PLUG-IN

B5 Networks and Telecommunications

LEARNING OUTCOMES

1. Compare LANs, WANs, and MANs.
2. List and describe the four components that differentiate networks.
3. Compare the two types of network architectures.
4. Explain topology and the different types found in networks.
5. Describe TCP/IP along with its primary purpose.
6. Identify the different media types found in networks.
7. Describe the business benefits associated with VoIP.
8. Explain the difference between a VPN and a VAN.
9. Identify the advantages and disadvantages of broadband technology.
10. List and describe many of the network security problems.

Networks and Telecommunications

Change is everywhere in the information technology domain, but nowhere is change more evident and more dramatic than in the realm of telecommunications and networking. Most information systems today rely on digital networks to communicate information in the form of data, graphics, video, and voice.

Companies large and small from all over the world use networked systems and the Internet to locate suppliers and buyers, to negotiate contracts with them, and to provide bigger, better, and faster services than ever before.

Telecommunication systems enable the transmission of data over public or private networks. A ***network*** is a communications, data exchange, and resource-sharing system created by linking two or more computers and establishing standards, or protocols, so that they can work together. Telecommunication systems and networks are traditionally complicated and historically inefficient. However, businesses can benefit from today's modern network infrastructures that provide reliable global reach to employees and customers. Businesses around the world are moving to network infrastructure solutions that allow greater choice in how they go to market—solutions with global reach. Plug-In B5 takes a detailed look at key network and telecommunication technologies being integrated into businesses around the world.

Network Basics

Networks range from small two-computer networks to the biggest network of all, the Internet. A network provides two principal benefits: the ability to communicate and the ability to share. Music is the hot product line at coffee retailer Starbucks. In Starbucks stores, customers can shop for music wirelessly through iTunes free, thanks to the company's own increasingly sophisticated in-store network.

Today's corporate digital networks include a combination of local area networks and the Internet. A ***local area network (LAN)*** is designed to connect a group of computers in close proximity to each other such as in an office building, a school, or a home. A LAN is useful for sharing resources like files, printers, games, or other applications. A LAN in turn often connects to other LANs, and to the Internet or wide area networks. A ***wide area network (WAN)*** spans a large geographic area, such as a state, province, or country. WANs often connect multiple smaller networks, such as local area networks or metropolitan area networks (MANs). A ***metropolitan area network (MAN)*** is a large computer network usually spanning a city. Email is the most popular form of network communication. Figure B5.1 illustrates each network type.

Networks are differentiated by the following:

- Architecture—peer-to-peer, client/server.
- Topology—bus, star, ring, hybrid, wireless.
- Protocols—Ethernet, Transmission Control Protocol/Internet Protocol (TCP/IP).
- Media—coaxial, twisted-pair, fiber-optic.

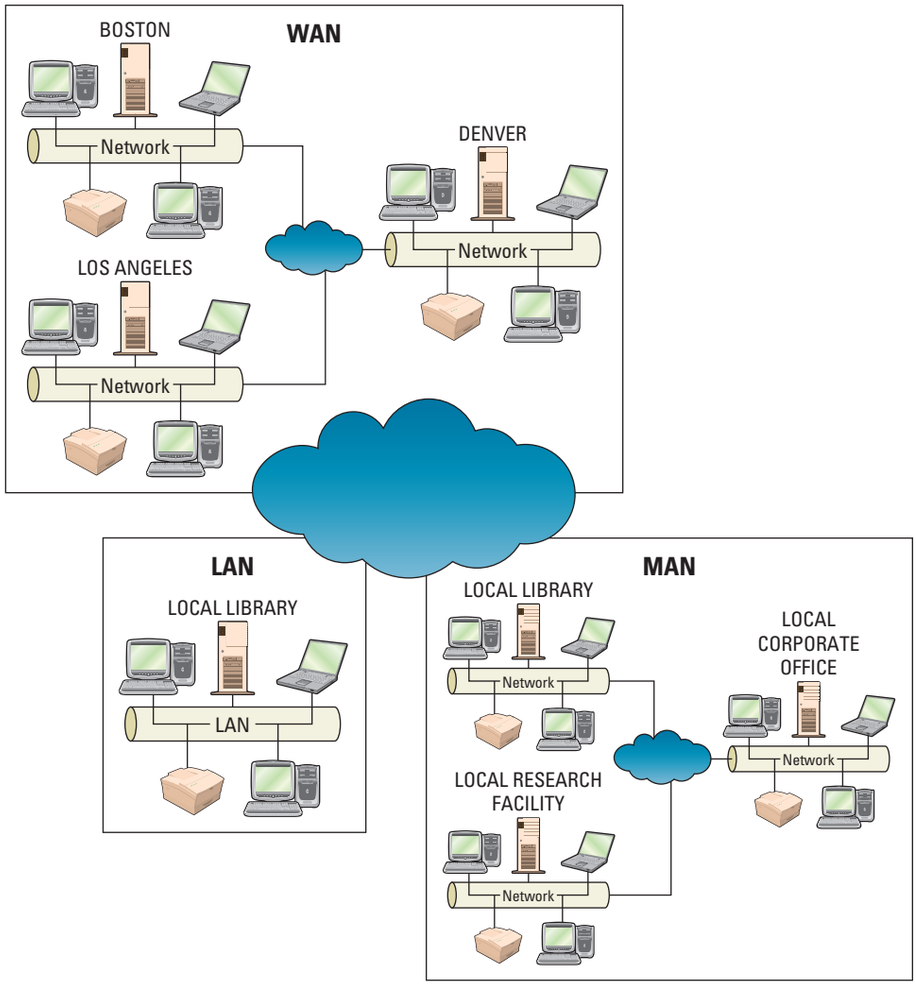


FIGURE B5.1
LAN, WAN, and MAN

Architecture

The two primary types of network architectures are: peer-to-peer networks and client/server networks.

PEER-TO-PEER NETWORKS

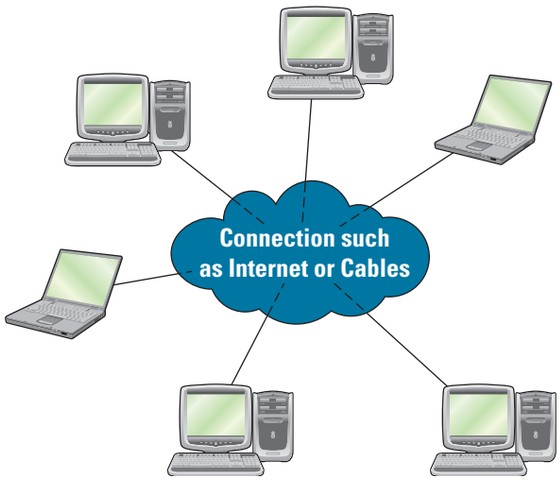


FIGURE B5.2
Peer-to-Peer (P2P) Networks

A ***peer-to-peer (P2P) network*** is any network without a central file server and in which all computers in the network have access to the public files located on all other workstations, as illustrated in Figure B5.2. Each networked computer can allow other computers to access its files and use connected printers while it is in use as a workstation without the aid of a server.

While Napster may be the most widely known example of a P2P implementation, it may also be one of the most narrowly focused since the Napster model takes advantage of only one of the many capabilities of P2P computing: file sharing. The technology has far broader capabilities, including the sharing of processing, memory, and storage, and the supporting of collaboration among vast numbers of distributed computers. Peer-to-peer computing enables immediate interaction among people and computer systems.

CLIENT/SERVER NETWORKS

A ***client*** is a computer that is designed to request information from a server. A ***server*** is a computer that is dedicated to providing information in response to external requests. A ***client/server network*** is a model for applications in which the bulk of the back-end processing, such as performing a physical search of a database, takes place on a server, while the front-end processing, which involves communicating with the users, is handled by the clients (see Figure B5.3). A ***network operating system (NOS)*** is the operating system that runs a network, steering information between computers and managing security and users. The client/server model has become one of the central ideas of network computing. Most business applications written today use the client/server model.

A fundamental part of client/server architecture is packet-switching. ***Packet-switching*** occurs when the sending computer divides a message into a number of efficiently sized units called packets, each of which contains the address of the destination computer. Each packet is sent on the network and intercepted by routers. A ***router*** is an intelligent connecting device that examines each packet of data it receives and then decides which way to send it onward toward its destination. The packets arrive at their intended destination, although some may have actually traveled by different physical paths, and the receiving computer assembles the packets and delivers the message to the appropriate application. The number of network routers being installed by businesses worldwide is booming (see Figure B5.4).

Eva Chen, CIO at Trend Micro, built a router that helps prevent worms and viruses from entering networks. The problem with most existing antivirus software is that it starts working after a destructive sequence of code is identified, meaning it starts doing its job only after the virus or worm has been unleashed inside the network. Chen's router, the Network VirusWall, sits on the edge of a corporate network, scanning data packets and detaining those that might contain viruses or worms. Any suspicious packets are compared with up-to-the-second information from Trend Micro's virus-tracking command center. Viruses and worms are then deleted and refused entry to the network, allowing the company to perform a preemptive strike.

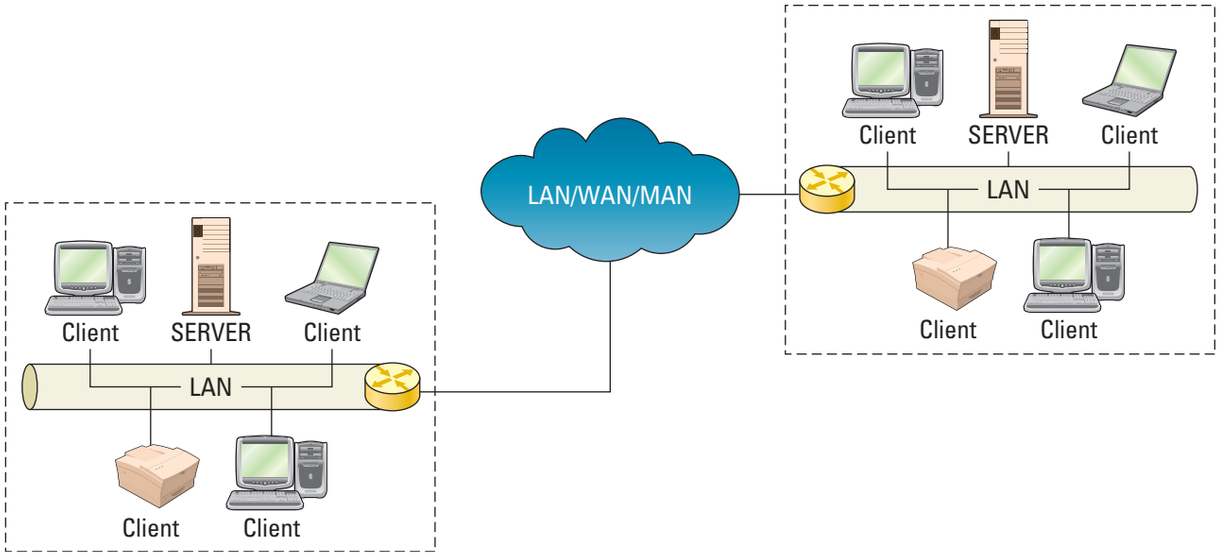


FIGURE B5.3
Client/Server Network

Topology

Networks are assembled according to certain rules. Cables, for example, have to be a certain length; each cable strand can support only a certain amount of network traffic. A ***network topology*** refers to the geometric arrangement of the actual physical organization of the computers (and other network devices) in a network. Topologies vary depending on cost and functionality. Figure B5.5 highlights the five common topologies used in networks, and Figure B5.6 displays each topology.

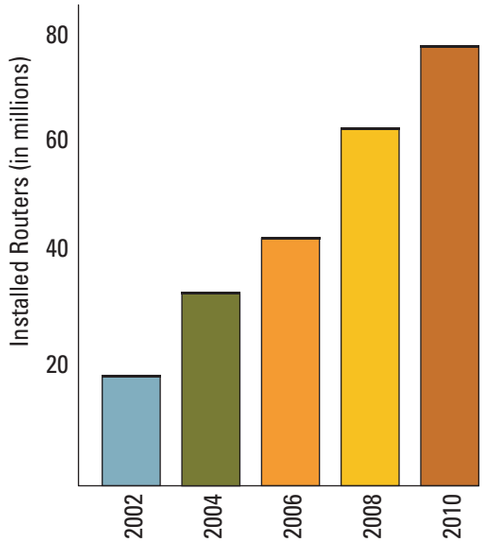


FIGURE B5.4
Worldwide Router Growth

Protocols

A ***protocol*** is a standard that specifies the format of data as well as the rules to be followed during transmission. Simply put, for one computer (or computer program) to talk to another computer (or computer program) they must both be talking the same language, and this language is called a protocol.

A protocol is based on an agreed-upon and established standard, and this way all manufacturers of hardware and software that are using the protocol do so in a similar fashion to allow for interoperability. ***Interoperability*** is the capability of two or more computer systems to share data and resources, even though they are made by different manufacturers. The most popular network protocols used are Ethernet and Transmission Control Protocol/Internet Protocol (TCP/IP).

ETHERNET

Ethernet is a physical and data layer technology for LAN networking (see Figure B5.7). Ethernet is the most widely installed LAN access method, originally developed by Xerox and then developed further by Xerox, Digital Equipment Corporation, and Intel. When it first began to be widely deployed in the 1980s, Ethernet supported a maximum theoretical data transfer rate of 10 megabits per second (Mbps). More recently, Fast Ethernet has extended traditional Ethernet technology to 100 Mbps peak, and Gigabit Ethernet technology extends performance up to 1,000 Mbps.

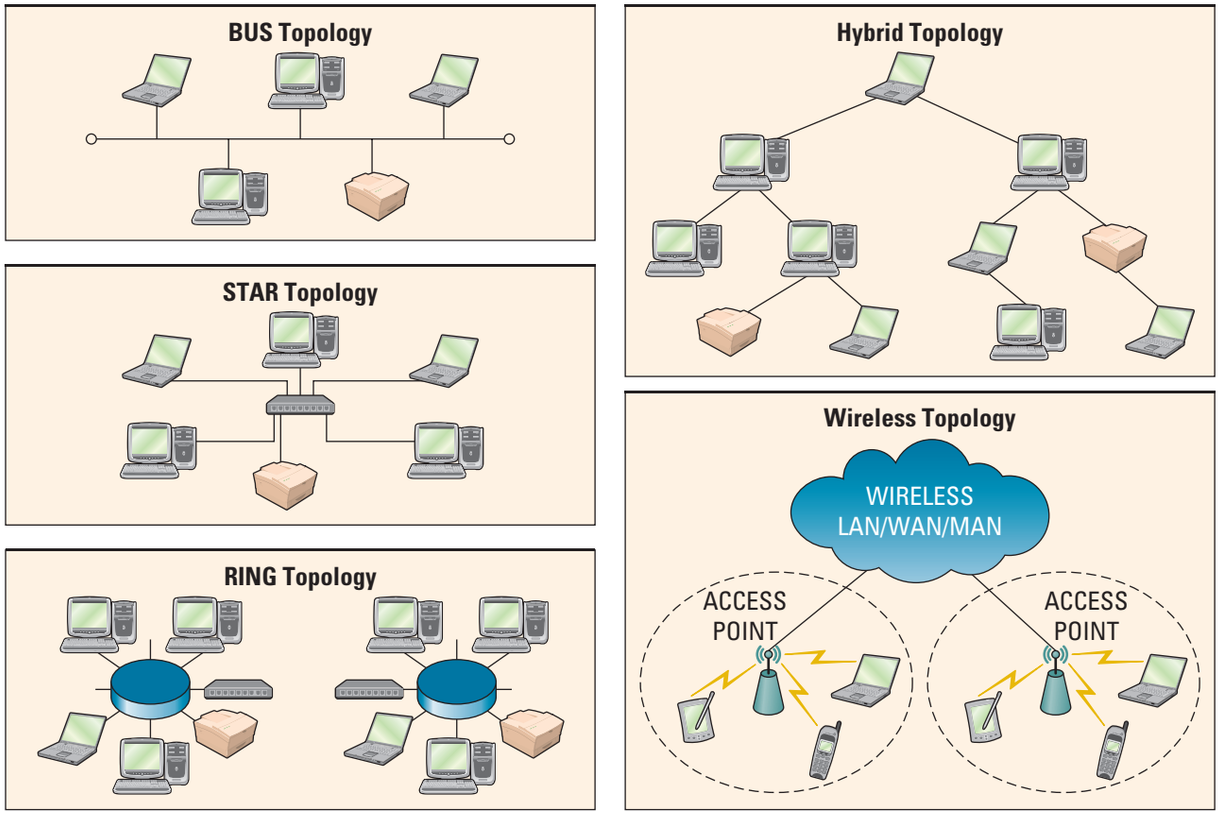
FIGURE B5.5
Five Network Topologies

Network Topologies	
Bus	All devices are connected to a central cable, called the bus or backbone. Bus networks are relatively inexpensive and easy to install for small networks.
Star	All devices are connected to a central device, called a hub. Star networks are relatively easy to install and manage, but bottlenecks can occur because all data must pass through the hub.
Ring	All devices are connected to one another in the shape of a closed loop, so that each device is connected directly to two other devices, one on either side of it. Ring topologies are relatively expensive and difficult to install, but they offer high bandwidth and can span large distances.
Hybrid	Groups of star-configured workstations are connected to a linear bus backbone cable, combining the characteristics of the bus and star topologies.
Wireless	Devices are connected by a receiver/transmitter to a special network interface card that transmits signals between a computer and a server, all within an acceptable transmission range.

Ethernet has survived as the major LAN technology—it is currently used for approximately 85 percent of the world's LAN-connected PCs and workstations—because its protocol has the following characteristics:

- Is easy to understand, implement, manage, and maintain.
- Allows low-cost network implementations.
- Provides extensive flexibility for network installation.
- Guarantees successful interconnection and operation of standards-compliant products, regardless of manufacturer.

FIGURE B5.6
Network Topologies



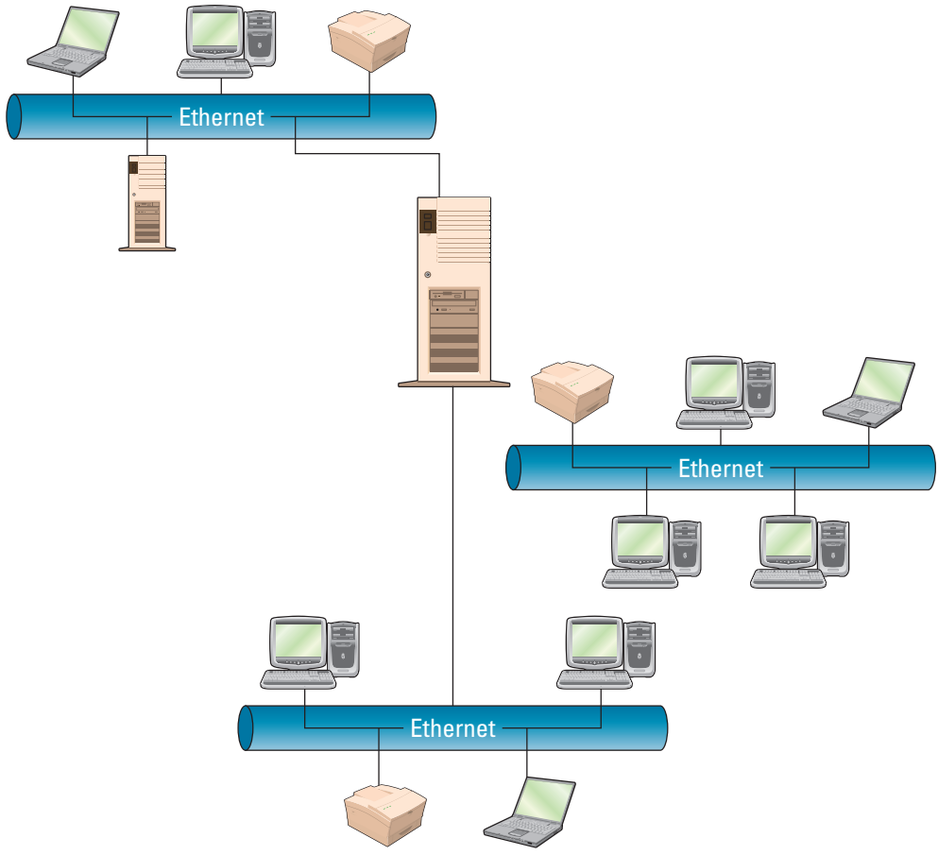


FIGURE B5.7
Ethernet Protocol

TRANSMISSION CONTROL PROTOCOL/INTERNET PROTOCOL

The most common telecommunication protocol is Transmission Control Protocol/Internet Protocol (TCP/IP), which was originally developed by the Department of Defense to connect a system of computer networks that became known as the Internet. ***Transmission Control Protocol/Internet Protocol (TCP/IP)*** provides the technical foundation for the public Internet as well as for large numbers of private networks. The key achievement of TCP/IP is its flexibility with respect to lower-level protocols. TCP/IP uses a special transmission method that maximizes data transfer and automatically adjusts to slower devices and other delays encountered on a network. Although more than 100 protocols make up the entire TCP/IP protocol suite, the two most important of these are TCP and IP. **TCP** provides transport functions, ensuring, among other things, that the amount of data received is the same as the amount transmitted. **IP** provides the addressing and routing mechanism that acts as a postmaster. Figure B5.8 displays TCP/IP's four-layer reference model:

- Application layer—serves as the window for users and application processes to access network services.
- Transport layer—handles end-to-end packet transportation.
- Internet layer—formats the data into packets, adds a header containing the packet sequence and the address of the receiving device, and specifies the services required from the network.
- Network interface layer—places data packets on the network for transmission.

FIGURE B5.8
TCP/IP Four-Layer Reference Model

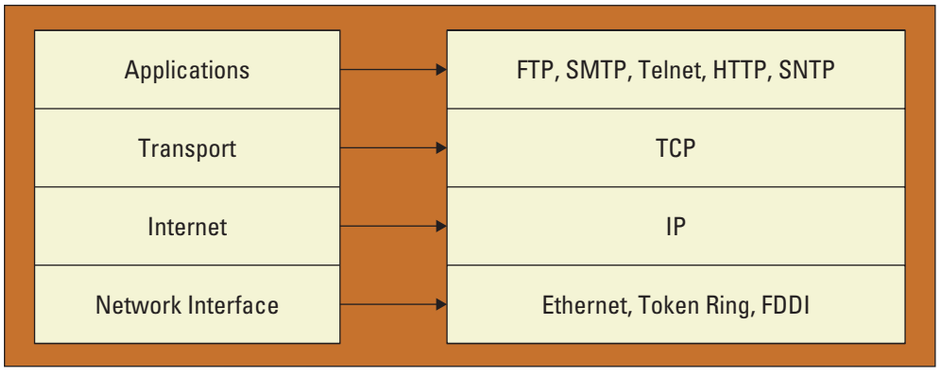


FIGURE B5.9
TCP/IP Applications

TCP/IP Applications	
File Transfer Protocol (FTP)	Allows files containing text, programs, graphics, numerical data, and so on to be downloaded off or uploaded onto a network.
Simple Mail Transfer Protocol (SMTP)	TCP/IP's own messaging system for email.
Telnet Protocol	Provides terminal emulation that allows a personal computer or workstation to act as a terminal, or access device, for a server.
Hypertext Transfer Protocol (HTTP)	Allows web browsers and servers to send and receive web pages.
Simple Network Management Protocol (SNMP)	Allows the management of networked nodes to be managed from a single point.

The TCP/IP suite of applications includes five protocols—file transfer, simple mail transfer, telnet, hypertext transfer, and simple network management (see Figure B5.9).

Another communication reference model is the seven-layer Open System Interconnection (OSI) reference model. Figure B5.10 shows the OSI model's seven layers.

The lower layers (1 to 3) represent local communications, while the upper layers (4 to 7) represent end-to-end communications. Each layer contributes protocol functions that are necessary to establish and maintain the error-free exchange of information between network users.

For many years, users thought the OSI model would replace TCP/IP as the preferred technique for connecting multivendor networks. But the slow pace of OSI standards as well as the expense of implementing complex OSI software and having products certified for OSI interoperability will preclude this from happening.

FIGURE B5.10
Open System Interconnection Model

OSI Model
7. Application
6. Presentation
5. Session
4. Transport
3. Network
2. Data Link
1. Physical

Media

Network transmission media refers to the various types of media used to carry the signal between computers. When information is sent across the network, it is converted into electrical signals. These signals are generated as electromagnetic waves (analog signaling) or as a sequence of voltage pulses (digital signaling). To be sent from one location to another, a signal must travel along a physical path. The physical path that is used to carry a signal between a signal transmitter and a signal receiver is called the transmission media. The two types of transmission media are wire (guided) and wireless (unguided).

WIRE MEDIA

Wire media are transmission material manufactured so that signals will be confined to a narrow path and will behave predictably. The three most commonly used types of guided media are (see Figure B5.11):

- Twisted-pair wiring
- Coaxial cable
- Fiber-optic cable

Twisted-Pair Wiring

Twisted-pair wiring refers to a type of cable composed of four (or more) copper wires twisted around each other within a plastic sheath. The wires are twisted to reduce outside electrical interference. Twisted-pair cables come in shielded and unshielded varieties. Shielded cables have a metal shield encasing the wires that acts as a ground for electromagnetic interference. Unshielded twisted-pair (UTP) is the most popular and is generally the best option for LAN networks. The quality of UTP may vary from telephone-grade wire to high-speed cable. The cable has four pairs of wires inside the jacket. Each pair is twisted with a different number of twists per inch to help eliminate interference from adjacent pairs and other electrical devices. The RJ-45 connectors on twisted-pair cables resemble large telephone connectors.

Coaxial Cable

Coaxial cable is cable that can carry a wide range of frequencies with low signal loss. It consists of a metallic shield with a single wire placed along the center of a shield and isolated from the shield by an insulator. This type of cable is referred to as coaxial because it contains one copper wire (or physical data channel) that carries the signal and is surrounded by another concentric physical channel consisting of a wire mesh. The outer channel serves as a ground for electrical interference. Because of this grounding feature, several coaxial cables can be placed within a single conduit or sheath without significant loss of data integrity.

Fiber-Optic Cable

Fiber optic (or ***optical fiber***) refers to the technology associated with the transmission of information as light impulses along a glass wire or fiber. The 10Base-FL and 100Base-FX optical fiber cable are the same types of cable used by most telephone companies for long-distance service. Optical fiber cable can transmit data over long distances with little loss in data integrity. In addition, because data are transferred as a pulse of light, optical fiber is not subject to interference. The light pulses travel through a glass wire or fiber encased in an insulating sheath.

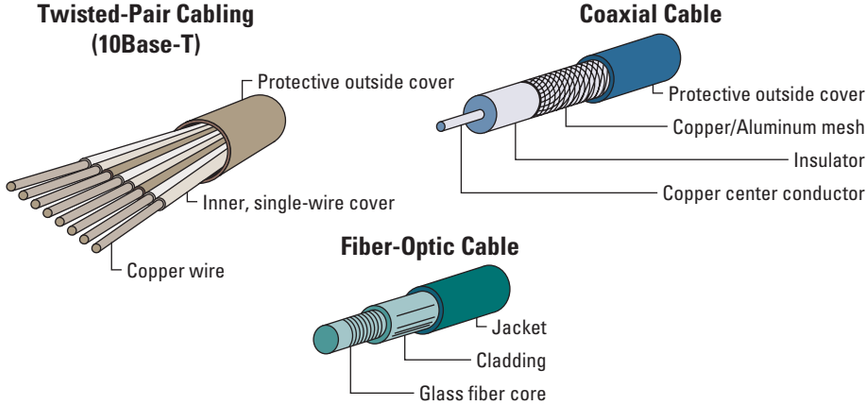


FIGURE B5.11
Twisted-Pair, Coaxial Cable, and Fiber-Optic

Optical fiber's increased maximum effective distance comes at a price. Optical fiber is more fragile than wire, difficult to split, and labor intensive to install. For these reasons, optical fiber is used primarily to transmit data over extended distances where the hardware required to relay the data signal on less expensive media would exceed the cost of optical fiber installation. It is also used where large amounts of data need to be transmitted on a regular basis.

WIRELESS MEDIA

Wireless media are natural parts of the Earth's environment that can be used as physical paths to carry electrical signals. The atmosphere and outer space are examples of wireless media that are commonly used to carry signals. These media can carry such electromagnetic signals as microwave, infrared light waves, and radio waves.

Network signals are transmitted through all media as a type of waveform. When transmitted through wire and cable, the signal is an electrical waveform. When transmitted through fiber-optic cable, the signal is a light wave, either visible or infrared light. When transmitted through the Earth's atmosphere, the signal can take the form of waves in the radio spectrum, including microwaves, infrared, or visible light.

Recent advances in radio hardware technology have produced significant advancements in wireless networking devices: the cellular telephone, wireless modems, and wireless LANs. These devices use technology that in some cases has been around for decades but until recently was too impractical or expensive for widespread use.

Using Networks and Telecommunications for Business Advantages

After gaining an understanding of networking and telecommunication fundamentals, it is easy to apply these to competitive advantages for any business including:

- Voice over IP.
- Networking businesses.
- Increasing the speed of business.
- Securing business networks.

VOICE OVER IP

Originally, phone calls made over the Internet had a reputation of offering poor call quality, lame user interfaces, and low call-completion rates. With new and improved technology and IT infrastructures, Internet phone calls now offer similar quality to traditional landline and cellular telephone calls. Today, many consumers are making phone calls over the Internet by using voice over Internet protocol (VoIP). ***Voice over IP (VoIP)*** uses TCP/IP technology to transmit voice calls over long-distance telephone lines. VoIP transmits over 10 percent of all phone calls in the United States and this number is growing exponentially.

The telecom industry is experiencing great benefits from combining VoIP with emerging standards that allow for easier development, interoperability among systems, and application integration. This is a big change for an industry that had relied on proprietary systems to keep customers paying for upgrades and new features. The VoIP and open standards combination has produced more choices, lower prices, and new applications.

Many VoIP companies, including Vonage, 8 × 8, and AT&T (CallVantage), typically offer calling within the United States for a fixed fee and a low per-minute

charge for international calls. Broadband Internet access (broadband is described in detail later in this chapter) is required, and regular house phones plug in to an analog telephone adapter provided by the company or purchased from a third party (such as DLink or Linksys) as displayed in Figure B5.12.

Since VoIP uses existing network and Internet infrastructure to route telephone calls more efficiently and inexpensively than traditional telephone service, VoIP offers businesses significant cost savings, productivity gains, and service enhancements.

Unfortunately, VoIP routes calls through the same paths used by network and Internet traffic; therefore it has the same vulnerabilities and is subject to the same Internet threats. Much like data, VoIP traffic can be intercepted, captured, or modified. Any threat that slows or degrades service even slightly will disrupt business. As a result, VoIP traffic must be secured.

Skype has long been one of the most popular VoIP options for consumers—largely because of its low cost (free for calls between Skype users and only a few dollars per month to call landlines). Now, it is gaining popularity in the business world as well.

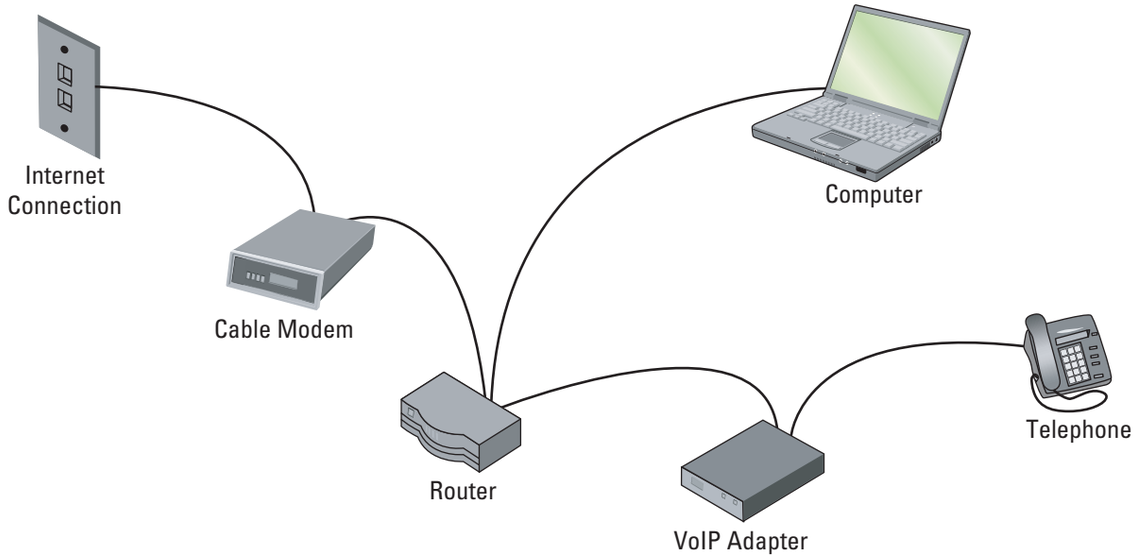
The company has been adding features that make it more business-friendly. Two examples are the Windows Installer/MSI package that makes it easy to roll out the application to multiple machines and the Skype for Business Control Panel that allows administrators to manage all of a company's Skype accounts from a centralized interface. The small-business market is especially amenable to Skype's budget-friendly and feature-rich service.

Rip Curl is one of the greatest surf and snow brands in the world. With more than 1,200 staff members and a retail presence in more than 60 countries, the company faces communications challenges in keeping abreast of global industry trends, sharing global marketing plans, coordinating events, and collaborating on design initiatives across many regions.

Rip Curl's finance and marketing divisions have been using Skype's free instant messaging and video calls for more than two years to track communications with international colleagues. Recently, Rip Curl's head of IT directed all staff to use Skype as their preferred method of communication.

Skype already includes many features that make it attractive to business users, including call forwarding and the ability to filter and block unwanted calls. In addition, Skype's conference calling feature lets users have conversations with multiple

FIGURE B5.12
Diagram of VoIP Connection



people (up to 10 participants), mixing participants who are using Skype, regular landline phones, and mobile phones.

Skype allows users to do more than just place voice calls. For instance, users with computers equipped with web cams can make video calls to get "face time" with coworkers or clients—without the hassle or expense of traveling. In addition to features built into the Skype software, many useful add-in programs are available to download that add functionality and enhance productivity (see Figure B5.13).

Skype also uses a file transfer feature that makes it easier to collaborate with colleagues over the phone; users can send copies of reports, pictures, or other files they need to share—with no limits on file size. This feature can be disabled if an administrator does not want users to be able to transfer files due to security or privacy issues.

Some features available using VoIP solutions include:

- Business application integration (for instance, tying IP telephony to a customer database).
- Calendar integration.
- Call waiting.
- Caller ID.
- Click-of-a-mouse simplicity—employees make or transfer calls right on their computer.

FIGURE B5.13
Skype Add-In Programs

Add-in	Function
Skype Office Toolbar	This add-on makes calls to names or phone numbers in a Word document, Excel spreadsheet, or PowerPoint presentation. After installing the add-in, users can use it to turn phone numbers in the document into links, which can be clicked to make a voice call or send an SMS message. Users can send the file they are working on in the Office application to a Skype contact.
Skylook	This add-on is an extension to Outlook that records calls and voice-mail to MP3 files and accesses them from Outlook. Users can call Outlook contacts over Skype and have emails read over the phone.
HotRecorder for VoIP	This add-on records Skype calls automatically using a third-party program, such as HotRecorder for VoIP (HR4VoIP). It works with Skype 3.0, as well as other VoIP applications such as Net2Phone, Google Talk, and Yahoo Messenger.
Universal Chat Translator	Today's business world is increasingly international in nature. If a user needs to communicate with people who speak another language, install the Universal Chat Translator to translate Skype chat conversations and read them. The add-on translator supports Arabic, Chinese (simplified and traditional), Dutch, French, German, Greek, Japanese, Italian, Korean, Portuguese, Russian, and Spanish. It translates the messages sent to the other language and translates the received messages to English. The translation takes place in real time for active chats or conversations can be stored in a chat history.
uSeeToo	This add-on shares photos, drawings, maps, and other graphical images. Users can add text captions and other content. It includes a drawing board, and it allows users to create, show, and save multiple boards.
PresenterNet	This add-in conducts interactive web meetings, sales presentations, "webinars," and more, using PowerPoint and Skype teleconferencing. It works with Windows, Windows Mobile, Linux, and Macintosh, and with Internet Explorer, Firefox, and Safari browsers.
Unyte	This add-in shares desktop applications with Skype contacts and others, and will share with multiple users.
TalkandWrite Extra for Skype 3.0	This add-on is a document collaboration program that allows two users to remotely work on the same document and annotate it, add text, and more, with the changes made by either party immediately made available to both.
RemoteCall	This add-in connects to remote desktops during a Skype call by clicking an icon added to the Skype Contacts and Tools menus.

- Conference call capabilities with on-screen document sharing.
- Comprehensive information about each caller.
- Desktop application (i.e., Microsoft Outlook) integration.
- Dial-by-name capability.
- Easy navigation.
- Four- or five-digit dialing to anyone, regardless of location.
- Mobility—users can work from anywhere.
- Three-way calling.

NETWORKING BUSINESSES

Retailer REI reports that one-third of all customers who buy online and pick up at the store make another purchase while there, spending an average of $90. From a technology perspective, in-store pickup needs to have some level of inventory integration to work effectively. The integration of data is critical in being able to display to the consumer the availability of products at the closest geographic store.

To set up an ebusiness even a decade ago would have required an individual organization to assume the burden of developing the entire network infrastructure. Today, industry-leading companies have developed Internet-based products and services to handle many aspects of customer and supplier interactions. "In today's retail market, you cannot be a credible national retailer without having a robust website," says Dennis Bowman, senior vice president and CIO of Circuit City, who adds that customers now expect seamless retailing between online and in-store just as they expect stores that are clean and well stocked. For this reason, retailers are working furiously to integrate their ebusiness sites with their inventory and point-of-sale (POS) systems so that they can accept in-store returns of merchandise bought online and allow customers to buy on the web and pick up in the store.

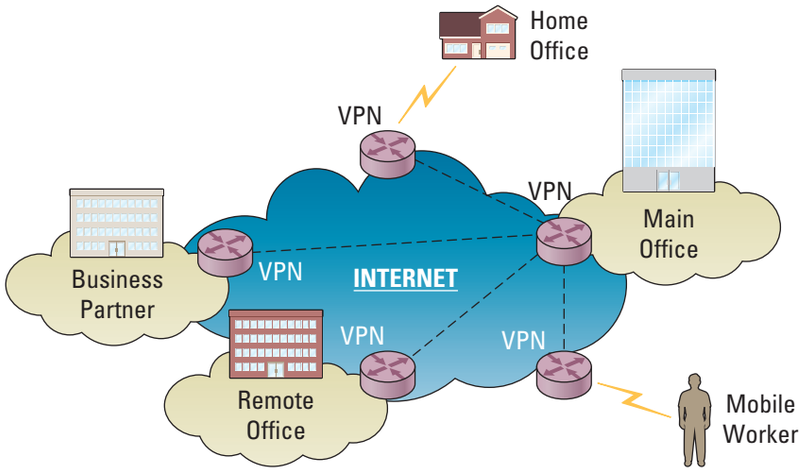
Some companies, such as Best Buy, Circuit City, Office Depot, and Sears, already have their physical and online stores integrated. These companies have been the fast movers because they already had an area in their stores for merchandise pickup (usually for big, bulky items such as TVs and appliances), and because long before the web they had systems and processes in place that facilitated the transfer of a sale from one store to another. To take on the challenge of business integration, an organization needs a secure and reliable network for mission-critical systems (see Figure B5.14).

A ***virtual private network (VPN)*** is a way to use the public telecommunication infrastructure (e.g., Internet) to provide secure access to an organization's network (see Figure B5.15). A ***valued-added network (VAN)*** is a private network, provided by a third party, for exchanging information through a high-capacity connection.

- Provide for the transparent exchange of information with suppliers, trading partners, and customers.
- Reliably and securely exchange information internally and externally via the Internet or other networks.
- Allow end-to-end integration and provide message delivery across multiple systems, in particular, databases, clients, and servers.
- Respond to high demands with scalable processing power and networking capacity.
- Serve as the integrator and transaction framework for both digital businesses and traditional brick-and-mortar businesses that want to leverage the Internet for any type of business.

FIGURE B5.14
Business Network Characteristics

FIGURE B5.15
Virtual Private Network Overview



Organizations engaging in ebusiness have relied largely on VPNs, VANs, and other dedicated links handling electronic data interchange transactions. These traditional solutions are still deployed in the market, and for many companies will likely hold a strategic role for years to come. However, these conventional technologies present significant challenges:

- By handling only limited kinds of business information, these contribute little to a reporting structure intended to provide a comprehensive view of business operations.
- They offer little support for the real-time business process integration that will be essential in the digital marketplace.
- Relatively expensive and complex to implement, conventional technologies make it difficult to expand or change networks in response to market shifts.

INCREASING THE SPEED OF BUSINESS

Transmission can occur at different speeds. By speed we do not mean how fast the signal travels in terms such as miles per hour, but rather the volume of data that can be transmitted per unit of time. Terms such as bandwidth, hertz (Hz), and baud are used to describe transmission speeds, whereas a measure such as bits transmitted per second (bits per second, or bps) would be more understandable. ***Bandwidth*** is the difference between the highest and the lowest frequencies that can be transmitted on a single medium, and it is a measure of the medium's capacity. *Hertz* is cycles per second, and *baud* is the number of signals sent per second. If each cycle sends one signal that transmits exactly one bit of data, which is often the case, then all these terms are identical.

In information technology publications, baud was formerly used for relatively slow speeds such as 2,400 baud (2,400 bits per second) or 14,400 baud (14,400 bps), while hertz (with an appropriate prefix) was used for higher speeds such as 500 megahertz (500 million bps) or 2 gigahertz (2 billion bps). More recently, the term *baud* has fallen into disfavor, but hertz is still widely used. For clarity, we will stick with bps in this chapter.

The notion of bandwidth, or capacity, is important for telecommunications. For example, approximately 50,000 bits (Os and 1s) are required to represent one page of data. To transmit this page over a 128,000 bps (128 Kbps) digital subscriber line (DSL) would take only four-tenths of a second. Graphics require approximately 1 million bits for one page. This would require about 8 seconds over a 128 Kbps DSL. Full-motion video transmission requires the enormous bandwidth

Transmission Medium	Typical Speeds
Twisted pair—voice telephone	14.4 Kbps–56 Kbps
Twisted pair—digital telephone	128 Kbps–1.544 Mbps
Twisted pair—LAN	10 Mbps–100 Mbps
Coaxial cable—LAN	10 Mbps–1 Gbps
Wireless—LAN	6 Mbps–54 Mbps
Microwave—WAN	50 Kbps–100 Mbps
Satellite—WAN	50 Kbps–100 Mbps
Fiber-optic cable—WAN	100 Mbps–100 Gbps

KEY: bps = bits per second
Kbps = thousand bits per second
Mbps = million bits per second
Gbps = billion bits per second

FIGURE B5.16
Telecommunications Transmission Speeds

of 12 million bps, and thus data compression techniques must be employed to be able to send video over the existing telephone network. The bandwidth determines what types of communication—voice, data, graphics, full-motion video—can reasonably be transmitted over a particular medium. Figure B5.16 outlines the typical transmission speeds found in business today (a few of the technologies mentioned in Figure B5.16 will be discussed in detail in the next section). Figure B5.17 gives an overview of the average time required to download specific Internet functions.

High-speed Internet, once an exotic and expensive service used only by larger companies, is now an inexpensive mainstream offering. The term ***broadband*** generally refers to high-speed Internet connections transmitting data at speeds greater than 200 kilobytes per second (Kbps), compared to the 56 Kbps maximum speed offered by traditional dial-up connections. While traditional dial-up access (using normal voice telephone line technology) suffices for some consumers, many need or want the much faster connections that technological advances now allow. The right option for Internet access will depend on a company's needs and which services are available. Figure B5.18 lists some of the advantages and disadvantages of current conventional broadband technology available.

SECURING BUSINESS NETWORKS

Networks are a tempting target for mischief and fraud. An organization has to be concerned about proper identification of users and authorization of network access, the control of access, and the protection of data integrity. A firm must identify users before they are granted access to a corporate network, and that access

Internet Function	Dial-up (56K)	Satellite (512K)	DSL (1M)	Cable (1M)	Wireless (5M)
An email	1 sec.	<1 sec.			
A basic web page (25K)	10 sec.	<1 sec.			
One five-minute song (5M)	15 min.	2 min.	1 min.		40 sec.
One two-hour movie (500M)	20 hrs.	4 hrs.	2 hrs.		70 min.

FIGURE B5.17
Internet Function Average Download Time

Technology	Typical Download Speed (Mbps)	Typical Uplink Speed (Mbps)	Advantages	Disadvantages
Digital subscriber line (DSL)	.5–3	1.0	– Good upload rates – Uses existing telephone lines	– Speeds vary depending on distance from telephone company's central office – Slower downloads than less expensive alternatives
Cable	.5–4	.5–1	– Uses existing cable infrastructure – Low-cost equipment	– Shared connections can overload system, slowing upload times
TI/T3 dedicated line	1.5–3	1.5–3	– Uses existing phone wiring	– Performance drops significantly with range – Susceptible to cross talk
Fiber-to-the-home	4.5	10.2	– Fast data speeds – Infrastructure has long life expectancy – Low maintenance – Low power costs	– Not widely available – Significant deployment cost (for company)
Fixed wireless	.5–12	.5	– Typically inexpensive to install, no underground digging	– Weather, topography, buildings, and electronics can cause interference
Satellite	.5–2	.05	– Nearly universal coverage – Available in otherwise inaccessible areas	– Expensive service/equipment – Upload/download delays

FIGURE B5.18

Advantages and Disadvantages of Broadband Technology

should be appropriate for the given user. For example, an organization may allow outside suppliers access to its internal network to learn about production plans, but the firm must prevent them from accessing other information such as financial records. In addition, the organization should preserve the integrity of its data; users should be allowed to change and update only well-specified data. These problems are exacerbated on the Internet where individuals must be very concerned about fraud, invalid purchases, and misappropriation of credit card information.

Providing network security is a difficult challenge. Almost all networks require some kind of log-on, including user name and password. Many people are casual with their passwords, making them easy to guess. A good password has both letters and numbers along with a few punctuation marks for added security. Most corporate security goes far beyond passwords, however. One common approach is a firewall, a computer that sits between an internal network and the Internet. The firewall allows access to internal data from specified incoming sites but tries to detect unauthorized access attempts and prevent them from occurring.

For highly secure communications, a sender can encrypt data, that is, encode the data so that someone without the "key" to decode them cannot read the message. There are a number of encryption approaches, and controversy exists over how strong the encryption should be. The most secure approaches use longer keys, making it much more difficult for an intruder to compute the key. The U.S. government is concerned about terrorists and criminals who might have access to strong encryption that is beyond the capabilities of law enforcement authorities to decrypt. There are export restrictions on encryption programs.

For Internet commerce, various schemes have been proposed for sending credit card or other payments over the network in a secure manner. Some involve

encryption and others various forms of digital certificates or digital cash. Many firms worry that customers will not want to complete transactions on the Internet because of the fear their credit card numbers might be stolen. However, a law limits individual liability for credit card misuse to $50.

Data Sharing

Even more important than the sharing of technology resources is the sharing of data. Either a LAN or a WAN permits users on the network to get data (if they are authorized to do so) from other points on the network. It is very important, for example, for managers to be able to retrieve overall corporate sales forecasts from corporate databases to use in developing spreadsheets (or any other program used for business analysis) to project future activity. To satisfy customers, automobile dealers need to be able to locate particular vehicle models and colors with specific equipment installed. Managers at various points in a supply chain need to have accurate, up-to-date data on inventory levels and locations. Accountants at corporate headquarters need to be able to retrieve summary data on sales and expenses from each of the company's divisional computer centers. The chief executive officer, using an executive information system, needs to be able to access up-to-the-minute data on business trends from the corporate network.

PLUG-IN SUMMARY

Networks come in all sizes, from two computers connected to share a printer, to the Internet, which is the largest network of all, joining millions of computers of all types all over the world. In between are business networks, which vary in size from a dozen or fewer computers to many thousands. There are three primary types of networks: local area network (LAN), wide area network (WAN), and metropolitan area network (MAN). The following differentiate networks:

- Architecture—peer-to-peer, client/server.
- Topology—bus, star, ring, hybrid, wireless.
- Protocols—Ethernet, Transmission Control Protocol/Internet Protocol (TCP/IP).
- Media—coaxial, twisted-pair, fiber-optic.

Networking and telecommunications offer competitive advantages for any business including:

- Voice over IP.
- Networking businesses.
- Increasing the speed of business.
- Securing business networks.

KEY TERMS

Bandwidth, B5.14
Broadband, B5.15
Client, B5.4
Client/server network, B5.4
Coaxial cable, B5.9
Ethernet, B5.5
Fiber optic (or optical fiber), B5.9
Interoperability, B5.5
Local area network (LAN), B5.3
Metropolitan area network (MAN), B5.3
Network, B5.2
Network operating system (NOS), B5.4
Network topology, B5.5
Network transmission media, B5.8
Packet-switching, B5.4
Peer-to-peer (P2P) network, B5.4
Protocol, B5.5
Router, B5.4
Server, B5.4
Telecommunication system, B5.2
Transmission Control Protocol/Internet Protocol (TCP/IP), B5.7
Twisted-pair wiring, B5.9
Valued-added network (VAN), B5.13
Virtual private network (VPN), B5.13
Voice over Internet Protocol (VoIP), B5.10
Wide area network (WAN), B5.3
Wire media, B5.9
Wireless media, B5.10

CLOSING CASE ONE

Watching Where You Step—Prada

Prada estimates its sales per year at $22 million. The luxury retailer recently spent millions on IT for its futuristic "epicenter" store—but the flashy technology turned into a high-priced hassle. The company needed to generate annual sales of $75 million by 2007 to turn a profit on its new high-tech investment.

When Prada opened its $40 million Manhattan flagship, hotshot architect Rem Koolhaas promised a radically new shopping experience. And he kept the promise—though not quite

according to plan. Customers were soon enduring hordes of tourists, neglected technology, and the occasional thrill of getting stuck in experimental dressing rooms. A few of the problems associated with the store:

1. **Fickle fitting rooms**—Doors that turn from clear to opaque confuse shoppers and frequently fail to open on cue.
2. **Failed RFID**—Touch screens meant to spring to life when items are placed in the RFID "closets" are often just blank.
3. **Pointless PDAs**—Salesclerks let the handheld devices gather dust and instead check the stockroom for inventory.
4. **Neglected network**—A lag between sales and inventory systems makes the wireless network nearly irrelevant.

This was not exactly the vision for the high-end boutique when it debuted in December 2001. Instead, the 22,000-square-foot SoHo shop was to be the first of four "epicenter" stores around the world that would combine cutting-edge architecture and 21st century technology to revolutionize the luxury shopping experience. Prada poured roughly 25 percent of the store's budget into IT, including a wireless network to link every item to an Oracle inventory database in real-time using radio frequency identification (RFID) tags on the clothes. The staff would roam the floor armed with PDAs to check whether items were in stock, and customers could do the same through touch screens in the dressing rooms.

But most of the flashy technology today sits idle, abandoned by employees who never quite embraced computing chic and are now too overwhelmed by large crowds to assist shoppers with handhelds. On top of that, many gadgets, such as automated dressing-room doors and touch screens, are either malfunctioning or ignored. Packed with experimental technology, the clear-glass dressing-room doors were designed to open and close automatically at the tap of a foot pedal, then turn opaque when a second pedal sent an electric current through the glass. Inside, an RFID-aware rack would recognize a customer's selections and display them on a touch screen linked to the inventory system.

In practice, the process was hardly that smooth. Many shoppers never quite understood the pedals and disrobed in full view, thinking the door had turned opaque. That is no longer a problem, since staff members usually leave the glass opaque, but often the doors get stuck. Some of the chambers are open only to VIP customers during peak traffic times.

With the smart closets and handhelds out of commission, the wireless network in the store is nearly irrelevant, despite its considerable expense. As Prada's debt reportedly climbed to around $1 billion in late 2001, the company shelved plans for the fourth epicenter store, in San Francisco. A second store opened in Tokyo to great acclaim, albeit with different architects in a different market. Though that store incorporates similar cutting-edge concepts, architect Jacques Herzog emphasized that avant-garde retail plays well only in Japan. "This building is clearly a building for Tokyo," he told *The New York Times.* "It couldn't be somewhere else."

The multimillion-dollar technology is starting to look more like technology for technology's sake than an enhancement of the shopping experience, and the store's failings have prompted Prada to reevaluate its epicenter strategy.

Questions

1. Explain how Prada was anticipating using its wireless network to help its stores operate more efficiently. What prevented the system from working correctly?
2. What could Prada have done to help its employees embrace the wireless network?
3. Would Prada have experienced the same issues if it had used a wire (guided) network instead of a wireless (unguided) network?
4. What security issues would Prada need to be aware of concerning its wireless network?
5. What should Prada do differently when designing its fourth store to ensure its success?

CLOSING CASE TWO

Banks Banking on Network Security

Bank of America, Commerce Bancorp, PNC Financial Services Group, and Wachovia were victims of a crime involving a person trying to obtain customer data and sell it to law firms and debt-collection agencies. New Jersey police seized 13 computers from the alleged mastermind with 670,000 account numbers and balances. There is no indication the data were used for identity theft, but it highlights how increasingly difficult it is to protect information against such schemes as the market value of personal information grows. In the past, banks were wary of the cost or customer backlash from adopting network security technologies. Today, banks are beefing up network security as more customers begin to view security as a key factor when choosing a bank.

Bank of America

Bank of America is moving toward a stronger authentication process for its 13 million online customers. Bank of America's new SiteKey service is designed to thwart scams in which customers think they are entering data on the bank's website, when they are actually on a thief's site built to steal data. This occurs when a worm tells a computer to reroute the bank's URL into a browser to another site that looks exactly like the bank's.

SiteKey offers two-factor authentication. When enrolling in SiteKey, a customer picks an image from a library and writes a brief phrase. Each time the customer signs on, the image and phrase are displayed, indicating that the bank recognizes the computer the customer is using and letting the customer know that he or she is at the bank's official website. The customer then enters a password and proceeds. When signing on from a different computer than usual, the customer must answer one of three prearranged questions.

Wells Fargo & Company

"Out-of-wallet" questions contain information that is not found on a driver's license or ATM card. Wells Fargo is implementing a security strategy that operates based on "out-of-wallet" questions as a second factor for network password enrollment and maintenance. It is also offering network security hardware such as key fobs that change passwords every 60 seconds. Last fall, it launched a two-factor authentication pilot in which small businesses making electronic funds transfers need a key fob to complete transactions.

E*Trade Financial Corporation

E*Trade Financial Corporation provides customers holding account balances of more than $50,000 with a free Digital Security ID for network authentication. The device displays a new six-digit code every 60 seconds, which the customer must use to log on. Accounts under $50,000 can purchase the Digital Security ID device for $25.

Barclays Bank

Barclays Bank instituted online-transfer delays of between several hours and one day. The delays, which apply the first time a transfer is attempted between two accounts, are intended to give the bank time to detect suspicious activity, such as a large number of transfers from multiple accounts into a single account. The online-transfer delay was adopted in response to a wave of phishing incidents in which thieves transferred funds from victims' bank accounts into accounts owned by "mules." Mules are people who open bank accounts based on email solicitations, usually under the guise of a business proposal. From the mule accounts, the thieves withdraw cash, open credit cards, or otherwise loot the account.

Barclays also offers account monitoring of customers' actions to compare them with historical profile data to detect unusual behavior. For instance, the service would alert the bank to contact the customer if the customer normally logs on from England and suddenly logs on from New York and performs 20 transactions.

Questions

1. What reason would a bank have for not wanting to adopt an online-transfer delay policy?
2. Why is network security critical to financial institutions?
3. Explain the differences between the types of network security offered by the banks in the case. Which bank would you open an account with and why?
4. What additional types of network security, not mentioned in the case, would you recommend a bank implement?
5. Identity three policies a bank should implement to help it improve network information security.

MAKING BUSINESS DECISIONS

1. Secure Access

Organizations that have traditionally maintained private, closed systems have begun to look at the potential of the Internet as a ready-made network resource. The Internet is inexpensive and globally pervasive: Every phone jack is a potential connection. However, the Internet lacks security. What obstacles must organizations overcome to allow secure network connections?

2. Rolling Out with Networks

As organizations begin to realize the benefits of adding a wireless component to their network, they must understand how to leverage this emerging technology. Wireless solutions have come to the forefront for many organizations with the rollout of more standard, cost-effective, and secure wireless protocols. With wireless networks, increased business agility may be realized by continuous data access and synchronization. However, with the increased flexibility comes many challenges. Develop a report detailing the benefits an organization could obtain by implementing wireless technology. Also, include the challenges that a wireless network presents along with recommendations for any solutions.

3. Wireless Fitness

Sandifer's Fitness Club is located in beautiful South Carolina. Rosie Sandifer has owned and operated the club for 20 years. The club has three outdoor pools, two indoor pools, 10 racquetball courts, 10 tennis courts, an indoor and outdoor track, along with a four-story exercise equipment and massage therapy building. Rosie has hired you as a summer intern specializing in information technology. The extent of Rosie's current technology includes a few PCs in the accounting department and two PCs with Internet access for the rest of the staff. Your first assignment is to create a report detailing networks and wireless technologies. The report should explain how the club could gain a business advantage by implementing a wireless network. If Rosie likes your report, she will hire you as the full-time employee in charge of information technology. Be sure to include all of the different uses for wireless devices the club could implement to improve its operations.