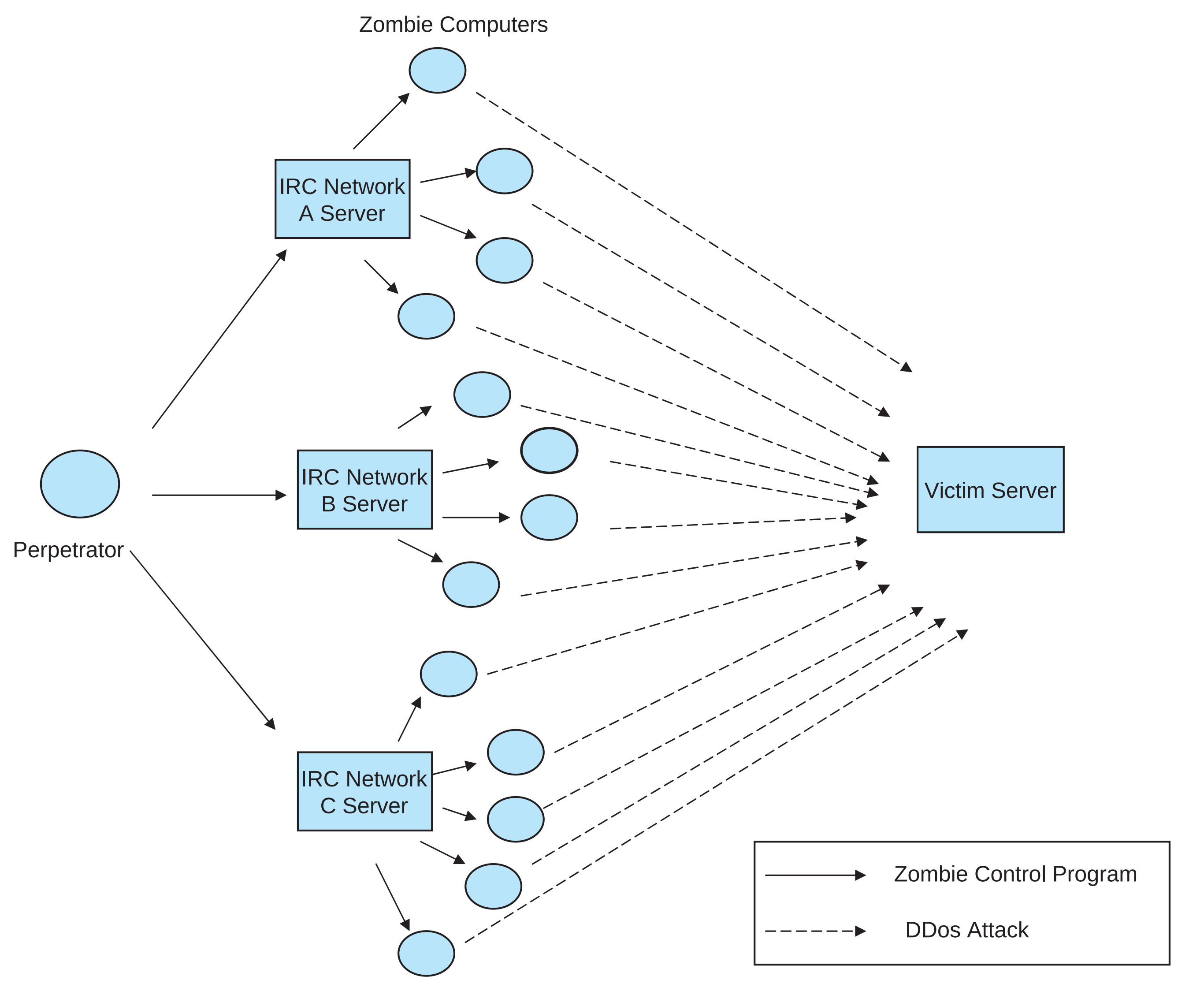


FIGURE 12-9 Distributed Denial of Service Attack



Via the zombie control program, the perpetrator has the power to direct the DDos to specific victims and turn on or off the attack at will. The DDos attack poses a far greater threat to the victim than a traditional SYN flood or smurf attack. For instance, a SYN flood coming from thousands of distributed computers can do far more damage than one from a single computer. Also, a smurf attack coming from a subnetwork of intermediary computers all emanate from the same server. In time, the server can be located and isolated by programming the victim's firewall to ignore transmissions from the attacking site. The DDos attack, on the other hand, literally comes from sites all across the Internet. Thousands of individual attack computers are harder to track down and turn off.

***Motivation behind Dos Attacks.*** The motivation behind Dos attacks may originally have been to punish an organization with which the perpetrator had a grievance or simply to gain bragging rights for being able to do it. Today, Dos attacks are also perpetrated for financial gain. Financial institutions, which are particularly dependent on Internet access, have been prime targets. Organized criminals threatening a devastating attack have extorted several institutions, including the Royal Bank of Scotland. The typical scenario is for the perpetrator to launch a short DDos attack (a day or so) to demonstrate what life would be like if the organization were isolated from the Internet. During this time, legitimate customers are unable to access their online accounts and the institution is unable to process many financial transactions. After the attack, the CEO of the organization receives a phone call demanding that a sum of money be deposited in an offshore account, or the attack will resume. Compared to the potential loss in customer confidence, damaged reputation, and lost revenues, the ransom may appear to be a small price to pay.

DDos attacks are relatively easy to execute and can have a devastating effect on the victim. Many experts feel that the best defense against DDos attacks is to implement a layered security program with multiple detection point capability. We revisit this issue in Chapter 16 to examine methods for dealing DDos attacks.

***Other Malicious Programs.*** Viruses and other forms of malicious programs such as worms, logic bombs, and Trojan horses pose a threat to both Internet and intranet users. These may be used to bring down a computer network by corrupting its operating systems, destroying or corrupting corporate databases, or capturing passwords that enable hackers to break in to the system. Malicious programs, however, are not exclusively an electronic commerce issue; database management, operating systems security, and application integrity are also threatened. Because of the broad-based implications, this class of risk is examined at length in Chapter 16.

## Security, Assurance, and Trust

Trust is the catalyst for sustaining electronic commerce. Both consumers and businesses are drawn to organizations that are perceived to have integrity. Organizations must convey a sense that they are competent and conduct business fairly with their customers, trading partners, and employees. This is a two-pronged problem. First, the company must implement the technological infrastructure and controls needed to provide for adequate security. Second, the company must assure potential customers and trading partners that adequate safeguards are in place and working. A large part of data security involves data encryption, digital authentication, and firewalls. These security techniques are outlined below, but are presented in more detail in Chapter 16. This section concludes with a review of seals of assurance techniques that promote trust in electronic commerce.

## Encryption

Encryption is the conversion of data into a secret code for storage in databases and transmission over networks. The sender uses an encryption algorithm to convert the original message (called cleartext) into a coded equivalent (called ciphertext). At the receiving end, the ciphertext is decoded (decrypted) back into cleartext.

The earliest encryption method is called the **Caesar cipher**, which Julius Caesar is said to have used to send coded messages to his generals in the field. Like modern-day encryption, the Caesar cipher has two fundamental components: a key and an algorithm.

The **key** is a mathematical value that the sender selects. The **algorithm** is the procedure of shifting each letter in the cleartext message the number of positions that the key value indicates. Thus a key value of +3 would shift each letter three places to the right. For example, the letter A in cleartext would be represented as the letter D in the ciphertext message. The receiver of the ciphertext message reverses the process to decode it and recreates the cleartext; in this case shifting each ciphertext letter three places to the left. Obviously, both the sender and receiver of the message must know the key.

Modern-day encryption algorithms, however, are far more complex, and encryption keys may be up to 128 bits in length. The more bits in the key, the stronger the encryption method. Today, nothing less than 128-bit algorithms are considered truly secure. Two commonly used methods of encryption are private key and public key encryption.

**Advanced Encryption Standard (AES),** also known as Rijndael, is a **private key** (or **symmetric key**) encryption technique. The U.S. government has adopted it as an encryption standard. To encode a message, the sender provides the encryption algorithm with the key, which produces the ciphertext message. This is transmitted to the receiver's location, where it is decoded using the same key to produce a cleartext message. Because the same key is used for coding and decoding, control over the key becomes an important security issue. The more individuals that need to exchange encrypted data, the greater the chance that the key will become known to an intruder who could intercept a message and read it, change it, delay it, or destroy it.

To overcome this problem, **public key encryption** was devised. This approach uses two different keys: one for encoding messages and the other for decoding them. The recipient has a private key used for decoding that is kept secret. The encoding key is public and published for everyone to use. This approach is illustrated in Figure 12-10.

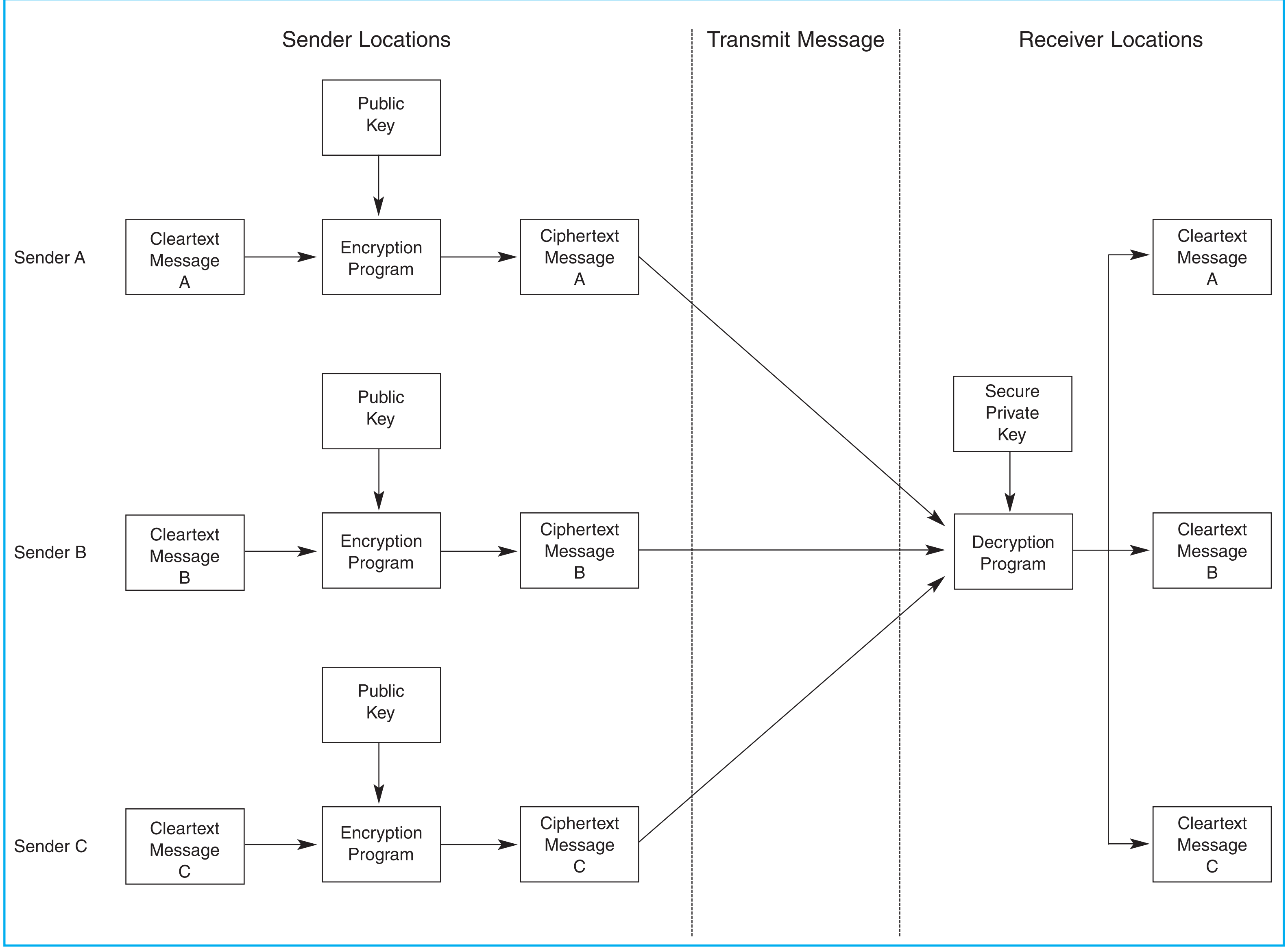
Receivers never need to share private keys with senders, which reduces the likelihood that they fall into the hands of an intruder. One of the most trusted public key encryption methods is **Rivest-Shamir-Adleman (RSA)**. This method is, however, computationally intensive and much slower than private key encryption. Sometimes, both private key and public key encryption are used together in what is called a **digital envelope**.

## Digital Authentication

Encryption alone cannot resolve all security concerns. For example, how does the supplier (receiver) know for sure that a hacker didn't intercept and alter a customer's (sender) purchase order (message) for 1,000 units of product to read 100,000? If such an alteration went undetected, the supplier would incur the labor, material, manufacturing, and distribution costs for the order. Litigation between the innocent parties may ensue.

A **digital signature** is an electronic authentication technique that ensures the transmitted message originated with the authorized sender and that it was not tampered with after the signature was applied. The digital signature is derived from a mathematically

FIGURE 12-10 **Public Key Encryption**



computed digest of the document that has been encrypted with the sender's private key. Both the digital signature and the text message are encrypted using the receiver's public key and transmitted to the receiver. At the receiving end, the message is decrypted using the receiver's private key to produce the digital signature (encrypted digest) and the cleartext version of the message. Finally, the receiver uses the sender's public key to decrypt the digital signal to produce the digest. The receiver recalculates the digest from the cleartext using the original hashing algorithm and compares this to the transmitted digest. If the message is authentic, the two digest values will match. If even a single character of the message was changed in transmission, the digest figures will not be equal.

Another concern facing the receiver is determining if the expected sender actually initiated a message. For example, suppose that the supplier receives a purchase order addressed from Customer A for 100,000 units of product, which was actually sent from an unknown computer criminal. Once again, significant costs would accrue to the supplier if it acts on this fraudulent order.

A **digital certificate** is like an electronic identification card that is used in conjunction with a public key encryption system to verify the authenticity of the message sender. Trusted third parties known as **certification authorities (CAs)** (for example, Veri-Sign, Inc.) issue digital certificates, also called digital IDs. The digital certificate is actually the sender's public key that the CA has digitally signed. The digital certificate is transmitted with the encrypted message to authenticate the sender. The receiver uses the CA's public key to decrypt the sender's public key, which is attached to the message, and then uses the sender's public key to decrypt the actual message.

Because public key encryption is central to digital authentication, public key management becomes an important internal control issue. **Public key infrastructure (PKI)** constitutes the policies and procedures for administering this activity. A PKI system consists of:

1. A certification authority that issues and revokes digital certificates.
2. A registration authority (RA) that verifies the identity of certificate applicants. The process varies depending on the level of certification desired. It involves establishing one's identity with formal documents such as a driver's license, notarization, fingerprints, and proving one's ownership of the public key.
3. A certification repository (CR), which is a publicly accessible database that contains current information about current certificates and a certification revocation list (CRL) of certificates that have been revoked and the reasons for revocation.

## Firewalls

A **firewall** is a system used to insulate an organization's intranet from the Internet. It can be used to authenticate an outside user of the network, verify his or her level of access authority, and then direct the user to the program, data, or service requested. In addition to insulating the organization's network from external networks, firewalls can also be used to protect LANs from unauthorized internal access.

A common configuration employs two firewalls: a network-level firewall and an application-level firewall. The **network-level firewall** provides basic screening of low-security messages (for example, e-mail) and routes them to their destinations based on the source and destination addresses attached. The **application-level firewall** provides high-level network security. These firewalls are configured to run security applications called proxies that perform sophisticated functions such as verifying user authentication.

## Seals of Assurance

In response to consumer demand for evidence that a web-based business is trustworthy, a number of trusted third-party organizations are offering seals of assurance that businesses can display on their website home pages. To legitimately bear the seal, the company must show that it complies with certain business practices, capabilities, and controls. This section reviews six seal-granting organizations: Better Business Bureau (BBB), TRUSTe, Veri-Sign, Inc., International Computer Security Association (ICSA), AICPA/CICA WebTrust, and AICPA/CICA SysTrust.

### *Better Business Bureau*

The BBB is a nonprofit organization that has been promoting ethical business practices through self-regulation since 1912. The BBB has extended its mission to the Internet through a wholly owned subsidiary called BBBOnline, Inc. To qualify for the BBBOnline seal, an organization must:

- Become a member of the BBB.
- Provide information about the company's ownership, management, address, and phone number. This is verified by a physical visit to the company's premises.
- Be in business for at least one year.
- Promptly respond to customer complaints.
- Agree to binding arbitration for unresolved disputes with customers.

The assurance BBBOnline provides relates primarily to concern about business policies, ethical advertising, and consumer privacy. BBBOnline does not verify controls over transaction processing integrity and data security issues.

### *TRUSTe*

Founded in 1996, TRUSTe is a nonprofit organization dedicated to improving consumer privacy practices among Internet businesses and websites. To qualify for the TRUSTe seal, the organization must:

- Agree to follow TRUSTe privacy policies and disclosure standards.
- Post a privacy statement on the website disclosing the type of information being collected, the purpose for collecting information, and with whom it is shared.
- Promptly respond to customer complaints.
- Agree to site compliance reviews by TRUSTe or an independent third party.

TRUSTe addresses consumer privacy concerns exclusively and provides a mechanism for posting consumer complaints against its members. If a member organization is found to be out of compliance with TRUSTe standards, its right to display the trust seal may be revoked.

### *Veri-Sign, Inc.*

Veri-Sign, Inc., was established as a for-profit organization in 1995. It provides assurance regarding the security of transmitted data. The organization does not verify security of stored data or address concerns related to business policies, business processes, or privacy. Its mission is to provide digital certificate solutions that enable trusted commerce and communications. Their products allow customers to transmit encrypted data and verify the source and destination of transmissions. Veri-Sign, Inc., issues three classes of certificates to individuals, businesses, and organizations. To qualify for class three certification, the individual, business, or organization must provide a third-party confirmation of name, address, telephone number, and website domain name.

### *International Computer Security Association*

The ICSA established its web certification program in 1996. ICSA certification addresses data security and privacy concerns. It does not deal with concerns about business policy and business processes. Organizations that qualify to display the ICSA seal have undergone an extensive review of firewall security from outside hackers. Organizations must be recertified annually and undergo at least two surprise checks each year.

### *AICPA/CICA WebTrust*

The AICPA and CICA established the WebTrust program in 1997. To display the AICPA/CICA WebTrust seal, the organization undergoes an examination according to the AICPA's Standards for Attestation Engagements, No. 1, by a specially web-certified CPA or CA. The examination focuses on the areas of business practices (policies), transaction integrity (business process), and information protection (data security). The seal must be renewed every 90 days.

### *AICPA/CICA SysTrust*

In July 1999, the AICPA/CICA introduced an exposure draft describing a new assurance service called SysTrust. It is designed to increase management, customer, and trading partner confidence in systems that support entire businesses or specific processes. The assurance service involves the public accountant evaluating the system's reliability against four essential criteria: availability, security, integrity, and maintainability.

The potential users of SysTrust are trading partners, creditors, shareholders, and others who rely on the integrity and capability of the system. For example, Virtual Company is considering outsourcing some of its vital functions to third-party organizations. Virtual needs assurance that the third parties' systems are reliable and adequate to provide the contracted services. As part of the outsourcing contract, Virtual requires the servicing organizations to produce a clean SysTrust report every three months.

In theory, the SysTrust service will enable organizations to differentiate themselves from their competitors. Those organizations that undergo a SysTrust engagement will be perceived as competent service providers and trustworthy. They will be more attuned to the risks in their environment and equipped with the necessary controls to deal with the risks.[15]

## Implications for the Accounting Profession

The issues discussed in this chapter carry many implications for auditors and the public accounting profession. As key functions such as inventory procurement, sales processing, shipping notification, and cash disbursements are performed automatically, digitally, and in real time, auditors are faced with the challenge of developing new techniques for assessing control adequacy and verifying the occurrence and accuracy of economic events. The following describes issues of increasing importance to auditors in the electronic commerce age.

[15] American Institute of Certified Public Accountants, Inc. and Canadian Institute of Chartered Accountants, AICPA/CICA SysTrust Principle and Criteria for Systems Reliability (1999): 3.

## Privacy Violation

**Privacy** pertains to the level of confidentiality that an organization employs in managing customer and trading partner data. Privacy applies also to data that websites collect from visitors who are not customers. Specific concerns include:

- Does the organization have a stated privacy policy?
- What mechanisms are in place to ensure the consistent application of stated privacy policies?
- What information on customers, trading partners, and visitors does the company capture?
- Does the organization share or sell its customer, trading partner, or visitor information?
- Can individuals and business entities verify and update the information captured about them?

The growing reliance on Internet technologies for conducting business has placed the spotlight on **privacy violation** as a factor that is detrimental to a client entity. In response to this threat, several firms have developed assurance services for evaluating their client's privacy violation risk. A KPMG white paper examines the importance customers place on their privacy.[16] The paper suggests that developing a set of privacy protection policies may prove to be a significant differentiation factor for commercial companies. As such, auditors engaged in certifying management's practices and established privacy policy need to exert particular care.

The **Safe Harbor Agreement** implemented in 1995 reasserts the importance of privacy. The two-way agreement between the United States and the European Union establishes standards for information transmittal. Approved by the European Commission in July 2000, the Safe Harbor principles essentially enable U.S. companies to do business in the European Union by establishing what is deemed to be an adequate level of privacy protection. Although the document is still evolving, it establishes that companies need to enter the Safe Harbor Agreement or provide evidence that they are abiding by the privacy regulations set forth in it. Noncompliant organizations may be effectively banned from doing business in the European Union. Compliance with the Safe Harbor Agreement requires that a company meet six conditions:[17]

***Notice.*** Organizations must provide individuals with clear notice of "the purposes for which it collects and uses information about them, the types of third parties to which it discloses the information, and how to contact the company with inquiries or complaints."

***Choice.*** Before any data is collected, an organization must give its customers the opportunity to choose whether to share their sensitive information (for example, data related to factors such as health, race, or religion).

***Onward Transfer.*** Unless they have the individual's permission to do otherwise, organizations may share information only with those third parties that belong to the Safe Harbor Agreement or follow its principles.

[16] "A New Covenant with Stakeholders: Managing Privacy as a Competitive Advantage, Privacy Risk Management," © 2001 KPMG LLP, the U.S. member firm of KPMG International, a Swiss association: 22–23.

[17] Ibid.

***Security and Data Integrity.*** Organizations need to ensure that the data they maintain is accurate, complete, and current and thus reliable for use. They must also ensure the security of the information by protecting it against loss, misuse, unauthorized access, disclosure, alteration, and destruction.

***Access.*** Unless they would be unduly burdened or violate the rights of others, organizations must give individuals "access to personal data about themselves and provide an opportunity to correct, amend, or delete such data."

***Enforcement.*** Organizations must "enforce compliance, provide recourse for individuals who believe their privacy rights have been violated, and impose sanctions on their employees and agents for non-compliance."

## Audit Implications of XBRL

Although the potential benefits of XBRL and associated web technologies have been extensively researched, little attention has been given to the audit implications of using XBRL. Areas of specific concern include:

***Taxonomy Creation.*** Taxonomy may be generated incorrectly, which results in an incorrect mapping between data and taxonomy elements that could result in material misrepresentation of financial data. Controls must be designed and in place to ensure the correct generation of XBRL taxonomies.

***Validation of Instance Documents.*** As noted, once the mapping is complete and tags have been stored in the internal database, XBRL instance documents (reports) can be generated. Independent verification procedures need to be established to validate the instance documents to ensure that appropriate taxonomy and tags have been applied before posting to a web server.

***Audit Scope and Timeframe.*** Currently, auditors are responsible for printed financial statements and other materials associated with the statements. What will be the impact on the scope of auditor responsibility as a consequence of real-time distribution of financial statements across the Internet? Should auditors also be responsible for the accuracy of other related data that accompany XBRL financial statements, such as textual reports?

## Continuous Auditing

Continuous auditing techniques need to be developed that will enable the auditor to review transactions at frequent intervals or as they occur. To be effective, such an approach will need to employ **intelligent control agents** (computer programs) that embody auditor-defined heuristics that search electronic transactions for anomalies. Upon finding unusual events, the control agent will first search for similar events to identify a pattern. If the anomaly cannot be explained, the agent alerts the auditor with an alarm or exception report.

## Electronic Audit Trails

In an EDI environment, a client's trading partner's computer automatically generates electronic transactions, which are relayed across a **value-added network (VAN),**[18] and the

[18] See the appendix for discussion of VANs.

client's computer processes the transactions without human intervention. In such a setting, audits may need to be extended to critical systems of all parties involved in the transactions. Validating EDI transactions may involve the client, its trading partners, and the VAN that connects them. This could take the form of direct review of these systems or collaboration between the auditors of the trading partners and VANs.

## Confidentiality of Data

As system designs become increasingly open to accommodate trading partner transactions, mission-critical information is at risk of being exposed to intruders both from inside and outside the organization. Accountants need to understand the cryptographic techniques used to protect the confidentiality of stored and transmitted data. They need to assess the quality of encryption tools used and the effectiveness of key management procedures that CAs use. Furthermore, the term *mission-critical* defines a set of information that extends beyond the traditional financial concerns of accountants. This broader set demands a more holistic approach to assessing internal controls that ensure the confidentiality of data.

## Authentication

In traditional systems, the business paper on which it was written determines the authenticity of a sales order from a trading partner or customer. In electronic commerce systems, determining the identity of the customer is not as simple a task. With no physical forms to review and approve, authentication is accomplished through digital signatures and digital certificates. To perform their assurance function, accountants must develop the skill set needed to understand these technologies and their application.

## Nonrepudiation

Accountants are responsible for assessing the accuracy, completeness, and validity of transactions that constitute client sales, accounts receivable, purchases, and liabilities. Transactions that a trading partner can unilaterally repudiate can lead to uncollected revenues or legal action. In traditional systems, signed invoices, sales agreements, and other physical documents provide proof that a transaction occurred. As with the problem of authentication, electronic commerce systems can also use digital signatures and digital certificates to promote nonrepudiation.

## Data Integrity

A nonrepudiated transaction from an authentic trading partner may still be intercepted and rendered inaccurate in a material way. In a paper-based environment, such alterations are easy to detect. Digital transmissions, however, pose much more of a problem. To assess data integrity, accountants must become familiar with the concept of computing a digest of a document and the role of digital signatures in data transmissions.

## Access Controls

Controls need to be in place that prevent or detect unauthorized access to an organization's information system. Organizations whose systems are connected to the Internet are at greatest risk from outside intruders. Accounting firms need to be expert in assessing their clients' access controls. Many firms are now performing penetration tests, designed to assess the adequacy of their clients' access control by imitating known techniques that hackers and crackers use.

## A Changing Legal Environment

Accountants have traditionally served their clients by assessing risk (both business and legal) and devising techniques to mitigate and control risk. This risk assessment role is greatly expanded by Internet commerce, whose legal framework is still evolving in a business environment fraught with new and unforeseen risks. To estimate a client's exposure to legal liability in this setting, the public accountant must understand the potential legal implications (both domestic and international) of transactions that the client's electronic commerce system processes. For example, a web page from which customers order goods opens the organization to national and international business communities and exposes it to multiple and possibly conflicting legal statutes. Legal issues relating to taxes, privacy, security, intellectual property rights, and libel create new challenges for the accounting profession, which must provide their clients with rapid and accurate advice on a wide range of legal questions.

# Summary

This chapter focused on Internet commerce, including business-to-consumer and business-to-business relationships. Internet commerce has been the source of intense interest because it enables thousands of business enterprises of all sizes and millions of consumers to congregate and participate in worldwide commerce. The chapter examined Internet technologies, including packet switching, the World Wide Web, Internet addressing, and protocols. Several advantages of Internet commerce were reviewed, including access to worldwide markets, reductions in inventory, creation of business partnerships, reductions in prices, and better customer service.

Electronic commerce is also associated with unique risks. The primary concerns intranets pose (discussed in the appendix) come from employees. Internet risks were characterized as a number of specific fraud schemes that threaten consumer privacy and the security of transmitted and stored data. Several measures were examined that can reduce risks and promote an environment of security and trust. These include data encryption, digital certificates, firewalls, and third-party trust seals for websites.

The chapter concluded with a review of implications for accountants and the profession. The issues covered included privacy issues, continuous process auditing, electronic audit trails, and the auditors' need for new skill sets to deal with highly technical, evidential matter that redefine traditional auditing concerns.

# Appendix

# Intra-Organizational Electronic Commerce

Distributed data processing was introduced in Chapter 1 as an alternative to the centralized model. Most modern organizations use some form of distributed processing to process their transactions; some companies process all of their transactions in this way. Organizations that own or lease networks for internal business use intranets. The following section examines several intranet topologies and techniques for network control.

## Network Topologies

A network topology is the physical arrangement of the components (for example, nodes, servers, communications links, and so on) of the network. In this section, we examine the features of five basic network topologies: star, hierarchical, ring, bus, and client-server. Most networks are a variation on, or combination of, these basic models. However, before proceeding, working definitions are presented for some of the terms that will be used in the following sections.

### *Local Area Networks and Wide Area Networks*

One way of distinguishing between networks is the geographic area that their distributed sites cover. Networks are usually classified as either local area networks (LANs) or wide area networks (WANs). LANs are often confined to a single room in a building, or they may link several buildings within a close geographic area. However, a LAN can cover distances of several miles and connect hundreds of users. The computers connected to a LAN are called nodes.

When networks exceed the geographic limitations of the LAN, they are called WANs. Because of the distances involved and the high cost of telecommunication infrastructure (telephone lines and microwave channels), WANs are often commercial networks (at least in part) that the organization leases. The nodes of a WAN may include microcomputer workstations, minicomputers, mainframes, and LANs. The WAN may be used to link geographically dispersed segments of a single organization or connect multiple organizations in a trading partner arrangement.

### *Network Interface Cards*

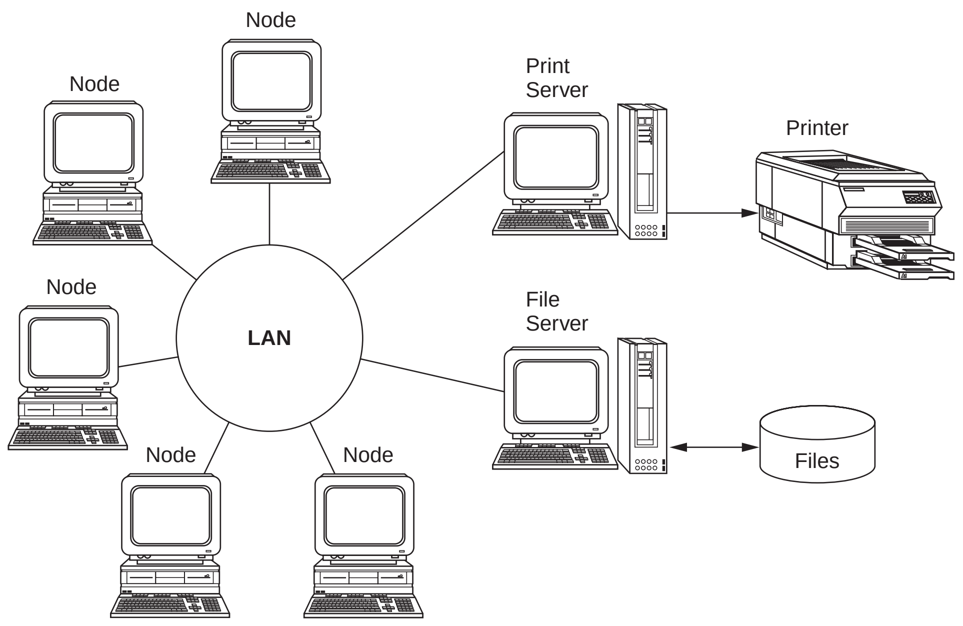
The physical connection of workstations to the LAN is achieved through a network interface card (NIC), which fits into one of the expansion slots in the microcomputer. This device provides the electronic circuitry needed for internode communications. The NIC works with the network control program to send and receive messages, programs, and files across the network.

### *Servers*

LAN nodes often share common resources such as programs, data, and printers, which are managed through special-purpose computers called servers as depicted in Figure 12-11. When the server receives requests for resources, the requests are placed in a queue and are processed in sequence.

In a distributed environment, there is often a need to link networks together. For example, users of one LAN may share data with users on a different LAN. Networks are linked via combinations of hardware and software devices called bridges and gateways. Figure 12-12 illustrates this technique. Bridges provide a means for linking LANs of the same type, for example, an IBM token ring to another IBM token ring. Gateways connect LANs of different types and are also used to link LANs to WANs. With these definitions in mind, we now turn our attention to the five basic network topologies.

FIGURE 12-11 LAN with File and Print Servers



## *Star Topology*

The star topology shown in Figure 12-13 describes a network of computers with a large central computer (the host) at the hub that has direct connections to a periphery of smaller computers. Communications between the nodes in the star are managed and controlled from the host site.

The star topology is often used for a WAN, in which the central computer is a mainframe. The nodes of the star may be microcomputer workstations, minicomputers, mainframes, or a combination. Databases under this approach may be distributed or centralized. A common model is to partition local data to

FIGURE 12-12 Bridges and Gateways Linking LANs and WANs

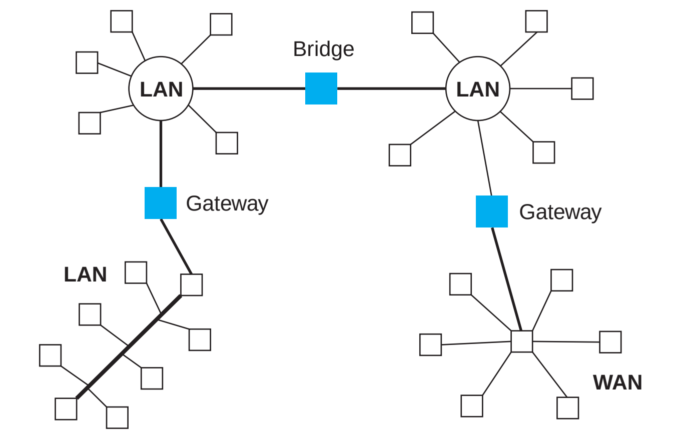
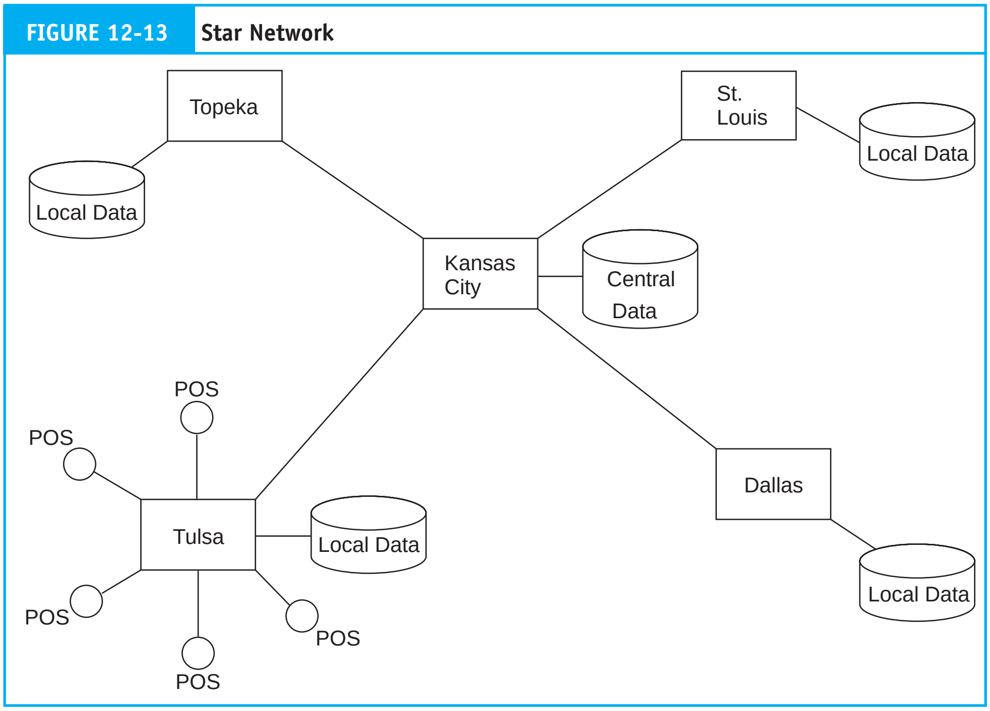


FIGURE 12-13 Star Network



the nodes and centralize the common data. For example, consider a department store chain that issues its own credit cards. Each node represents a store in a different metropolitan area. In Figure 12-13, these are Dallas, St. Louis, Topeka, and Tulsa. The nodes maintain local databases such as records for customers holding credit cards issued in their areas and records of local inventory levels. The central site—Kansas City—maintains data common to the entire regional area, including data for customer billing, accounts receivable maintenance, and overall inventory control. Each local node is itself a LAN, with point-of-sales (POS) terminals connected to a minicomputer at the store.

If one or more nodes in a star network fail, communication between the remaining nodes is still possible through the central site. However, if the central site fails, individual nodes can function locally, but cannot communicate with the other nodes.

Transaction processing in this type of configuration could proceed as follows. Sales are processed in real time at the POS terminals. Local processing includes obtaining credit approval, updating the customer's available credit, updating the inventory records, and recording the transaction in the transaction file (journal). At the end of the business day, the nodes transmit sales and inventory information to the central site in batches. The central site updates the control accounts, prepares customer bills, and determines inventory replenishment for the entire region.

The assumption underlying the star topology is that primary communication will be between the central site and the nodes. However, limited communication between the nodes is possible. For example, assume a customer from Dallas was in Tulsa and made a purchase from the Tulsa store on credit. The Tulsa database would not contain the customer's record, so Tulsa would send the transaction for credit approval to Dallas via Kansas City. Dallas would then return the approved transaction to Tulsa via Kansas City. Inventory and sales journal updates would be performed at Tulsa.

This transaction processing procedure would differ somewhat depending on the database configuration. For example, if local databases are partial replicas of the central database, credit queries could be made directly from Kansas City. However, this would require keeping the central database current with all the nodes.

## *Hierarchical Topology*

A hierarchical topology is one in which a host computer is connected to several levels of subordinate, smaller computers in a master–slave relationship. This structure is applicable to firms with many organizational levels that must be controlled from a central location. For example, consider a manufacturing firm with remote plants, warehouses, and sales offices like the one illustrated in Figure 12-14. Sales orders from the local sales departments are transmitted to the regional level, where they are summarized and uploaded to the corporate level. Sales data, combined with inventory and plant capacity data from manufacturing, are used to compute production requirements for the period, which are downloaded to the regional production scheduling system. At this level, production schedules are prepared and distributed to the local production departments. Information about completed production is uploaded from the production departments to the regional level, where production summaries are prepared and transmitted to the corporate level.

## *Ring Topology*

The ring topology illustrated in Figure 12-15 eliminates the central site. All nodes in this configuration are of equal status; thus, responsibility for managing communications is distributed among the nodes. Every node on the ring has a unique electronic address, which is attached to messages such as an address on an envelope. If Node A wishes to send a message to Node D, then Nodes B and C receive, regenerate, and pass on the message until it arrives at its destination. The ring topology is a peer-to-peer arrangement in which all nodes are of equal status. This is a popular topology for LANs. The peer nodes manage private programs and databases locally. However, a file server that is also a node on the network ring can centralize and manage common resources that all nodes share.

The ring topology may also be used for a WAN, in which case the databases may be partitioned rather than centralized. For example, consider a company with widely separated warehouses, each with different

**FIGURE 12-14** **Hierarchical Topology**

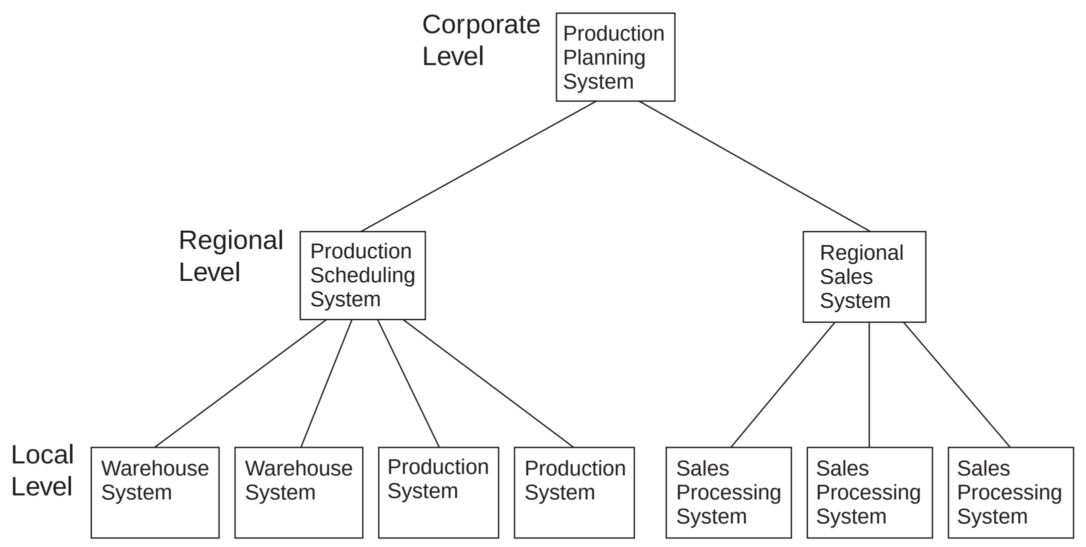
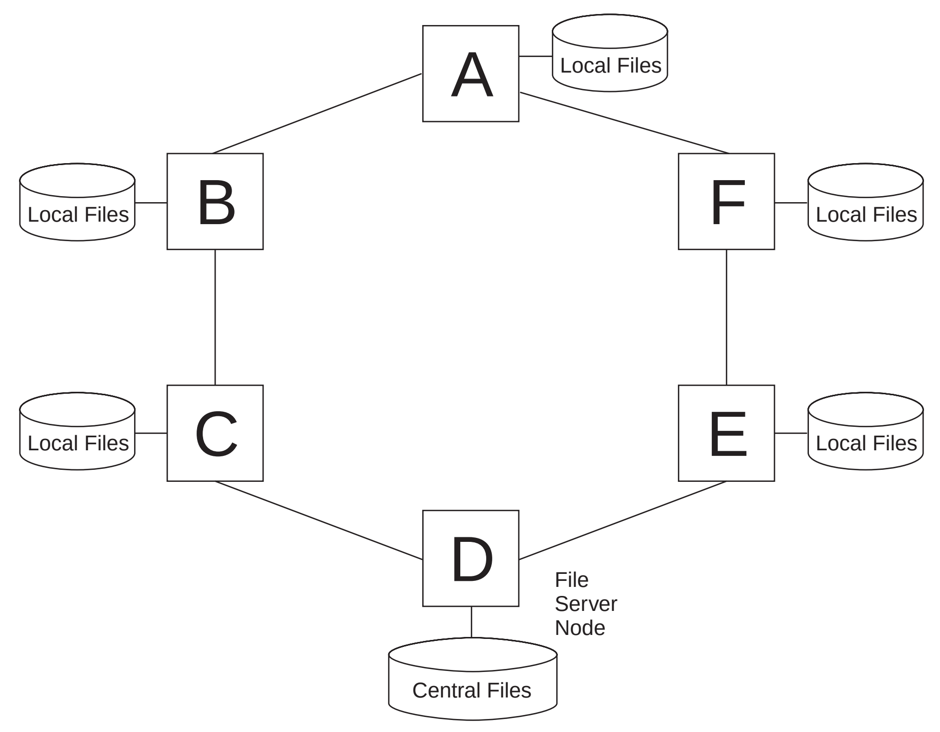


FIGURE 12-15 **Ring Topology**



suppliers and customers and each processing its own shipping and receiving transactions. In this case, where there is little 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*

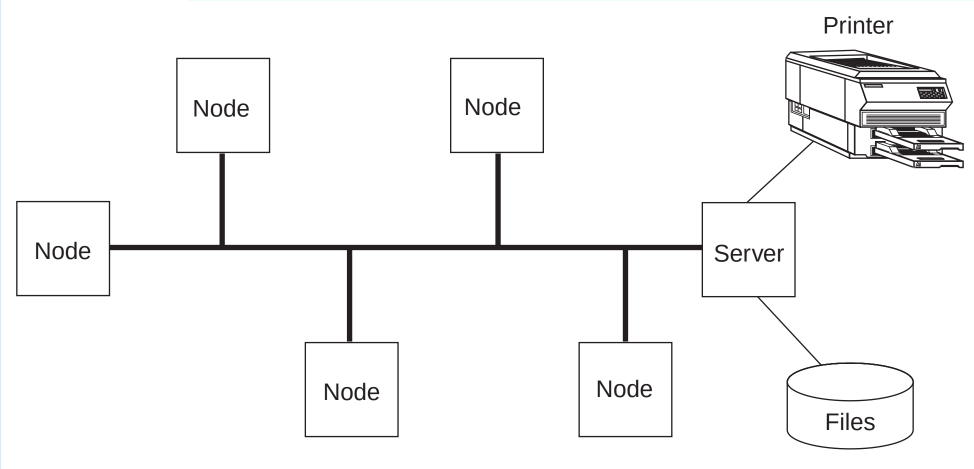
The bus topology illustrated in Figure 12-16 is the most popular LAN topology. It is so named because the nodes are all connected to a common cable—the bus. One or more servers centrally control communications and file transfers between workstations. As with the ring topology, each node on the bus has 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 12-17 illustrates the approach.

To explain the client-server difference, let’s review the features of a traditional distributed data processing system (DDP). 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

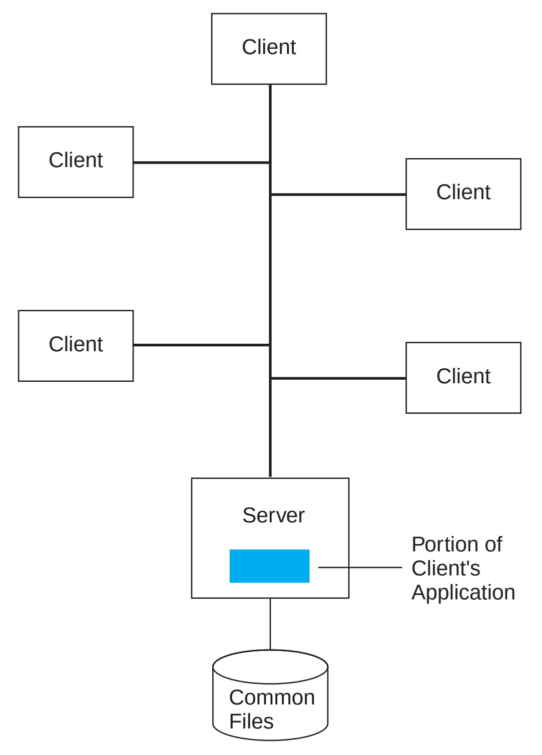
FIGURE 12-16 Bus Topology



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.

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

FIGURE 12-17 Client-Server Topology



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 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 (for example, ring, star, or bus). Figure 12-17 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*

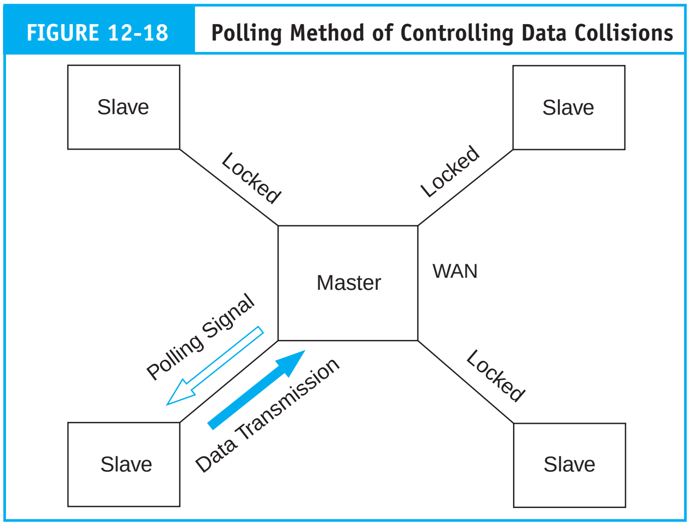
**Polling** is the most popular technique for establishing a communication session in WANs. One site, designated the master, polls the other slave sites to determine if they have data to transmit. If a slave responds in the affirmative, the master site locks the network while the data are transmitted. The remaining sites must wait until they are polled before they can transmit. The polling technique illustrated in Figure 12-18 is well suited to both the star and the hierarchical topologies. 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 12-19. Because nodes are permitted

**FIGURE 12-18** Polling Method of Controlling Data Collisions



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 on 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 below). IBM's version of token ring is emerging as an industry standard.

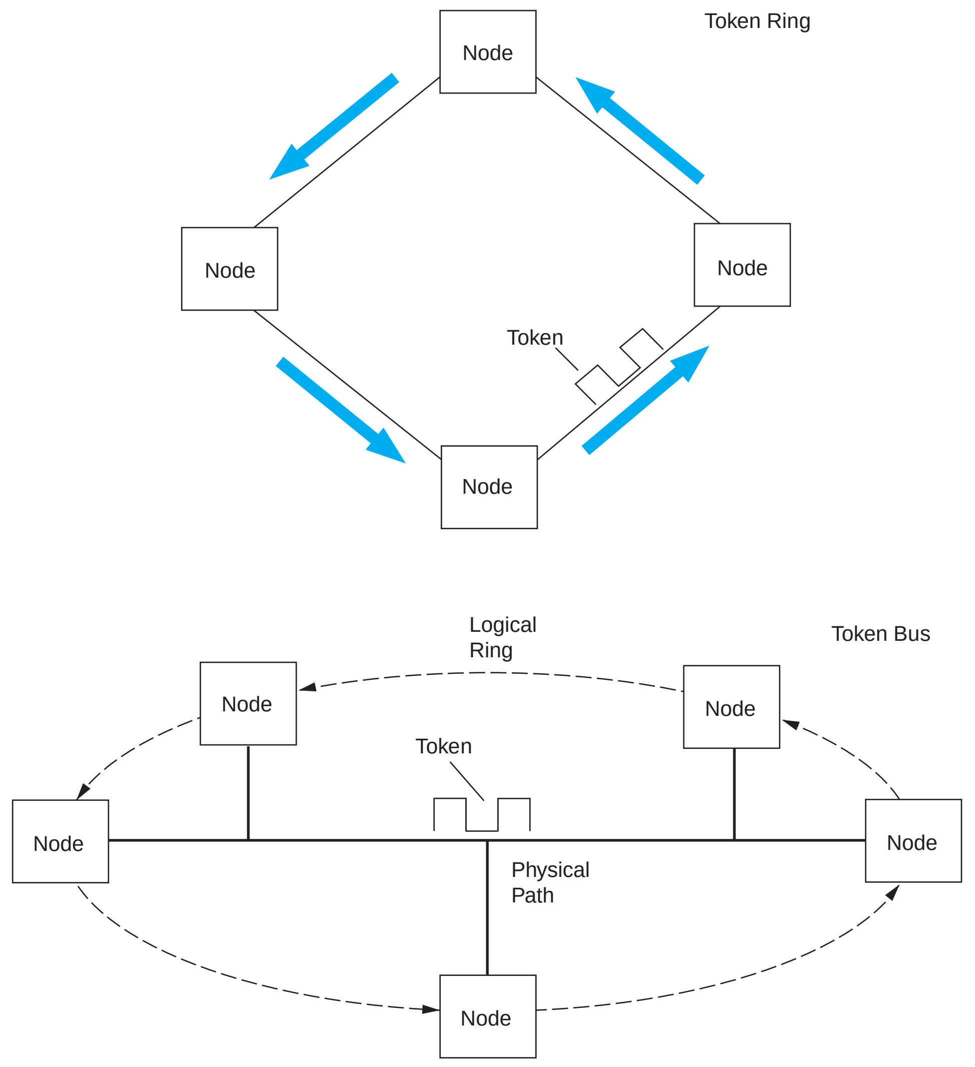
## Carrier Sensing

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 (CSMA/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.[19] 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.

[19] "The Ethernet, a Local Area Network Version 1.0." Digital Equipment Corporation, Maynard, MS; Intel Corporation, Santa Clara, CA; and Xerox Corporation, Stanford, CT.

**FIGURE 12-19** Token-Passing Approach to Controlling Data Collision



# 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 **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 interorganization 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 12-20 shows an overview of an EDI connection between two companies. Assume that the transaction in Figure 12-20 is the customer' (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 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 12-20 shows a direct communications link between companies. But many companies choose to use a third-party VAN to connect to their trading partners. Figure 12-21 illustrates this arrangement. The originating company transmits its EDI messages to the network rather than directly to the trading

**FIGURE 12-20** **Overview of EDI**

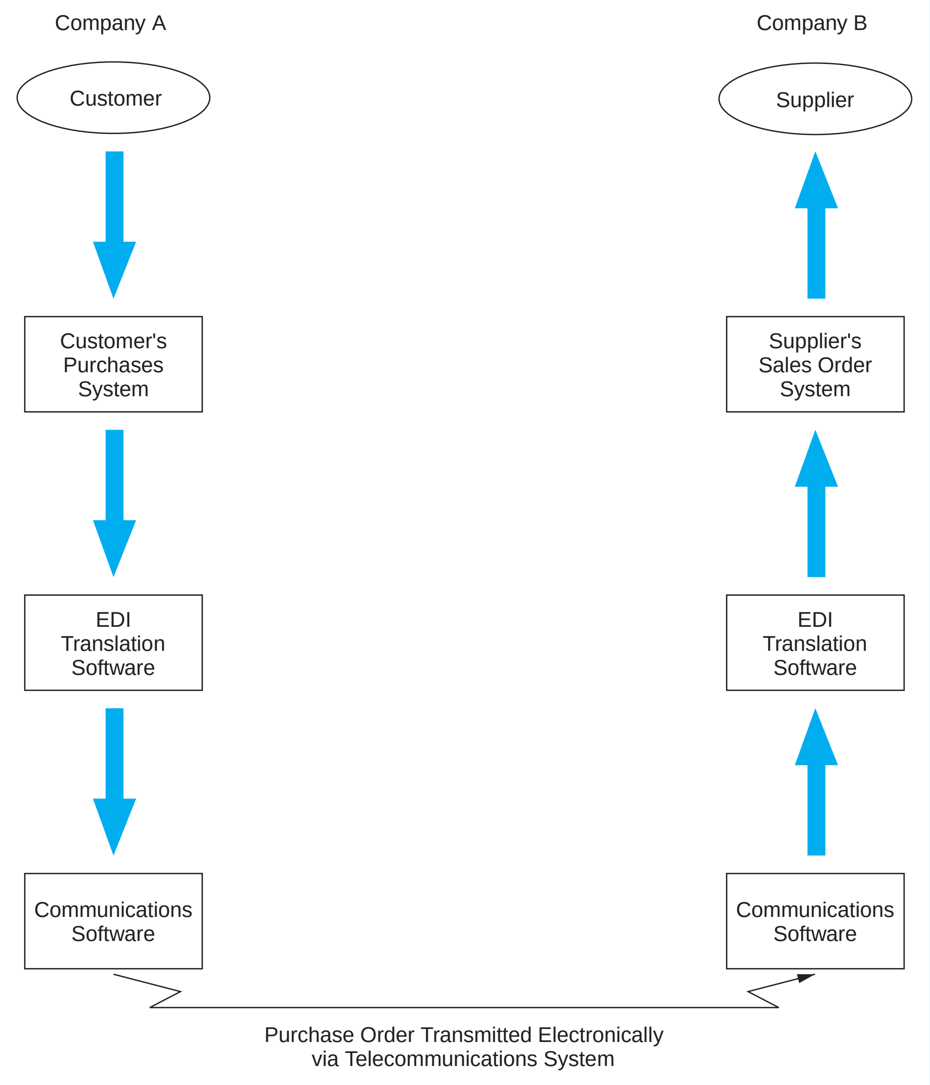
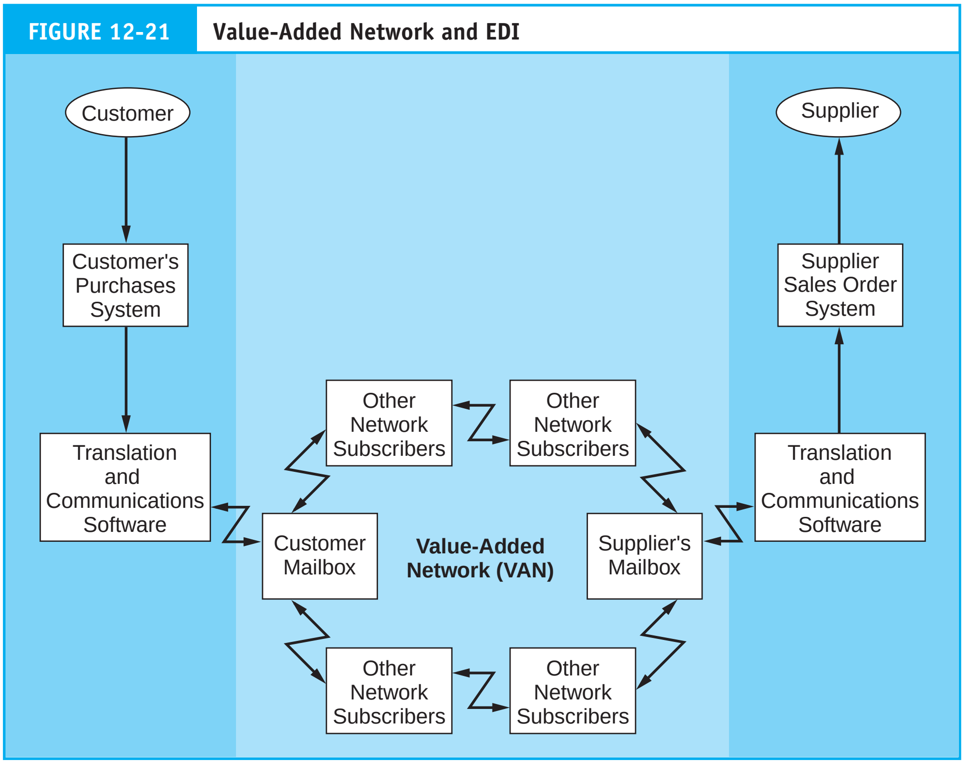


FIGURE 12-21 Value-Added Network and EDI


Customer
Customer's Purchases System
Translation and Communications Software
Customer Mailbox
Other Network Subscribers
Other Network Subscribers
Value-Added Network (VAN)
Other Network Subscribers
Other Network Subscribers
Supplier's Mailbox
Translation and Communications Software
Supplier Sales Order System
Supplier

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.

## EDI Standards

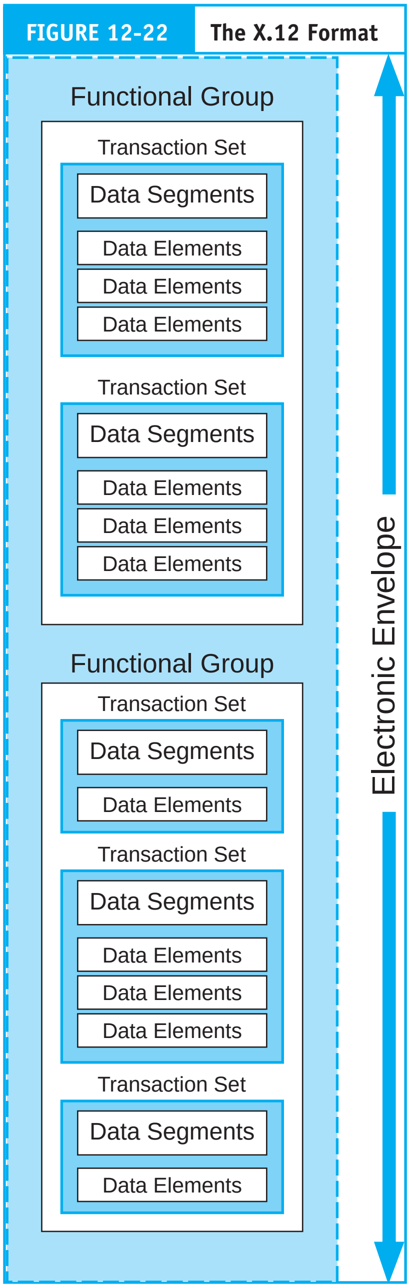
Key to EDI success is the use of a standard format for messaging between dissimilar systems. Over the years, both in the United States and internationally, a number of formats have been proposed. The standard in the United States is the American National Standards Institute (ANSI) X.12 format. The standard used internationally is the EDI For Administration, Commerce, and Transport (EDIFACT) format. Figure 12-22 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 12-23 relates these terms to a conventional document.[20]

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 12-23, these include such items as REX-446, $127.86, and Ozment Supply.

[20] J. M. Cathey, "Electronic Data Interchange: What the Controller Should Know," *Management Accounting* (November 1991): 48.

FIGURE 12-22 The X.12 Format

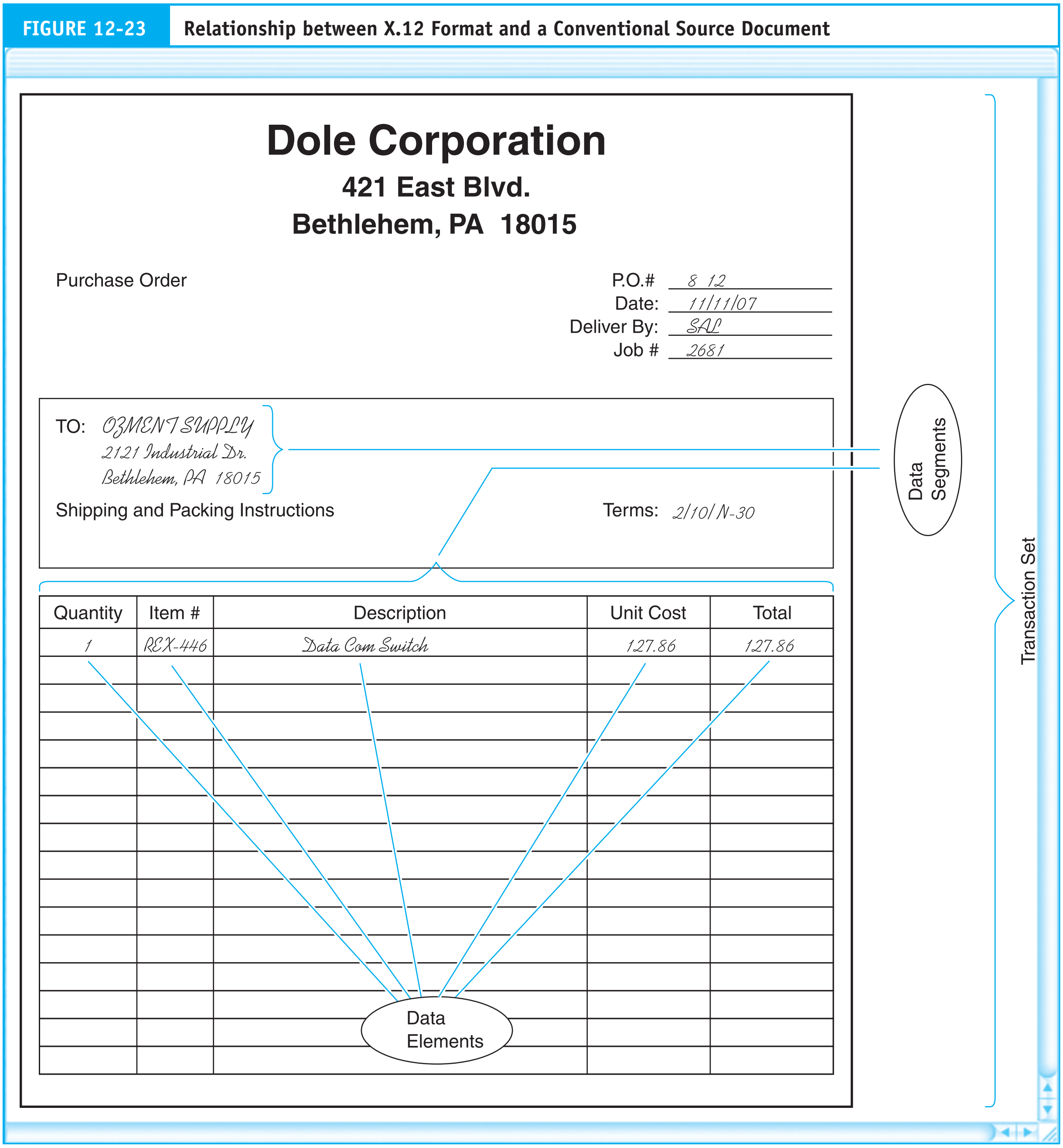


***Source:*** B. K. Stone, *One to Get Ready: How to Prepare Your Company for EDI* (CoreStates, 1988): 12.

## 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.

**FIGURE 12-23** Relationship between X.12 Format and a Conventional Source Document



# Dole Corporation

421 East Blvd.
Bethlehem, PA 18015

Purchase Order

P.O.# 8 12
Date: 11/11/07
Deliver By: SAL
Job # 2681

TO: OZMENT SUPPLY
2121 Industrial Dr.
Bethlehem, PA 18015

Shipping and Packing Instructions

Terms: 2/10/N-30

| Quantity | Item # | Description | Unit Cost | Total |
|---|---|---|---|---|
| 1 | REX-446 | Data Com Switch | 127.86 | 127.86 |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |

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

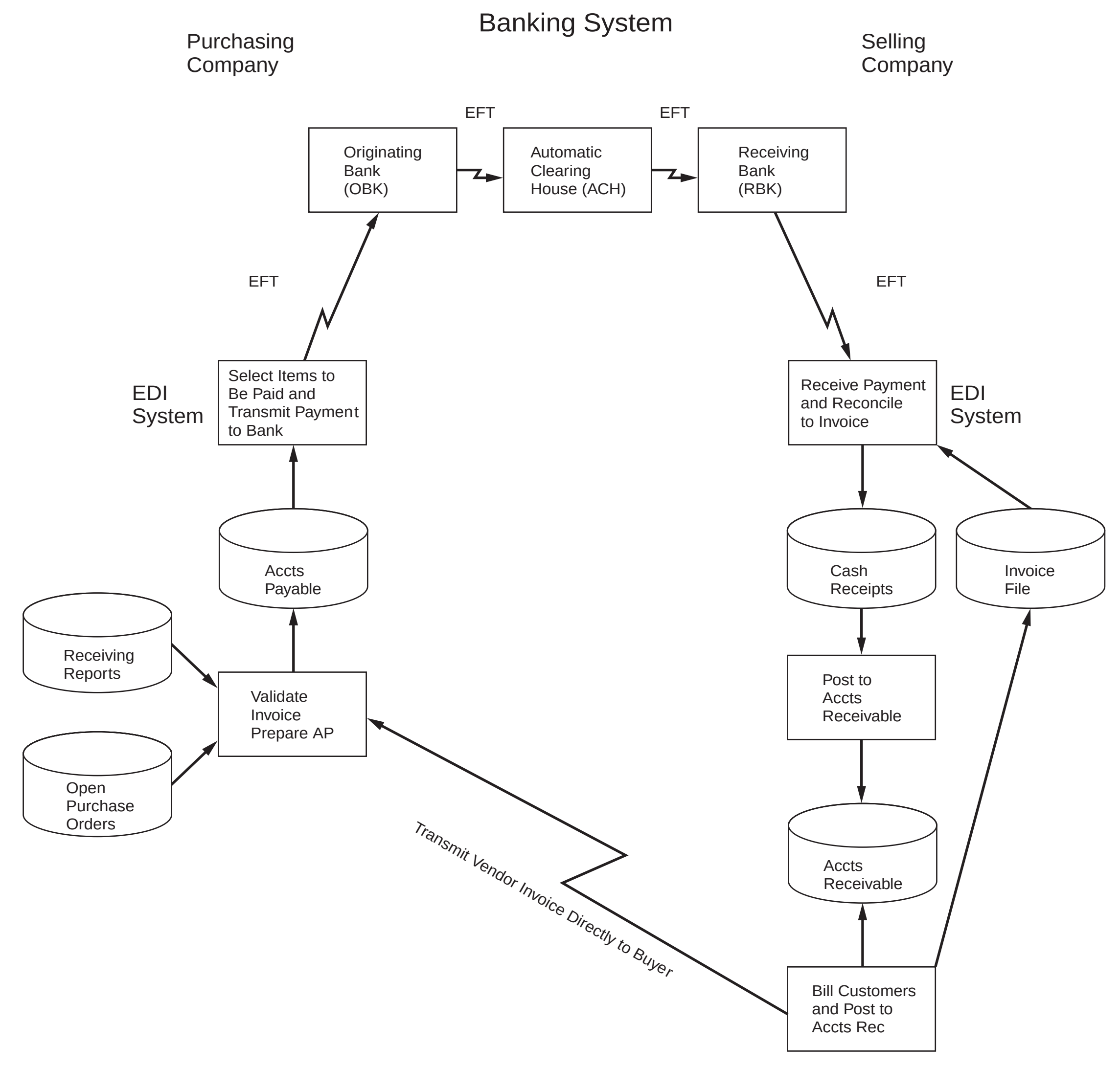
- *Data keying.* EDI reduces or even eliminates the need for data entry.
- *Error reduction.* Firms using EDI see reductions in data keying errors, human interpretation and classification errors, and filing (lost document) errors.
- *Reduction of paper.* The use of electronic envelopes and documents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

## 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 12-24. The buyer's EDI system receives the purchase

**FIGURE 12-24** **EFT Transactions between Trading Partners**



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 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 12-25 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 below.

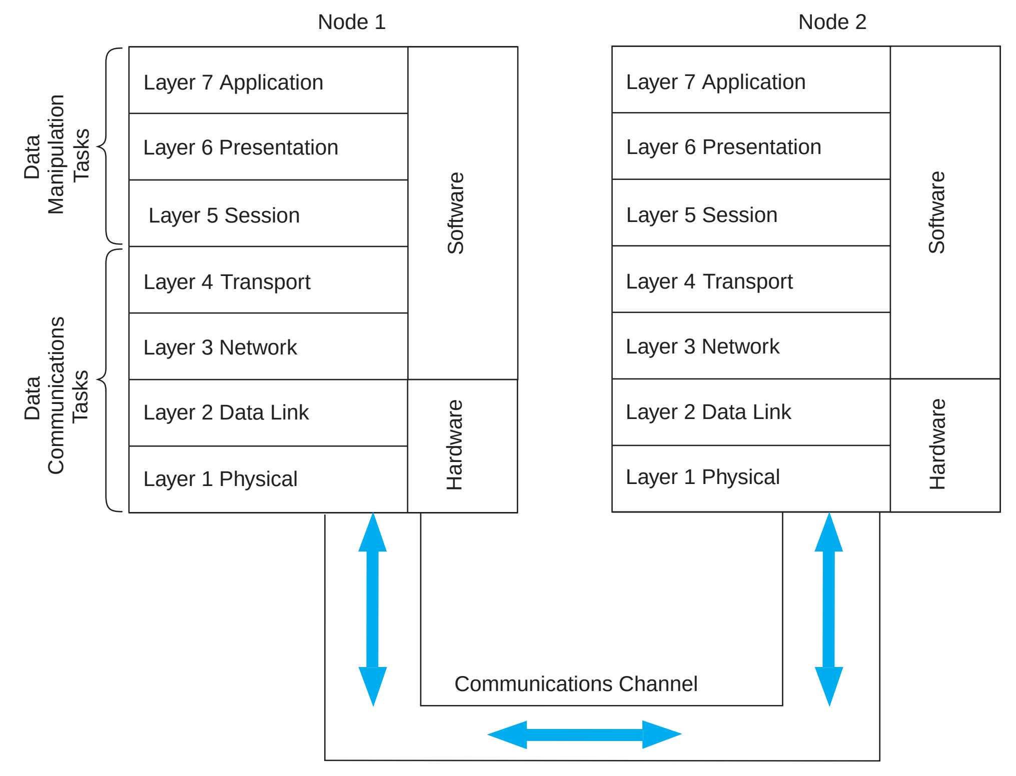
## *Layer Functions*

***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

FIGURE 12-25 The OSI Protocol



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 DBMS may provide the application layer protocols for managing file transfers.

## Key Terms

advanced encryption standard (AES) (588)
algorithm (588)
application-level firewalls (590)
botnets (584)
Caesar cipher (588)
certification authorities (CAs) (590)
cookies (582)
data collision (603)
denial of service attack (Dos) (583)
digital certificate (590)
digital envelope (588)
digital signature (588)
distributed denial of service (DDos) (584)
distribution level (578)
document name (567)
domain name (567)
dynamic virtual organization (578)
extranet (565)
firewall (590)
File Transfer Protocol (FTP) (569)
home page (566)
HyperText Markup Language (HTML) (570)
HyperText Transfer Protocol (HTTP) (566)
HyperText Transport Protocol–Next Generation (HTTP-NG) (570)
Internet Message Access Protocol (IMAP) (569)
information level (577)
intelligent control agents (594)
International Standards Organization (569)
Internet Relay Chat (IRC) (584)
IP broadcast address (584)
IP spoofing (583)
key (588)
network-level firewall (590)
Network News Transfer Protocol (NNTP) (570)
Open System Interface (OSI) (569)
packet switching (564)
ping (584)
Private Communications Technology (PCT) (570)
Privacy Enhanced Mail (PEM) (570)
polling (603)
Post Office Protocol (POP) (569)
privacy (593)
privacy violation (593)
private key (588)
protocol (567)
protocol prefix (567)
public key encryption (588)
public key infrastructure (PKI) (590)
risk (579)
Rivest-Shamir-Adleman (RSA) (588)
Safe Harbor Agreement (593)
Secure Electronic Transmission (SET) (570)
Simple Network Mail Protocol (SNMP) (569)
Secure Sockets Layer (SSL) (570)
smurf attack (584)
subdirectory name (567)
symmetric key (588)
SYNchronize–ACKnowledge (SYN-ACK) (583)
SYN flood attack (583)
Transfer Control Protocol/Internet Protocol (TCP/IP) (569)
TELNET (569)
transaction level (577)
Uniform Resource Locator (URL) (566)
value-added network (VAN) (594)
virtual private network (VPN) (565)
web page (566)
websites (566)
eXtensible Business Reporting Language (XBRL) (571)
XBRL instance document (572)
XBRL taxonomies (571)
eXtensible Markup Language (XML) (570)
zombie (584)

## Review Questions

1. What is packet switching?
2. What is a VPN?
3. Name the three types of addresses used on the Internet.
4. Describe the elements of an e-mail address.
5. Networks would be inoperable without protocols. Explain their importance and what functions they perform.
6. What is the purpose of the TCP portion of TCP/IP?
7. What does the HTTP do?
8. How do HTTP and HTTP-NG differ?
9. What is XML?
10. What is XBRL?
11. What is the World Wide Web?
12. Define IP spoofing.
13. What is a cookie?
14. What is a malicious program?
15. Who are the three parties in a smurf attack?
16. What is a ping and how does it work?
17. What is a seal of assurance?
18. Name and describe an audit implication of XBRL.
19. What is a VAN?
20. What is a LAN?
21. What is a WAN?
22. What is a NIC?
23. What is a server?
24. What is meant by the term *client-server topology*?
25. What is meant by data collision?
26. What is the purpose of EDI?
27. What is OSI?

## Discussion Questions

1. What purpose do protocols serve?
2. Explain the purpose of the two elements of TCP/IP.
3. Distinguish between the FTP and TELNET protocols.
4. Discuss the three levels of Internet business models.
5. What is a dynamic virtual organization?
6. Define risk in an electronic commerce setting.
7. How can intranet expansion increase risk to an organization?
8. What are cookies and why are they used?
9. What security concerns pertain to cookies?
10. How does IP spoofing support Internet crime?
11. Describe a distributed denial of service (DDos) attack.
12. What is a digital envelope?
13. What is a digital signature?
14. What is a digital certificate? How is it different from a digital signature?
15. Distinguish between a network-level firewall and an application-level firewall.
16. What is a certification authority, and what are the implications for the accounting profession?
17. Discuss the key aspects of the following five seal-granting organizations: BBB, TRUSTe, Veri-Sign, Inc., ICSA, and AICPA/CICA WebTrust.
18. Discuss three audit implications of XBRL.
19. Differentiate between a LAN and a WAN. Do you have either or both at your university or college?
20. Explain the purpose of each of the layers in the OSI protocol model.

## Multiple-Choice Questions

1. Which of the following statements is correct?
   a. TCP/IP is the basic protocol that permits communication between Internet sites.
   b. TCP/IP controls web browsers that access the web.
   c. TCP/IP is the document format used to produce web pages.
   d. TCP/IP is used to transfer text files, programs, spreadsheets, and databases across the Internet.
   e. TCP/IP is a low-level encryption scheme used to secure transmissions in higher-level (HTTP) format.
2. Which of the following best describes a system of computers that connects the internal users of an organization distributed over a wide geographic area?
   a. LAN
   b. Internet
   c. decentralized network
   d. multidrop network
   e. intranet
3. Sniffer software is
   a. used by malicious websites to sniff data from cookies stored on the user's hard drive.
   b. used by network administrators to analyze network traffic.
   c. used by bus topology intranets to sniff for carriers before transmitting a message to avoid data collisions.
   d. an illegal program downloaded from the web to sniff passwords from the encrypted data of Internet customers.
   e. illegal software for decoding encrypted messages transmitted over a shared intranet channel.
4. Which of the following statements is true?
   a. Cookies were originally intended to facilitate advertising on the web.
   b. Cookies always contain encrypted data.
   c. Cookies are text files and never contain encrypted data.
   d. Cookies contain the URLs of sites the user visits.
   e. Web browsers cannot function without cookies.
5. A message that is contrived to appear to be coming from a trusted or authorized source is called
   a. a denial of service attack.
   b. digital signature forging.
   c. Internet protocol spoofing.
   d. URL masquerading.
   e. a SYN-ACK packet.
6. A DDos attack
   a. is more intensive than a Dos attack because it emanates from single source.
   b. may take the form of either a SYN flood or smurf attack.
   c. is so named because it affects many victims simultaneously, which are distributed across the Internet.
   d. turns the target victim's computers into zombies that are unable to access the Internet.
   e. none of the above is correct.
7. A ping signal is used to initiate
   a. URL masquerading.
   b. digital signature forging.
   c. Internet protocol spoofing.
   d. a smurf attack
   e. a SYN-ACK packet.
8. A digital signature
   a. is the encrypted mathematical value of the message sender's name.
   b. is derived from the digest of a document that has been encrypted with the sender's private key.
   c. is derived from the digest of a document that has been encrypted with the sender's public key.
   d. is the computed digest of the sender's digital certificate.
   e. allows digital messages to be sent over an analog telephone line.

9. Which of the following statements about the client-server model is correct?
   a. It is best suited to the token ring topology because the random-access method this topology uses detects data collisions.
   b. It distributes both data and processing tasks to the server node. The client-server model can use the bus or ring topology.
   c. It is most effective when used as a bus topology because its deterministic access method avoids collisions and prevents data loss during transmissions.
   d. It is more efficient than the bus or ring topologies because it transmits an entire file of records to the requesting node rather than only a single record.
   e. It is not used in conjunction with either the bus or ring topologies.

10. Which of the following statements is correct?
    a. A bridge is used to connect a LAN and a WAN.
    b. Packet switching combines the messages of multiple users into a packet for transmission. At the receiving end, the packet is disassembled into individual messages and distributed to the user.
    c. The decision to partition a database assumes that no identifiable primary user exists in the organization.
    d. Message switching is used to establish temporary connections between network devices for the duration of a communications session.
    e. A deadlock is a temporary phenomenon that disrupts transaction processing. It will resolve itself when the primary computer completes processing its transaction and releases the data the other nodes need.

## Problems

### 1. Encryption

The coded message that follows is an encrypted message from Brutus to the Roman Senate. It was produced using the Caesar cipher method, in which each letter is shifted by a fixed number of places (determined by the key value).

OHWV GR MXOLXV RQ PRQGDB PDUFK 48

GUHVV: WRJD FDVXDO (EBRG)

***Required:***

Determine the key used to produce the coded message above and decode it.

### 2. Encryption

a. Develop a Caesar cipher-type encryption algorithm with a little more complexity in it. For example, the algorithm could alternatively shift the cleartext letters positive and negative by the amount of the key value. Variations on this are limitless.
b. Select a single-digit key.
c. Code a short message using the algorithm and key.
d. Give your instructor the algorithm, key, cleartext, and ciphertext.
e. Optional: Your instructor will randomly redistribute to the class the ciphertext messages completed in part d above. You are to decode the message you receive as an additional assignment.

### 3. Seals of Assurance

Visit 10 websites that sell products or services and record the following for each:

a. The URL.
b. Did the site issue you a cookie?
c. Did the site have a published privacy policy?
d. Does the site reserve the right to distribute or sell customer data?
e. Does the site use encryption for transmission of personal/financial data?

### 4. XBRL

John Ozment, director of special projects and analysis for Ozment's company, is responsible for preparing corporate financial analyses and monthly statements and reviewing and presenting the financial impacts of proposed strategies to upper management. Data for such financial analyses are obtained from operations and financial databases through direct queries of Ozment's department staff. Reports and charts for presentations are then prepared by hand and typed. Multiple copies are prepared and distributed to various users. The pressure on Ozment's group has intensified as demand for more and more current information increases. A solution to this reporting problem must be found.

The systems department wants to develop a proprietary software package to produce the reports automatically. The project would require the company to make a considerable programming investment. Ozment is concerned about the accuracy, completeness, and currency of data in automatically produced reports. He has heard about a reporting system called XBRL and wonders whether a new system based on this technology would not be more effective and reliable.

***Required:***

a. Research the current state of XBRL and determine if this technology is appropriate for internal reporting projects such as this.

b. Identify the enhancements to current information and reporting that the company could realize by using XBRL.

c. Discuss any data integrity, internal control, and reporting concerns associated with XBRL.

### 5. Certification Authority Licensing

Research the current state of certification authority licensing in the United States and Europe. Write a brief report of your findings.

### 6. Privacy

Visit 10 websites that sell products or services and record the URL of each. Evaluate each site's published privacy policy in terms of the conditions needed for compliance with the Safe Harbor Agreement. Write a report of your findings.

### 7. Electronic Data Interchange

The purchase order for one firm is the source document for the sales order of another firm. Consider the following purchase order and sales order data elements stored for two firms. Discuss any differences that may be problematic in transferring information between the two firms.

*Purchasing Firm:*

GH BETTIS
A Division of Galveston-Houston Corp.
1200 Post Oak Blvd.
P.O. Box 4768
Houston, TX 77637-9877

*Data Elements*

Vendor Number
Vendor Name
Vendor Address
Vendor City
Vendor State
Vendor Country
Vendor Zip Code
Purchase Order No.
Date
Shipment Destination Code
Vendor Part No.
Item Description
Quantity Ordered
Unit Price
Total

*Selling Firm:*

Oakland Steel Company
469 Lakeland Blvd.
Chicago, IL 60613-8888

*Data Elements*

Customer Number
Customer Name
Customer Address
Customer City
Customer State

Customer Country
Customer Zip Code
Purchase Order No.
Sales Order No.
Date
Shipping Company
Vendor Part No.
Item Description
Quantity Ordered
Unit Price
Total
Discount Offered
Tax
Freight Charges

### 8. Internal Controls Assessment and Electronic Data Interchange: Gresko Toys Factory

*(Prepared by Robertos Karahannas, Lehigh University)*

Mr. and Mrs. Gresko started Gresko Toys in the early 1960s. Initially, the company was small and few toys were produced. The talent and skills of Mr. Gresko were by far the major assets of the company. Toys were mainly made of wood and had few or no electronic parts; they were mainly manually operated and included toy cars, several kinds of dolls, and toy guns. Gresko Toys became part of the Pennsylvania tradition. Kids loved them and parents had no choice but to buy them.

Gresko Toys quickly expanded, and by 1969 it reported a sales volume of $400,000, $50,000 of which was profit. Such profits caught the attention of other businesspeople, who began entering the market. The innovative spirit of some competitors through the introduction of fancy, battery-operated toys stole some of Gresko's market share. As the competition became more intense, the Greskos saw their market share declining even further. Children liked battery-operated toys.

Mr. Gresko saw this as both a threat and a challenge. He would not give up, however. He knew that he needed better machinery to make competitive toys. With a loan from the local bank and his savings, he sought and bought what he needed. After a period of training and test marketing, Gresko Toys was again in the market and boosting sales. However, the company was generating orders that the factory could not handle. The workforce rose from a low of 50 to a high of 350 people. Most of the workforce was on the factory floor. More equipment was purchased and the company has been expanding ever since.

Today, the company sells $20 million of toys per year. The president of the company is Mrs. Gresko. Mr. Gresko felt that he should be on the factory floor managing production. Under him are the purchasing agent, supervising a buyer; the warehouse manager, managing two inventory clerks; a chief engineer; and a supervisor who is in charge of the factory workers. The controller of the company is Randi, the Greskos' elder daughter. An accounting clerk, a cashier, and a personnel manager work for her. Finally, Bob, the Greskos' only son, is the sales manager. A credit manager and two salespeople work for him.

#### *Company Information*

At present, the company's profit margin is 9 percent, only 2 percent below the industry average. According to Mr. Gresko, $850,000 in sales was lost last year because of insufficient inventory of parts. Because of the seasonal nature of the market and the short popularity span of most toys, Gresko customers require fast delivery; if the parts are not available, it takes at least two weeks to get the paperwork ready, order the parts, and have the suppliers deliver them. Some customers cannot wait that long; others order the toys and subsequently cancel the order if it takes too long to complete. Often orders are accepted on the assumption that the parts are readily available in the warehouse; when they are not, orders are delayed for weeks. A missing part not only delays an order, but the whole assembly line.

To alleviate the problem, many parts are rushed in, which raises the cost of the toys tremendously. The fine quality of the products allows for slight price increases to make up for part of the extra cost, but customers have already complained about such price fluctuations.

The Greskos are on good terms with their suppliers. After all, the market is so competitive that a reliable supplier is crucial to a firm's survival. Most of their major suppliers are located in Pennsylvania, where the Greskos have about 35 percent of the market share. However, those suppliers deal with the Greskos' competitors as well. There are about a dozen suppliers with whom the Greskos deal; eight of them supply about 95 percent of all inventory parts.

Even though good supplier relations are crucial to Gresko Toys, suppliers have often complained about the Greskos' promptness in paying. The Greskos demand on-time delivery; the payment of the supplier invoice, however, is usually not timely. Mr. Gresko said that he does not have the time to run from the factory to the accounting department to make sure payments are on time. Late payments, however, also mean a loss of the 2 percent discount the suppliers offer for early payment.

Besides resulting in lost sales, insufficient inventory of parts also delays the whole assembly line. Workers spend much time switching jobs. A just-in-time inventory system would, according to Mr. Gresko, be more appropriate for the factory. If the parts were available in the warehouse, the machines could be set up on an assembly-line fashion and operated on scheduled runs. But the fact that the necessary parts are frequently missing, forcing production to switch to another job, is a major obstacle to a just-in-time inventory system.

### *The Purchasing Cycle*

Gresko Toys is very involved in purchasing the parts used in the production of toys. The company uses a periodic inventory system. When sales orders are received, Bob Gresko sends a copy to the production floor. This copy is used to trigger production as well as to indicate the potential need of parts not available in inventory. The inventory clerks search for parts; when parts are out of stock, the inventory clerks issue two copies of a purchase requisition. Mr. Gresko approves this requisition before a purchase order is issued. One copy is sent to the purchasing manager and the other to the accounting department.

The buyer checks the suppliers' prices for the needed parts. Based on cost as well as past experience with a particular supplier, two suppliers are recommended. The purchasing manager subsequently decides on the supplier, and four copies of a purchase order are issued. The first copy is sent to the supplier, the purchasing manager files the second copy, the third is sent to the warehouse, and the fourth is sent to the accounting department. All purchase order copies are filed by supplier number.

Approximately a week after the initiation of the purchase, the parts are received. The warehouse manager, along with the inventory clerks, inspect and count the received parts. The purchase order copy that the purchasing manager previously received is used as the basis of comparison. A receiving report in three parts is prepared. If prices and quantities received agree with those ordered and with the information on the packing slip the carrier receives, the parts are accepted. If any differences exist, Mr. Gresko is called in to decide whether to accept or reject the parts. On many occasions, acceptance of parts will be delayed for days until the suppliers are informed and an agreement is reached.

One copy of the receiving report is sent to the purchasing manager and another to the accounting department. The original copy is kept at the warehouse. The accounting clerk files the receiving report along with the purchase requisition and the purchase order by supplier number. The clerk also prepares the necessary journal entry and credits the related supplier in the subsidiary ledger. When the supplier sends the invoice, the accounting clerk matches the information to the purchase requisition, purchase order, and receiving report and prepares a disbursement voucher. This voucher is used for two purposes. It initiates the journal entry for the disbursement of cash, and the cashier uses it to issue a check. Randi Gresko, as well as Mrs. Gresko, must sign the checks before they are sent to the suppliers.

### *Electronic Data Interchange*

In search of anything that could improve the present system at the Gresko Toys factory, Mr. Gresko came across the EDI system. One of his suppliers had attended a conference on EDI and had supplied Mr. Gresko with the conference material. Looking at the present system, Mr. Gresko tried to find EDI applications that would benefit the company's operations and at the same time improve its financial position.

For EDI to be implemented, certain databases will need to be established. An inventory master file with all relevant information is the key to the system. Predetermined order quantities and minimum inventory levels will need to be set for each item based on forecasts. At the warehouse, the inventory clerks will be constantly updating this database. When inventory levels drop below acceptable levels, an EDI purchase requisition will be issued to the purchasing department.

A supplier master file with related information on supplier performance will be accessed to identify potential suppliers. Depending on how advanced the system is, the computer or the purchasing manager will choose the proper supplier and issue an EDI order. This means that the factory's suppliers will also need to be using EDI.

Various ways of developing EDI links with suppliers are available. In the Gresko case, developing an independent system seems more appropriate; it is cheaper and perhaps easier to convince suppliers to join in. Software is readily available in the market and is easy to set up. Someone, however, should help set up the EDI links with the suppliers.

Once an EDI order is issued, the supplier will receive the message instantaneously. The open purchase order will be kept in a database until the receipt of the parts. Any changes to the order can be made by accessing the particular transmitted order and making the change. Suppliers can send the parts as well as their invoices more quickly. An EDI invoice can be sent to the Gresko factory upon shipment.

On arrival of the parts, the receiving clerk will prepare a receiving report and file it in a receiving database file. This report will be used to verify prices by accessing the purchase order. Credit terms, volume discounts, trade allowances, and other adjustments to quoted prices can be settled through EDI-transmitted messages. If adjustments from disagreements occur, the transaction is entered into the adjusted database file. The inventory master file is also updated, and the open purchase order is closed. In addition, the supplier-history file and the accounts payable file are updated, and an evaluated receipts settlement (ERS) is established.

An ERS is a database containing records to be used for the payment of suppliers. The EDI order is matched against the receiving and adjusted database files. This comparison creates a payment input file that contains the following three data items: (1) the scheduled payment date, within which any discount can be obtained; (2) the latest possible payment date; and (3) the remittance record for such payments.

At the beginning of every day, the treasurer (who presently does not exist at Gresko Toys) should receive a listing of the payment input file; this listing will indicate what has to be paid and when. The treasurer will initiate an EDI payment pending the approval of Mrs. Gresko. Upon approval and the transmission of the payment, the supplier records as well as the accounts payable records will be automatically updated. For an EFT to occur, the banks that serve Gresko and its suppliers will also need to be using EDI. If such intermediary banks are not using EDI, Gresko and its suppliers will need to rely on a manual system of cash disbursement to settle their transactions.

### *Conclusion*

Mr. Gresko has hired you to look at the present accounting system and his suggested EDI implementation plan. He wants you to identify the problem areas and look into the feasibility of setting up EDI links with the company's suppliers.

***Required:***

a. Draw a document flowchart of the present accounting system at Gresko.

b. What control problems, if any, exist in the accounting system?

c. Draw a document flowchart of the accounting system of the Gresko Toys factory using EDI as Mr. Gresko suggested.

d. Do some research on your own. What EDI options, other than the one Mr. Gresko suggested, are available to the Gresko Toys factory?

e. Discuss the possible implementation of an EDI system at the Gresko Toys factory. What areas should Mr. Gresko concentrate on, and what are the related issues associated with implementing EDI at the factory?

## 9. Electronic Fraud

In a recent financial fraud case, city employees in Brooklyn, New York, accessed electronic databases to defraud the city of $20 million. Several employees in collusion with the former deputy tax collector completely erased or reduced $13 million in property taxes and $7 million in accrued interest that taxpayers owed. In exchange for this service, the taxpayers paid the employees involved bribes of 10 to 30 percent of their bills.

***Required:***
Discuss the control techniques that could prevent or detect this fraud.

## 10. Santa'sAttic.com

Santa'sAttic.com is an online retailer/manufacturer of children's toys. Its main competitors are larger electronic commerce toy companies including Amazon.com; Yahoo Shopping, which includes ToysRUs.com and KBKids .com; and all of the other retail stores with online shopping. It has a low market share compared to the industry leaders and is possibly a victim of Internet fraud. The CEO of Santa'sAttic.com has noticed that the level of accounts receivable has been quite high in comparison to prior years. He is wondering if this is a sign of weak internal controls. He has also heard through the grapevine that some of his customers were noticing unauthorized charges on their credit cards and is wondering if there may be online security issues to deal with as well. For this reason, you have been contacted to help Santa'sAttic.com restructure its company to prevent possible company failure.

Santa'sAttic.com employs 100 individuals, 75 of whom work directly on the manufacturing line and 25 of whom hold administrative positions. Its customer base consists mainly of individuals, but also smaller toy stores, day care centers, and schools. Santa'sAttic.com works on a cash basis with its customers and accepts all major credit cards. It has running credit balances with all of its suppliers. Its credit terms are 2/10, n30.

Being the technical genius that he is, the vice president of marketing took it upon himself to design the company website. The website has pages where customers can view all of the products and prices. There is a virtual shopping cart available for each customer once he or she has set up a demographical information account. If the customer chooses to make a purchase, he or she simply clicks on the direct link to the shopping cart from the product that he or she wishes to purchase and proceeds to the checkout. Here the customer is prompted to choose a payment method and enter the shipping address. Once this information has been entered, the customer chooses a shipping method. All shipping is done through U.S. Mail, UPS, Federal Express, Airborne Express, or certified mail. The customer is then informed of the total price and the date to expect shipment.

Within the purchasing system, Santa'sAttic.com purchases raw materials for production, such as plastics, wood, metal, and certain fabrics. There is no formal purchasing department at Santa'sAttic.com. Judy, the inventory clerk in the warehouse department, is responsible for all purchasing activity. Santa'sAttic.com currently has only one warehouse, which is located in Cooperstown, New York. Within the warehouse department, Judy has access to the inventory records and knows when certain materials have to be repurchased. If materials are needed, she prepares a single purchase requisition and also five copies of the purchase order form. Judy includes all of the necessary information on all copies of the form, including the material to be purchased, the price of the material, the quantity needed, and the requested delivery date. Once completed, two copies of the form are sent to the vendor along with the order. One is placed in the open purchase order file in the warehouse, and one is used to update the inventory records that are also kept within the warehouse department. The final copy is forwarded to the receiving department.

Harry, the receiving clerk, receives the materials and creates four copies of a receiving report based on the packing slip and purchase order information. Two of these receiving reports are forwarded to the warehouse, where one is used to update inventory records and the other is filed. One copy of the receiving report is also maintained within the receiving department and is filed along with the packing slip and the purchase order. The final copy is sent to the accounts payable department, where it is reconciled with the vendor invoice.

Once the receiving report and the vendor invoice are reconciled in the accounts payable department, the liability is posted to the purchases journal and the total amount due is paid to the vendor. Finally, both the receiving report and the invoice are filed within the accounts payable department and Joanna, the accounts payable clerk, posts the liability to the general ledger.

Santa'sAttic.com's production workers each have timecards that they punch at a punch-in station when they arrive and when they leave. The punch-in station is located at the entrance to the plant and is not monitored. At the end of the week, the supervisor reviews, authorizes, and signs the timecards. He then sends the timecards to cash disbursements. Supervisors do not keep their own attendance records. Rose, in cash disbursements, receives the timecards and reconciles them with personnel records on the company database to verify the timecards for accuracy.

All personnel records are maintained in a database. Access to the database is restricted. Personnel can update the records only once a year. Rose's only view displays employee demographic information and does not allow access to salary information. Rose prepares the paychecks and signs them. She then prepares the payroll register using only information gained from the timecards.

Sally in accounts payable receives a copy of the payroll register and uses it to update the general ledger. Accounts payable receives no information besides the payroll register. Rose, in cash disbursements, hands the prepared paychecks to the supervisors of each department for distribution. All checks are written directly from the company's only cash account. Supervisors distribute the checks directly to the employees and themselves.

Engaging in electronic commerce has exposed Santa'sAttic.com to a whole new nature of risks within its real-time revenue cycle. A customer has the option of paying with a credit card or personal check. Upon entering the credit card information, it becomes attached to the customer's e-mail file. This information includes the type of card, the customer's name as it appears on the card, the credit card number, and the expiration date. Once an order is placed, an employee reviews the order in question, verifies credit, and enters the transaction into Santa'sAttic.com's main database.

The main problem with this system is that orders have been placed with the company where the customer in question honestly denies ever submitting orders. It turns out that their children have placed many of these orders without the customer's knowledge. The children were able to gain access to their parent's account after the system recognized cookies in the hard drive. When the children went to the website, the page recognized them as the users of the account and gave them authorized access to make purchases.

Another problem with the information in the revenue cycle has been that hackers have been able to enter the database and obtain information concerning customers. This unauthorized access has sent top management into a frenzy knowing that their customer information is insecure.

***Required:***

a. Discuss the control and security weaknesses in this system.

b. Make specific recommendations for improving controls.