

Local Area Networks

Wayne C. Summers, *Columbus State University*

Introduction to Local Area Networks	1	Site Design	14
Why Do We Want to Network Computers?	1	Server Configuration	15
Types of LANs	2	Installation Schedule	15
Difference Between LANs and WANs	3	Installation	15
LAN Topology	3	LAN Administration	16
LAN Architecture	4	Configuration List	16
LAN Hardware and Media	6	System Log	16
Copper Wire	6	Training	16
Fiber Wire	7	Backup	16
Wireless	7	Security	16
Hardware Devices	8	LAN Security	16
Virtual LAN	10	Physical Security	17
LAN Software	10	Access Security	17
Role and Applications of LANs	11	Data Security	17
Wireless Local Area Networks (WLANs)	11	Network Security	17
WLAN Standards	11	Malware	18
WLAN Management	12	Policy, Procedures, and Awareness	18
WLAN Security	12	Conclusion	19
LAN Installation	13	Glossary	19
Needs Analysis	13	Cross References	19
Site Analysis	13	References and Suggested Readings	19
Equipment Selection	13		

INTRODUCTION TO LOCAL AREA NETWORKS

A network is a collection of two or more devices linked together. Typically, the connection is a physical connection using wires or cables, although wireless connections are also widely available. In addition to the hardware required for this connection, there is specialized software necessary to allow the communications to occur. Networking facilitates the sharing of resources, including hardware, software, and data as well as providing a mechanism for enhancing communications between computers and users of computers.

Networks have traditionally been classified as local area networks (LANs) and wide area networks (WANs). The size or radius of the network has been typically used to distinguish between these types of networks. A LAN is a network where the computers are physically close together. This may mean that the computers are in the same room, the same building, or even at the same site. Computers in a WAN are often distributed beyond metropolitan areas. WANs are usually made up of multiple LANs as in the case of the Internet. Other classifications of networks include personal area networks (PANs), campus area networks (CANs), metropolitan area networks (MANs), and storage area networks (SANs). Networks are also classified by the network protocols at the physical/data-link layers of the network. Often the distinction between LANs and WANs depends on who controls the network. The Internet service provider (ISP) typically controls WANs, while LANs are more often controlled by the local network administrator.

Why do we Want to Network Computers?

In the early days of computing, there were a small number of isolated computers, each used by only one person or one process at a time. With the emergence of time-sharing, by linking terminals to mainframe computers in the 1960s multiple users were able to use individual computers simultaneously. This significantly expanded the functionality of computers, but had several limitations. Chief among the limitations was that as more users connect to the shared computer, the amount of resources available to each user's transaction diminishes. In the late 1970s and early 1980s, the personal computer (PC) resulted in the return of one computer—one user (Figure 1.1). In the 1990s, hardware and software became available to network multiple PCs (Figure 1.2). Before LANs, every user of the data kept copies of data on each computer, and copies of software or application programs used by each user had to be installed on each computer. Printing a document required that every computer needed its own printer or the user walked to the computer with the attached printer and loaded the document on that computer. Networking computers alleviates some of this need for redundancy, although there will still be some redundancy needed for backup purposes.

Data in a networked environment can be shared. Users can access data from multiple computers via the network. This feature helped speed the transition from mainframe computing to networked computing. Using networked computers, different computer users were able to share important information. Rather than keeping copies of data on each computer, one copy of the data is kept on

a centralized system, called the server, and is accessed remotely via the network. Changes to the data are made once, and then accessed by all.

Rather than installing software on every computer, software can also be shared in a network environment. Application programs can be stored on one computer and run remotely from another computer. In an office configured with multiple non-networked computers, each computer must have an installed copy of each application program. In addition to the need to purchase copies of the software for each computer, the software must be installed and maintained on each computer. Network versions of many application programs can be purchased and installed once on a networked server. A network version of software is typically cheaper than purchasing large numbers of a particular piece of software. Network software only needs to be installed once on a server allowing users on the other computers to access the software. When it is time to upgrade the software, it only needs to be done once on the server, instead of on all of the computers. Installing software on multiple computers simultaneously can be facilitated using networked computers with the software residing on the server.

Networks facilitate the sharing of hardware. Hardware can be installed in one location and accessed over the network from other computers. Printers and scanners can be networked so that multiple users can share the same printer or other hardware device. Other peripheral devices might include CD-ROMs, DVD-ROMs, and other shared devices.

Before LANs, computer users that needed to communicate with others had to use traditional methods such as a physical visit to another user, a telephone call, or a letter

delivered to the other person. Communications using e-mail, instant messaging (IM), and other mechanisms like weblogs (blogs) has been enhanced tremendously by the use of LANs.

TYPES OF LANS

Computers that can access a network are considered to be networked workstations or hosts. Any device (workstation, printer, modem) that connects to a network is called a node. Many of the networks in the early 1980s only allowed the sharing of resources directly between PCs. These types of networks are peer-to-peer networks where each computer has the same potential for sharing files and hardware devices. A peer-to-peer network is easy to design and maintain, but is limited in its capabilities.

Most networks today are classified as client/server networks. In a client/server network, one or more of the computers will function as a server, whereas the remainder of the computers functions as clients. A server is a computer that provides a service, whereas a client computer makes use of the service provided. Examples of servers include print servers, file servers, mail servers, and Web servers. A print server (Figure 1.3) is a computer or peripheral device that provides access to one or more printers across the network. Print servers were among the earliest type of servers. A file server provides a repository for files that are accessed by other computers over the network. Mail or communication servers manage the flow of incoming and outgoing electronic mail for users accessing the server from client workstations. Web servers are computers running specialized software that provides access to World Wide Web documents.



Figure 1.1: Before Networks

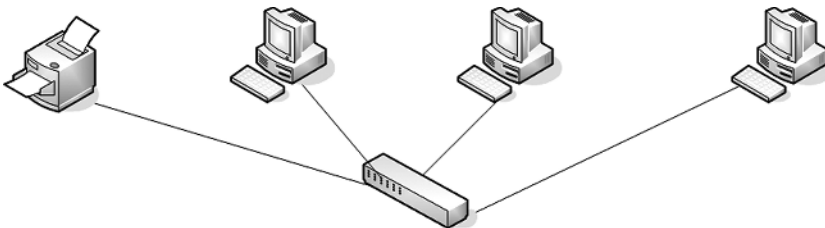


Figure 1.2: Networked Computers

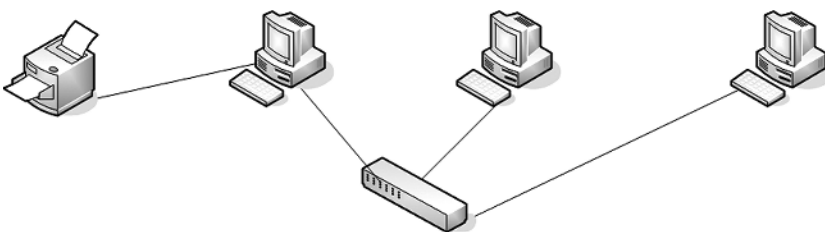


Figure 1.3: Print Server

Network servers can run more than one type of server software and function as multiple types of servers. For example, a computer can have both Web server and e-mail server software installed and function as both a Web server and a communications server. A workstation can function both as a server and simultaneously as a client for another server. For example, a computer can be a Web server running Web server software, but print through the network using another computer that functions as a print server. It is generally not recommended that one computer function as more than one server. Doing so increases the likelihood of one point of attack on the network. However, using a separate computer for each server results in more potentially vulnerable computers and increased administration costs. This increases the points of attack and needs to be taken into consideration. Running only one main service (e.g., e-mail) can significantly increase the reliability of the network, because instability and maintenance associated with that service will typically not affect other services running on separate servers.

Similarly, it is recommended that servers not function as clients. Using a server as a client increases the opportunity for introducing vulnerabilities that might compromise the security of the server.

One solution that allows multiple servers on one physical computer is virtualization. Each server resides in its own virtual space on the computer. This requires the use of special software like VMWare, Parallels, or Microsoft Virtual Server. Virtualization lowers the total cost of investment and can provide additional security. One drawback to virtualization is the additional workload to install and maintain the systems.

Difference between LANs and WANs

As mentioned earlier, one distinction between LANs and WANs is the radius of the network. A LAN is a network where the nodes are physically close together. Typically, the nodes are in the same room, but they can be in the same building or in nearby buildings. In today's networks, the nodes are often scattered across the organization. Historically, networks with a radius greater than a kilometer or two have been typically classified as WANs. Other ways of distinguishing between LANs and WANs include transmission speed and ownership. LANs are typically faster networks with speeds of at least 100 Mbps to 10 Gbps. WANs are generally significantly slower, with most WANs operating at speeds around 1.54 Mbps (T1/DS1) or 45 Mbps (T3/DS3). Today very high-speed WANs exist that approach LAN speeds. LANs are owned by the organization where the network is used. WANs generally use hardware that is owned and operated by a network provider, although there are public agencies that do own and operate their own WANs. A final distinction is with the difference in technologies used by LANs and WANs. The next section describes two of the technologies (Ethernet and token ring) used by LANs. WANs typically use different technologies, including Frame Relay, ATM, and X.25. Recently Ethernet has started to be deployed in WANs as MANs. These distinctions will continue to blur significantly as WANs get faster and LANs get larger.

LAN Topology

LANs can be organized in a variety of ways. One way to classify networks is by their electrical configuration or logical topology. This is often called the signal topology and is determined by how the nodes communicate with each other. This is the way that the data is transmitted between nodes. The two main logical topologies are bus and ring.

In a traditional bus network, the data is broadcast from one node to all other nodes in the LAN even though the data may be intended for only one node. Each of the nodes receives the data, but it is only "read" by the node where the data is intended. The data includes an address for the destination node or nodes. Ethernet is the primary technology that supports the logical bus topology.

In a ring network, the data is sent from one node to the next in sequential order in a circular fashion. Each node inspects the destination address of the data packet to determine if the data is meant for it. If the data is not meant for the node, the data packet is passed along to the next node in the logical ring.

LANs can also be classified by the physical layout of the network. The way that the nodes are physically connected to the network is known as the physical topology. The physical topology of the network can have a significant influence on a LAN's performance and reliability. The three main physical topologies are bus, ring, and star. There are also hybrid networks including star-bus and star-ring, which incorporate parts of both types of networks. These "mixed" topologies are implementations that are more common.

In a bus topology (Figure 1.4), the nodes are arranged in a linear fashion, with terminators (Figure 1.5) on each end of the network. The nodes are connected to the "bus" with connectors. Bus networks are easy to install but not very reliable. Any break in the connection, or a loose connection, will bring down a portion of the network and possibly the entire network. This is old technology rarely used in modern LANs.

In a ring topology (Figure 1.6), each connected node is an active participant in the ring network. Each data packet is received by a node, and if it is not intended for the node, it is passed along the ring to the next node. If one of the nodes or its network card malfunctions, the network subsequently stops functioning.

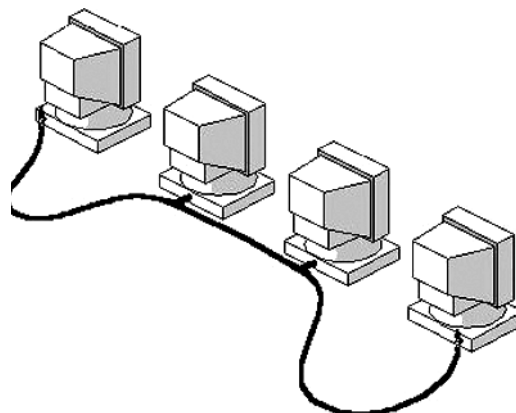


Figure 1.4: Bus Network

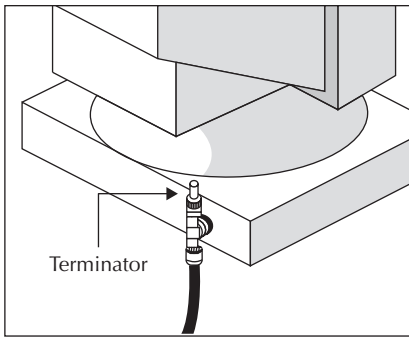


Figure 1.5: Terminator and BNC T-Connector

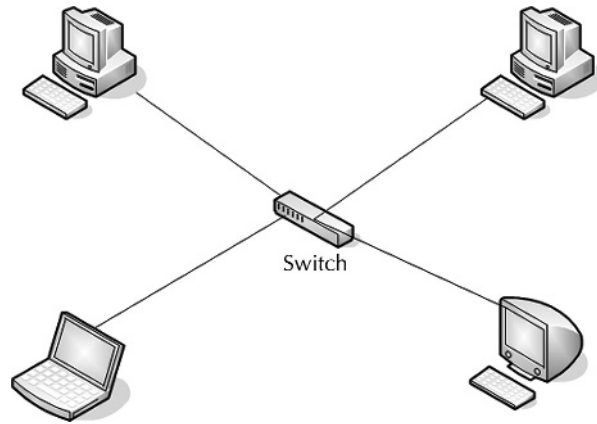


Figure 1.7: Star Physical Network

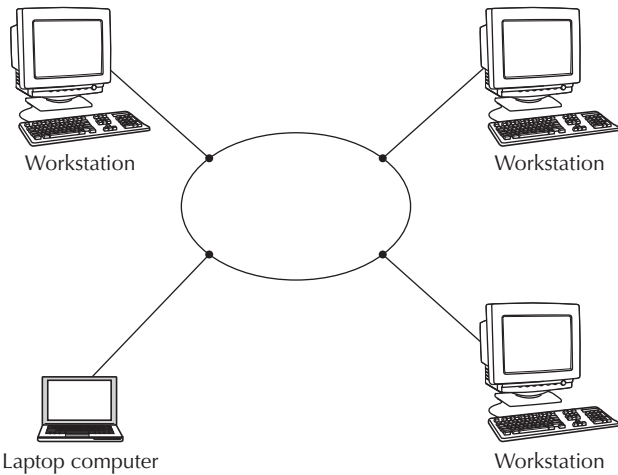


Figure 1.6: Ring Network

In a star network (Figure 1.7), each connected node is attached to a central device. Typically, this device is a hub or a switch, but it could also be other devices, including a multistation access unit (MAU). Star networks are more reliable and easier to troubleshoot. Star networks do require an additional hardware device like a hub or switch, and additional cable. Because each node is independently connected to the central device, a failure only affects the single node. Of course, if the central device fails, the entire network fails.

A network's physical and logical topologies are not necessarily the same. For example, a twisted-pair Ethernet network using a hub is physically arranged in a star topology, although the data is transmitted via a logical bus topology.

LAN Architecture

The most dominant network architecture for LANs today is Ethernet. Ethernet was developed by Robert Metcalfe

and others at the Palo Alto Research Center (PARC) in the mid-1970s (Metcalfe 1976).

Ethernet uses the carrier sense multiple access with collision detection (CSMA/CD) access method. Carrier sense refers to each node being able to "listen" for other users using the network, only attempting to use the network if it is not being used. Multiple access means that any node on the network may use the network without requiring further permission. Collision detection lets the node know if a message was not delivered and controls the mechanism for retransmitting the data packet. CSMA/CD is most efficient when there are a limited number of nodes requesting access to the network. As the radius of the network and number of nodes on the network increases, the likelihood of collisions increases. Collisions are a normal part of a CSMA/CD network. Collisions are only considered a problem if more than 5 percent of the data on the network is involved in a collision.

In 1981, the first Ethernet standard was developed by a consortium comprised of Digital, Intel, and Xerox. This was followed by a second Ethernet standard in 1982, called Ethernet II. Ethernet II (Figure 1.8) had the following characteristics:

- Bus topology
- Coaxial cable using baseband signaling
- 10 Mbit/sec data rate
- Maximum station separation of 2.8 kilometers
- 1024 maximum number of stations

In addition, the Institute of Electrical and Electronics Engineers (IEEE) developed a standard, also often referred to as Ethernet, called the IEEE 802.3 standard (Figure 1.9). The two standards are very similar and have similar frame layouts as shown. Although Ethernet has continued to evolve over the past 25 years, the main concepts have remained.

Preamble	Destination MAC Address	Source MAC Address	Type	Data Unit and Padding	Frame Check Sequence
8 octets	6 octets	6 octets	2 octets	46-1500 bytes	4 octets

Figure 1.8: Ethernet II Frame Layout

Preamble	SFD	Destination MAC Address	Source MAC Address	Length	Logical Link Control IEEE 802.2 Data and Pad	Frame Check Sequence
7 octets	1 octet	6 octets	6 octets	2 octets	46- 1500 bytes	4 octets

Figure 1.9: IEEE 802.3 Frame Layout

Table 1.1: Types of Network Media

Standard	Popular Name	Speed	Media	Maximum Segment Length
10Base2	Thinnet; cheapnet	10 Mbps	Thin coaxial cable RG-58	185 meters
10Base5	Thicknet, yellow hose	10 Mbps	Thick coaxial cable RG-8 or RG-11	500 meters
10BaseT	10BaseT twisted-pair Ethernet UTP	10 Mbps	Unshielded twisted-pair CAT3, CAT5	100 meters
10BaseFL	Fiber Ethernet FOIRL	10 Mbps	Multimode fiber optic cable	1000 meters
100BaseT4	Fast Ethernet	100 Mbps	4 pair telephone grade cable	100 meters
100BaseTX	Fast Ethernet	100 Mbps	2 pair data grade cable	100 meters
100BaseFX	Fast Ethernet	100 Mbps	2 strands fiber cable	400 meters
1000BaseT	Gigabit Ethernet	1 Gbps	4 pair Cat5e	100 meters
1000BaseLX/LH	Long haul Gigabit Ethernet	1 Gbps	Multimode fiber	10 kilometers
1000BaseZX	Extended Gigabit Ethernet	1 Gbps	Single-mode Fiber	100 kilometers
10GBase	10 Gigabit Ethernet	10 Gbps	Fiber, CAT6A, CAT7, CAT7B	300 meters
10GBaseLX4	Long haul 10 GB Ethernet	10 Gbps	Single-mode fiber	10 kilometers

Ethernet can run over a variety of media types including several types of coax, twisted-pair, and fiber optic cable, as well as wireless formats, including radio signals and infrared. Table 1.1 lists several of these media types. The first number indicates the speed in megabits, the “base” refers to baseband transmission meaning that the entire bandwidth is dedicated to just one data channel, and the last number or letter indicates the approximate maximum segment length or the media type.

A second network architecture, token ring, or IEEE 802.5 (Figure 1.10), was developed in the early 1970s by IBM. A token ring network is often preferred for time-sensitive and mission-critical applications. Token ring networks use the token passing access method. Only the computer that has the 24-bit packet of data called the token may use the network. This token is generated by a designated computer called the active monitor and

passed around the ring until one of the computers wishes to use the network. When a computer wants to use the network, it seizes the token, changes the status of the token to busy, inserts its data frame onto the network, and only releases the token when it receives a confirmation that the data packet has been received. A token ring network uses a sequential logical topology, which was traditionally a ring physical topology but now is typically a star topology. IBM specified two architectures that operated at 4 and 16 Mbps. Token ring networks are no longer widely supported. Ethernet and token ring standards are typically associated with the data-link layer of the open systems interconnection basic reference (OSI) model (Figure 1.11), in particular the media access control (MAC) sublayer that defines the access method and framing format corresponding to the LAN protocol.

Starting Delimiter	Access Control	Frame Control	Destination Address	Source Address	Optional Routing Information Field	Optional LLC Fields	DATA	Frame Check Sequence	Ending Delimiter	Frame Status
1 octet	1 octet	1 octet	6 octets	6 octets	Up to 18 octets	3 or 4 octets	Unlimited size	4 octets	1 octet	1 octet

Figure 1.10: IEEE 802.5 Token Frame Layout

Layer Name	Example of Protocols or Standards		Comments
7 Application	X.400, X.500		Utilities that support end-user application programs
6 Presentation			Encryption, code translation, compression
5 Session			Establishes, maintains, and terminates sessions between applications
4 Transport	TCP, UDP, SPX		Provides reliability (end-to-end recovery and flow control)
3 Network	IP, IPX		Establishes, maintains, and terminates end-to-end network links
2 Data Link	Logical link control sublayer	CSMA/CD - IEEE 802.3 IEEE 802.4 - Token Bus IEEE 802.5 - token Ring Arcnet	Delivers reliability for point-to-point connections [built into NICs]
	Media access control sublayer		
1 Physical	RS-232-C, 10Base-T, 10Base-2, 10Base-5, 10Base-F		Establishes, maintains, and terminates physical connections

Figure 1.11: Categorizing LAN Architectures: The OSI Model

In the mid-1980s, the American National Standards Institute (ANSI) X3T9.5 standards committee released a standard for data communications in a local area network called fiber distributed data interface (FDDI). FDDI is similar to token ring, using dual counter-rotating rings. The primary ring is used for data transmission with the main function of the secondary ring for backup. FDDI can extend the range of a local area network up to 100 kilometers at 100 Mbps. FDDI uses optical fiber as the transmission media. A similar architecture uses copper and is called copper distributed data interface (CDDI).

LAN Hardware and Media

There is a variety of media choices for connecting computers to a local area network. Early networks used copper wires—either coaxial or twisted-pair. The standards detailing the LAN hardware and media are associated with the physical layer of the OSI Model.

Copper Wire

Coaxial cable consists of a center wire surrounded by insulation and then a grounded shield of braided wire. The shield minimizes electrical and radio frequency interference. A coaxial cable was typically referred to as

either thinnet or thicknet. Thicknet (Figure 1.12) was the original standard for Ethernet and is defined by the IEEE 10Base-5 standard and uses 50 ohm coaxial cable (RG-8 or RG-11 A/U) with maximum lengths of 500 meters. Thinnet (Figure 1.13) is defined by the IEEE 10Base-2 standard and uses 50 ohm coaxial cable (RG-58 A/U) with maximum lengths of 185 meters. RG-58 is similar to the coaxial cable used with cable TVs. Cables in the 10Base-2 system connect to other devices with BNC connectors (Figure 1.14).

Twisted-pair networking cable also has two different forms—UTP (unshielded twisted-pair) and STP (shielded twisted-pair). Both types of cable consist of either two or four pairs of wire. Each pair is twisted together. Shielded twisted-pair cable has an additional layer of conducting material surrounding the twisted-pairs of wires. Unshielded twisted-pair cable does not have the additional layer. Telephone companies use UTP cable with two twisted-pairs of wires. UTP is the most common and least expensive method for networking computers (Figure 1.15). There are seven categories of unshielded twisted-pair cabling ranging from Category 1 (CAT1), which is ordinary telephone cable used to carry voice, to Category 7 (CAT7) (Figure 1.16), which is designed for high-speed networks. CAT6 and CAT7 use 23 AWG copper as opposed

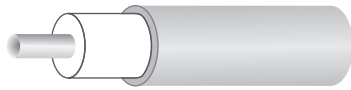


Figure 1.12: RG-58 Coaxial Cable



Figure 1.13: RG-8 Coaxial Cable



Figure 1.14: BNC Connector



Figure 1.15: CAT5 Patch Cable

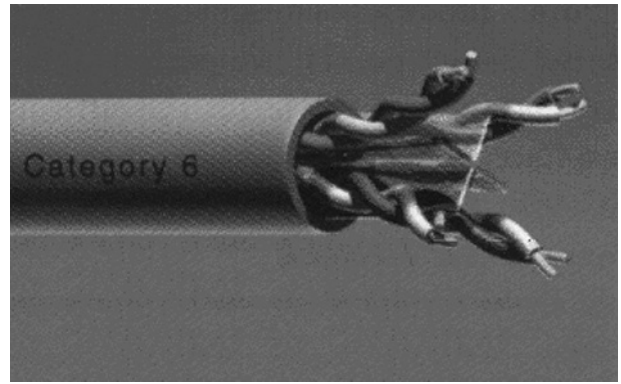


Figure 1.16: CAT6 Twisted-Pairs of Wires

to the 24 AWG used in CAT5/CAT5e and lower, resulting in less signal attenuation (loses signal strength) at higher speeds and distances. CAT6 also uses a tighter twist ratio that reduces the internal crosstalk. CAT7 uses individually foil-shielded twisted-pairs to minimize crosstalk. UTP and STP use RJ45 connectors (Figure 1.17) for connectivity to different networking devices.

Fiber Wire

Fiber-optic cable (Figure 1.18) has become common as demand increases for higher transmission speeds. Fiber-optic cable transmits data using pulsating laser light instead of electricity. Fiber-optic cable consists of a thin glass or plastic filament protected by thick plastic padding and an external plastic sheath. A light signal allows the data to travel faster, farther, more reliably, and more securely than electricity. Fiber cable can send reliable signals at speeds of 100 GB/s as far as 40 kilometers. Unfortunately, fiber-optic cable is expensive to buy, install, and maintain. Although not impossible, it is more difficult to intercept data carried by fiber-optic cable. Fiber-optic cable is less susceptible to noise and interference.

Wireless

Wireless LANs have become commonplace in businesses and homes. WLANs are often referred to as WiFi or 802.11 networks. Early wireless LANs were light-based using infrared light to transmit the data. Wireless LANs that are light-based require line of sight for all devices on the network. Because of this limitation and the slow data speed, there are only a few light-based infrared wireless LANs.

Most wireless LANs use radio waves for data transmission. Each device in a wireless network requires an antenna to receive and transmit the radio signals. Wireless LANs can be peer-to-peer or ad hoc networks (Figure 1.19), requiring that each device be equipped with a wireless network card that contains the antenna, or a more complete network called an infrastructure network that requires an access point (Figure 1.20). The access point contains an antenna, a radio transmitter, and a wired network interface, typically an RJ45 port. The access point acts as a base station (similar to a hub) for the wireless network and as a bridge between the wireless and wired networks.

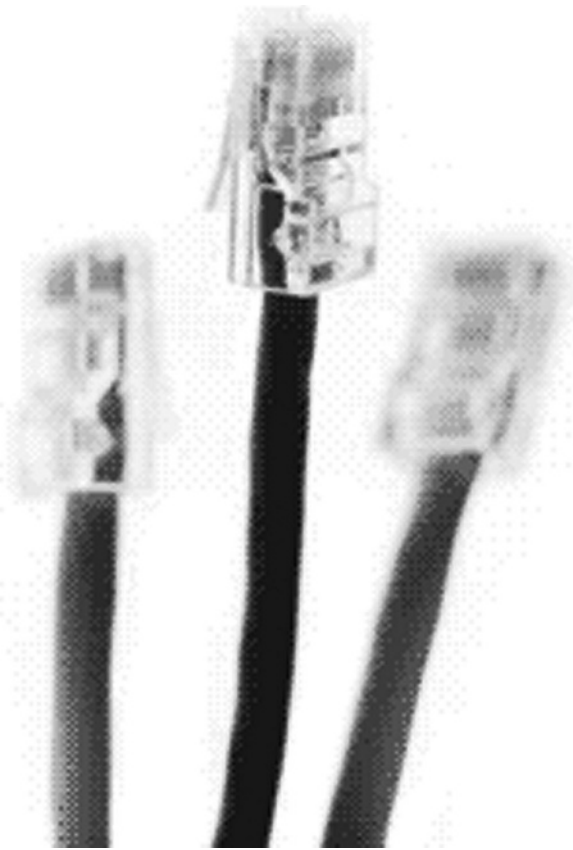


Figure 1.17: RJ45 Connector



Figure 1.18: Fiber-Optic Cable

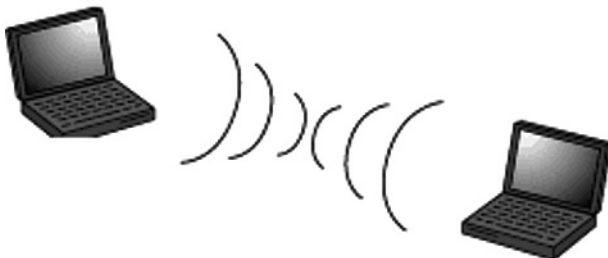


Figure 1.19: Peer-to-Peer Wireless Network

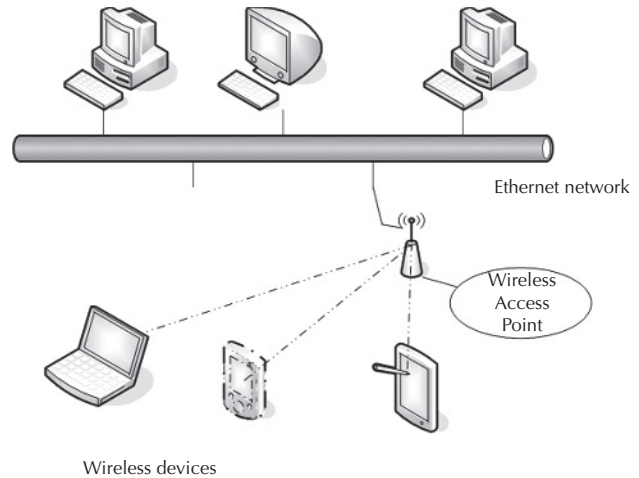


Figure 1.20: Wireless Network with Access Point

Hardware Devices

Regardless of whether the network is wired or wireless, every device on the network must be connected to the network with a network adapter or network interface card (NIC) (Figures 1.21, 1.22, and 1.23). The card must be physically connected to the device, either installed on the motherboard, directly into a slot in the computer or connected via a port like a USB port. Most laptops and tablet PCs manufactured after 2004 have built-in wired and wireless interfaces. The network card provides the interface between the node on the network and the network media. Because communication in a wireless network occurs through the air, it is easier for the signal to be intercepted. As wireless becomes more pervasive, security has become a significant issue.

Several factors limit the radius of a local area network. The farther a signal travels along the wire or through the air, the more likely it is to be degraded by noise. As the signal travels, it loses energy and becomes weaker, thus becoming difficult to read. As the network radius increases, it becomes more likely that two or more machines will transmit at the same time, causing a "collision." It will take longer for the machines to detect the collision. There are several ways to increase the radius of a network.

The simplest device to use is a repeater. A repeater (Figure 1.24) is an electronic device used to extend the distance of a network by amplifying the signal and reducing the electrical interference within the network. The repeater relays the data from one segment of the network to another without inspecting or modifying the data. Repeaters can also be used to connect segments of the network that use different cable media. Repeaters operate at the OSI Model physical layer of the network.

A hub (Figure 1.25) is a multiport repeater that allows the distance of the network to be extended as well as allowing multiple devices to connect to the LAN. A hub is a device that aggregates more than one connection (Figure 1.26). Like a repeater, the hub does not inspect or modify the data. Ethernet networks with only hubs and repeaters are constrained by the 5-4-3 rule that limits the

connections between two end points to no more than five segments each with no more than four repeaters where no more than three of the repeaters connect additional active nodes.

Repeaters and hubs boost the signals on a network, but don't solve problems involving collisions. Other devices, however, alleviate this problem by limiting traffic on the network. A bridge (Figure 1.27) is a device that connects two or more networks typically running the same network protocols. It allows the isolation of the different networks. The different networks may have different topologies. Bridges are used to increase the efficiency of a network by limiting the collision domain to "one side" of



Figure 1.23: PCMCIA Wireless NIC

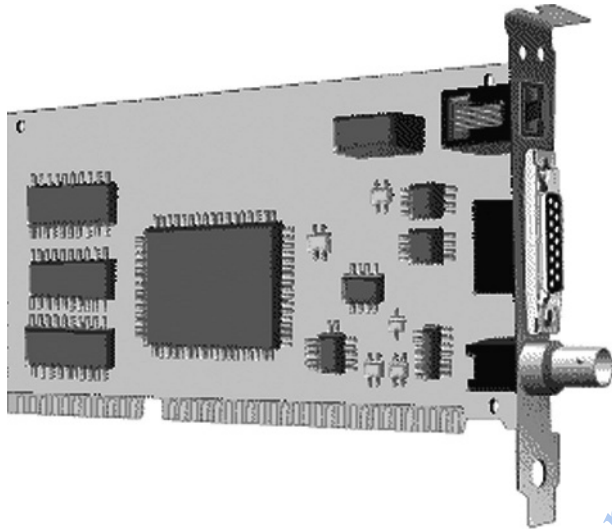


Figure 1.21: Network Interface Card (NIC) with RJ45, BNC, and AUI Connections



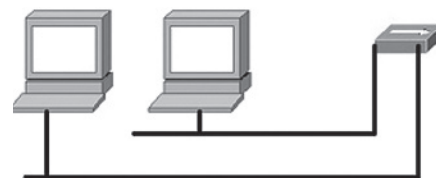
Figure 1.24: Repeater



Figure 1.22: Network Interface Card with RJ45 Connection



Figure 1.25: Four-Port Hub



Two hosts connected with a hub.

Figure 1.26: Hub Connecting Two Hosts

the bridge. By doing this, networks can be expanded without a significant increase of traffic. Bridges operate at the physical and data-link layers and make use of the physical addresses associated with the network cards. Segmenting can also improve LAN traffic by isolating workstations that pass large files or data sets between them.

A switch (Figure 1.28) is a multiport bridge. Switches may also be referred to as switching hubs. A switch combines the appearance and functionality of a hub with the additional functionality of a bridge. Switches provide full duplex transmission between nodes, eliminating collisions and enhancing the performance of the network. Switches have typically replaced hubs in most local area network installations. A specialized type of bridge or switch called a “translating bridge” or gateway can be used to connect two or more networks using different protocols, such as Ethernet and token ring.

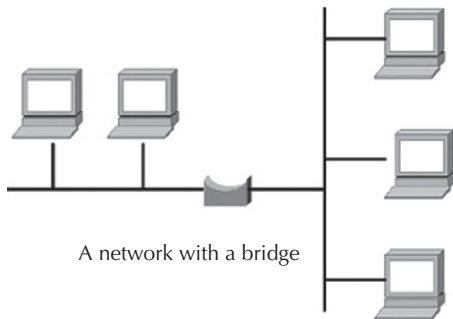


Figure 1.27: Bridges



Eight-port switch

Figure 1.28: Switches

Although typically not part of a LAN, routers provide the interface between a LAN and WAN, or between different LANs. Routers route the traffic between different networks by maintaining tables that identify a network by its associated addresses. Routers forward layer 3 IP packets between different layer 2 domains. Routers are more sophisticated than switches and bridges and work at a higher level of the network.

Virtual LAN

Traditional networks use hardware devices, like routers to limit the broadcast of packets of data between sub-networks. A software solution that provides the same functionality is a Virtual LAN (VLAN). VLAN is a logical local area network that extends a traditional LAN to a collection of LAN segments, even if the LAN segments are on different network switches. VLANs improve the bandwidth usage by segmenting the LAN into a group of broadcast domains that restrict the broadcast of packets to the virtual LAN. VLANs provide a software solution for managing multiple networks in addition to addressing issues of security and scalability.

LAN SOFTWARE

LAN software can be classified into three categories: network operating systems, network utilities, and network applications software. Not too many years ago, operating systems and network operating systems were distinct. Today almost all operating systems have the client functionality of a network operating system built in. In other words, you do not need to add any additional software to the operating system to get the computer to function on a network. All of today’s popular operating systems including all recent versions of Microsoft Windows, all versions of Linux and UNIX, and all versions of the Macintosh OS support the connection of a computer to a network right out of the box. In addition to the usual computing tasks performed by an operating system, a network operating system also:

- Manages the network connection
- Manages data traffic between the computer and the network

Table 1.2: Networking Devices

Networking Device	OSI Model Layer	Function
Repeater	Physical (1)	Retransmits the communication signal and is used for extending the radius of a network
Hub	Physical (1)	Multiport repeater
Bridge	Data-link (2)	Connects two or more local area networks that typically use different media but the same network protocol
Switch	Data-link (2)	Connects multiple network segments. It functions as a multiport bridge featuring micro-segmentation that allows two devices to communicate only with each other at that moment.
Router	Network (3)	Connects two or more networks that may use different network protocols

- Manages the flow of data between the different devices
- Manages communication and messages between the network users
- Provides for security of the data and other resources available on the network

The network operating system provides the interface between the LAN hardware and the applications running on the host.

Included with most of the network operating systems are specific network utilities like ping, ARP, and traceroute, which provides network control/management functions. Ping is used to test whether a specific device is accessible over the network. It accomplishes this by sending an Internet control message protocol (ICMP) ECHO_REQUEST packet to another device and waits for an ECHO_REPLY packet of data from the other device. This provides verification of successful connectivity and gives an indication of the time it takes to reach the target machine. Ping is a useful utility for troubleshooting networking problems. Address resolution protocol (ARP) is used to map the physical address of a networked device to the corresponding network IP address that has been assigned to the device. Traceroute uses the ping utility to map the route that packets of data take from a source to a destination machine. Network operating systems typically include drivers for most network adapters so that the adapter can be plugged into the computer and the computer can be functioning on the network without additional configuration.

Network application software includes client front-end software that is specific for use by client computers. This would include programs like Web browsers and e-mail software clients that would be run when needed. Hosts functioning as servers would have server software that would be constantly running waiting for connections from clients. Web servers and e-mail servers would be examples of this. Other types of network application software would include database client and server software as well as groupware software.

ROLE AND APPLICATIONS OF LANS

One of the major uses of LANs is to facilitate connections by users to the Internet. This requires the connection of the LAN to the Internet either via a dial-up telephone connection, a broadband connection, or a leased line. A dial-up connection requires a modem that converts the network's serial digital signal to the phone line's analog signal. A broadband connection typically requires a digital subscriber line (DSL), integrated services digital network (ISDN), or cable modem and a router and switch. Most commercial off-the-shelf devices include the functionality of a router, a switch, and often a wireless access point. A leased line connection requires a router that is connected to another hardware device called a channel service unit/data service unit (CSU/DSU). The CSU/DSU in turn connects the network's router to the end of the leased line (e.g., T1 or T3) and converts the network's serial data signal to and from the leased line's digital signal. The leased line provides a high-speed Internet connection for the organization owning the LAN. Typically,

the leased line is rented from a telecom provider through an ISP. The ISP maintains the actual connection to the Internet using its own upstream router.

Connecting a LAN to the Internet requires that the devices on the LAN support the TCP/IP suite of protocols that provide the foundation of the Internet. At a minimum, a computer accessing the Internet must have or be assigned an IP address, subnet mask, and default gateway. These protocols are necessary for computers on the LAN to be able to communicate with devices in other parts of the Internet. The TCP/IP suite of protocols include:

- Transmission control protocol (TCP) [RFC 793]—establishes and maintains the Internet connection
- Internet protocol (IP) [RFC 791]—handles the routing of packets of data across the Internet
- Simple mail transfer protocol (SMTP) [RFC 821]—handles the transferring of e-mail messages
- Post office protocol (POP/POP3) [RFC1939]—facilitates e-mail drop services
- HyperText transfer protocol (HTTP) [RFC 2616]—facilitates the delivery of Web documents
- File transfer protocol (FTP) [RFC 959]—transfers files
- Telnet [RFC854]—allows users to remotely connect to other computers over the Internet
- Secure shell (SSH) [RFC 4250]—allows users to securely connect to other computers over the Internet

Many organizations have set up their own internal Internet called an intranet. An intranet is a private network that uses the same protocols as the Internet. An intranet appears to the user like the Internet, but it is typically not open to anyone outside the organization. An intranet is not a replacement for a LAN, but rather runs within a LAN and supports many of the same applications as the Internet, typically Web servers and browsers, e-mail servers and clients, as well as additional groupware software. The core of most intranets is the web site, which typically contains most of the internal documents that need to be disseminated among the organization's members. Setting up an intranet site on an organization's LAN requires a lot of organization and planning in selecting the hardware, software, and data needed to create a functional intranet.

Some organizations have taken the intranet concept one step further and link to external partners of the organization through the Internet via an extranet. An extranet is an intranet that may include access by customers, suppliers, and trusted partners.

WIRELESS LOCAL AREA NETWORKS

WLAN Standards

Wireless local area networks (WLANs) have become ubiquitous in offices and many homes. WLANs provide the freedom to access data without being tethered to the network with wires. WLANs enable users to take laptops and handheld computers anywhere, anytime and still be able to access the network. This is becoming more important in today's world of information.

Wireless networks are generally easier and less expensive to install. Most laptop and other portable devices can be purchased with a built-in WiFi card (wireless NIC). WiFi cards and USB WiFi devices can be installed with older laptops and desktop computers. Wireless networks require spending less money for the purchase and installation of the network media. Wireless access points and NICs have become more affordable in the past several years.

The Institute of Electrical and Electronics Engineers (IEEE) created the first wireless standard, 802.11, in 1997. In 1999, the IEEE 802.11 working group developed and released two standards: 802.11a and 802.11b. The 802.11b standard operates at 2.4 GHz ISM band and became the more popular of the two standards. 802.11a networks operate at 5 GHz and support a higher bandwidth. However, 802.11a networks are more costly to install and have a shorter radius.

In 2002–2003, the IEEE 802.11 group released the 802.11g standard in an attempt to take advantage of the 802.11a and 802.11b standards. 802.11g operates at 2.4 GHz and is compatible with 802.11b networks. 802.11g networks support a higher bandwidth and larger radius than 802.11b at a slightly higher cost for the devices. Both standards 802.11b and 802.11g use the unlicensed 2.4 GHz ISM band, and support transmission speeds up to 11 Mbps and 54 Mbps respectively. Many cordless phones and other electronic home devices that can cause interference also use the 2.4 GHz ISM band. 802.11a uses the 5 GHz UNII band and supports transmission speeds up to 54 Mbps.

The draft 7.0 of the 802.11n standard was approved in 2008. The official standard is expected to be ratified in 2009. Many manufacturers have released 802.11n access points based on the draft standard. 802.11n devices are expected to replace older WiFi devices with ones that will be able to communicate at up to 250 Mbps. 802.11n devices make more efficient use of the available spectrum and as a result boost performance. The standard 802.11n is based on multiple-input multiple-output (MIMO) technology where two or more radio antennas allow increased communication speeds.

Other wireless networking standards are Bluetooth for very short range (less than 10 meters) and low bandwidth communications and WiMax (based on the IEEE 802.16 WAN standard) for long-range wireless communications.

WLAN Management

Installing a wireless network involves turning on the access points, installing the software for the access points and NICs, and identifying the access points to which the NICs connect. Modifying a wireless network is easier, but

does have its issues. There is no need to remove and/or relocate cable. Concern for network cable failure is minimized. Companies are using WLANs for keeping track of inventory in warehouses. Workers that need to be constantly in contact with their network are more frequently using wireless LANs. WLAN devices have become commonplace among workers in the health care industry. One area where WLANs are beginning to have a great impact is in education. Students and faculty no longer need to find wired computer labs to communicate and work. With wireless devices, students and faculty can access the networks in any building where wireless access points have been installed.

Wireless networks still have some drawbacks. Chief among these drawbacks are the limitations on distance and bandwidth. The radius of a WLAN can be extended by adding additional access points and radiofrequency (RF) repeaters to the network. Adding additional access points on the same channel can also help optimize the use of the limited bandwidth of the WLAN. There are also standards and associated wireless devices that support increased bandwidth. If these devices are unable to communicate at the preferred speed, the devices will drop the speeds to optimize the communications. This often happens when there is interference in the communications from other devices. Changing the channels can often overcome this problem.

WLAN Security

The other major drawback for WLANs is security. A WLAN transmits radio signals in the clear over a broad area. This allows an intruder to lurk anywhere within range and intercept the signals from the wireless networks. One way of inhibiting access to wireless networks is to turn on encryption. By default, most wireless networks use wired equivalent privacy (WEP). WEP relies on a secret key that is shared between a mobile station and the access point. The secret key is used to encrypt packets before they are transmitted, and an integrity check is used to ensure that packets are not modified in transit. Unfortunately, WEP is easily compromised. Better security can be obtained by using WiFi protected access (WPA and WPA2), which uses a pass phrase as a seed for the encryption. There are a variety of additional security measures that should be implemented to better secure the wireless network.

In 2004, the IEEE released an amendment to the 802.11 standards to deal specifically with security over 802.11 wireless networks. The 802.11i replaced the WEP encryption standard with WPA2, which uses the advanced encryption standard (AES) block cipher and requires a second encryption standard known as temporal key

Table 1.3: 802.11 Standards

Standard	Frequency Band	Maximum Transmission Speed	Indoor Range
802.11a	5 GHz	54 Mbps	35 meters
802.11b	2.4 GHz	11 Mbps	38 meters
802.11g	2.4 GHz	54 Mbps	38 meters
802.11n	2.4 and/or 5 GHz	100–250 Mbps	70 meters

integrity protocol (TKIP). 802.11i includes the 802.1X standard for authentication.

LAN Installation

Before a LAN is installed, a lot of planning needs to take place. The process can typically be broken down into seven steps:

1. Needs analysis
2. Site analysis
3. Equipment selection
4. Site design
5. Server configuration
6. Installation schedule
7. Installation

Needs Analysis

The first aspect of installing a LAN is determining the needs of the organization and the users by asking a series of questions:

- Is a LAN needed?
- What aspects of the network are needed?
- Who will be using the network?
- What will they be using the network for?
- Will a LAN help the bottom line of the organization?

There are many reasons for installing a local area network. These might include:

- Need for improved communication
- Need for centralizing data
- Need for sharing hardware
- Need for application sharing
- Need for automating work flow
- Need for enhanced security of data

Site Analysis

Once a need has been established, it is necessary to determine where the LAN will be installed. What parts of the organization's site will be networked? Where will the servers be located? A site plan will need to be drawn. If a fire escape plan is available, it can be used as a template for the building and for the location of rooms and doors. It is best if the architectural plans can be found. The site plan (Figure 1.29) is a map of the location where the network is installed and should include:

- The dimensions of the site, including the location of each employee
- The location of all immovable objects, including doors and windows
- The current location of all moveable objects
- The location of heating, ventilation, and air conditioning systems and ducts
- The location of electrical outlets and the current wiring scheme
- The current location of all computer equipment and the planned location for any additional devices
- The number and location of network connections in each room

Equipment Selection

As the site plan is developed, an inventory of equipment on hand needs to be conducted. An inventory of equipment will identify the capabilities of the equipment incorporated into the proposed network. This will identify which equipment will be obsolete once the network is installed and which equipment will require modification. For example, older workstations may still be useful as print servers. Table 1.4 shows a table of the features to be noted in the equipment survey.

Once the current equipment has been inventoried, it is now time to identify new equipment that will need to be purchased. This list should be correlated with the

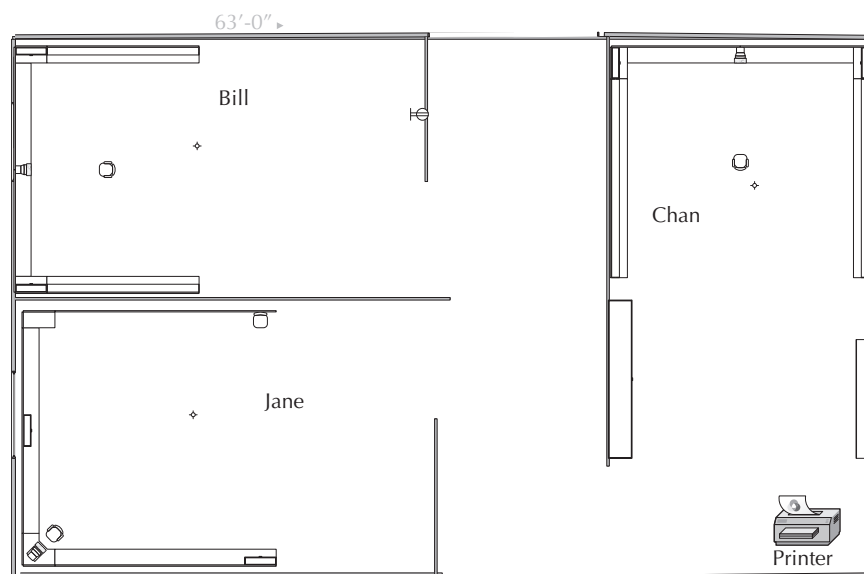


Figure 1.29: Sample Site Plan

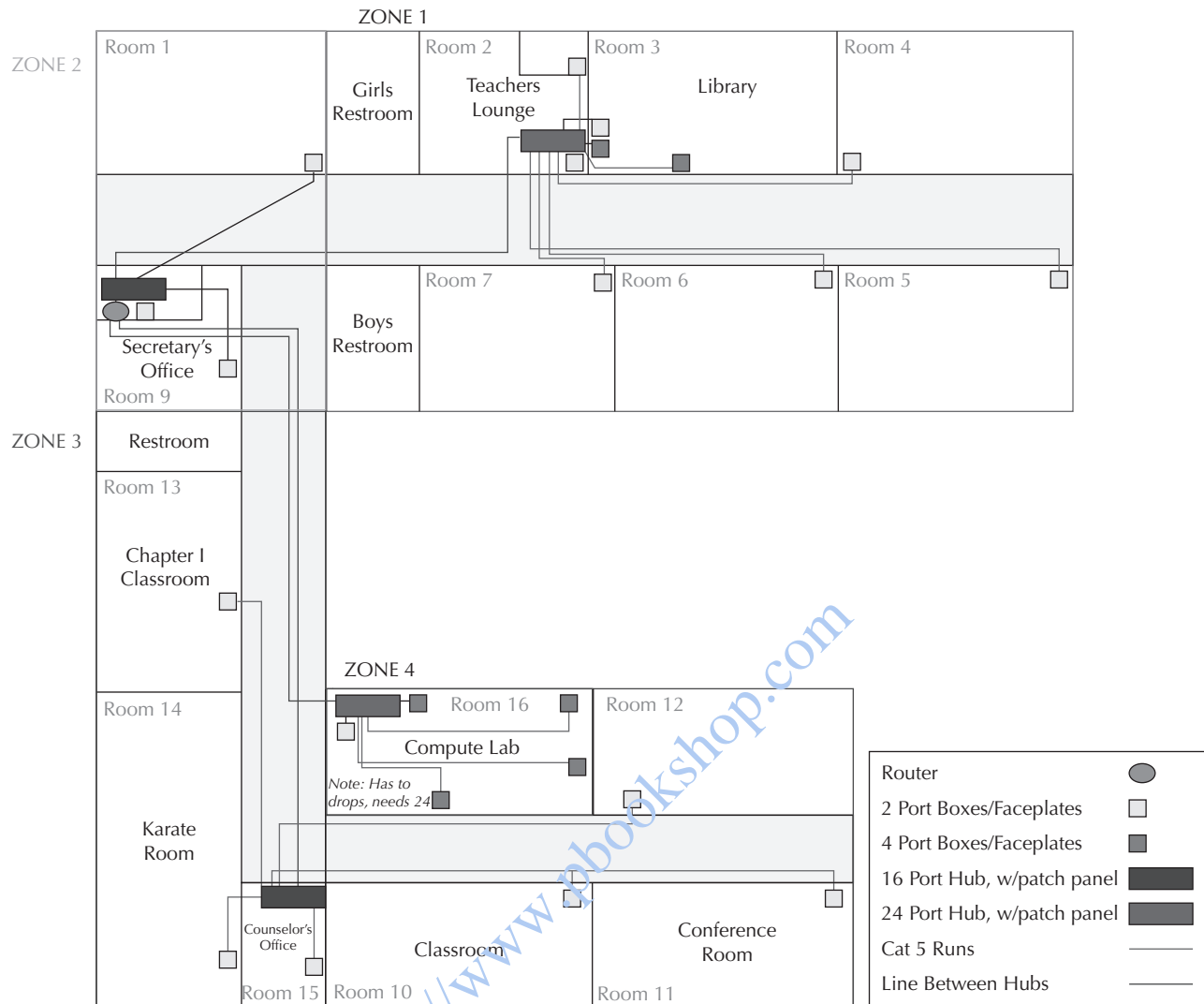


Figure 1.30: Sample Site Design

Server Configuration

Once the computers arrive that will be installed as servers, they need to be configured. Server software needs to be installed, and the directory structure of the server needs to be organized. The directory structure begins with the root directory with all other directories within it and the files and subdirectories within those. Typically, you will have directories for the network operating system, separate directories for each server application, and directories for the clients who will be connecting to the server. Network information, including MAC and IP addresses for all devices, needs to be recorded and stored in a secure location.

Installation Schedule

Networks take a considerable amount of time to install. It is important to have an installation schedule. There will be times when employees' computers will need to be turned off and possibly moved. Disruption needs to be minimized wherever possible. Be sure to include in the installation

schedule the possibility for shipping delays on the equipment that has been ordered. Be sure to read the manuals before the installation begins so that there will not be any surprises once the installation starts. Also prepare the site before the installation begins. This may involve moving furniture, installing new outlets, and removing equipment that will no longer be used. Do not forget to back up any data that is on systems that will be affected by the move.

Installation

Before the installation begins, it is best to discuss everything with someone who has been through a LAN installation before. Have this person look over the designs, schedules, and forms to ensure that nothing has been forgotten. Depending on the size of the installation, it may take anywhere from a couple of hours to a couple of days. Be prepared for delays. If this is a wired network, conduit may need to be installed, and the cable media will need to be pulled. This is the part that typically takes

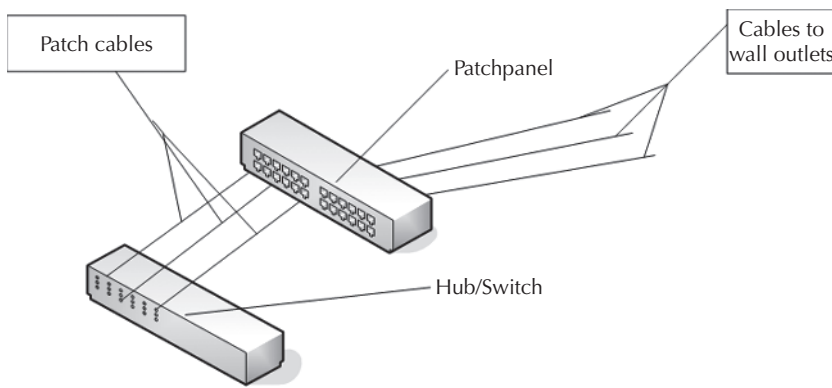


Figure 1.31: Configuration of Wiring Closet

the longest time. While the cable media is being pulled or shortly thereafter, the remaining components will need to be installed. This would typically include the patch panels in the communications rooms and the wall outlets for each device that will be networked (Figure 1.31). Once this is completed, the electronic devices (hubs, switches, etc.) will need to be installed. If network cards need to be installed in the older computers, this will be done next. Finally, the software for the network cards will need to be installed on each workstation and server if it hasn't already been done. Be sure to install the appropriate network software.

The final two stages of the installation are the testing and training. Every device will need to be tested to ensure that its network connection works. This should be done before any of the users access the network. Be sure to test all of the network devices and the networked printers. Applications, service, and end-to-end testing must be performed. It is imperative that the security analysis of the network, including the wireless components, be conducted. The final phase is training. Users will need to be trained in the procedures they will need to follow to use the network.

LAN ADMINISTRATION

Once the LAN has been installed, there are several key aspects of administering the network.

Configuration List

Using the equipment inventory forms developed during the installation along with similar documentation for the new devices, a set of configuration lists needs to be developed. These would include a list of all computers similar to the equipment inventory form, directory lists for each server that is installed, a list of all server users, a list of all printers and other shared devices. It is also very important to keep copies of the network plans developed for the installation of the network.

System Log

The system log is documentation for the network. It provides a detailed history of the network's hardware, software, and configuration features. As changes are made to the network, these changes need to be documented in

the system log. As problems arise with the network, these also need to be documented in the system log. This log needs to be maintained from the beginning. The system log should include all hardware and software warranties, hardware and software information, current setup structure, backup and recovery plans, backup logs, and error/downtime logs.

Training

Training does not end after the network has been installed. The network is a dynamic part of an organization's computing system. As changes are made, employees will need additional training.

Backup

As more and more data is kept on networked servers and shared by more than one user, it becomes critical that a procedure be established for backing up critical data. This may be the most important task for a network administrator. Hardware and software can be replaced. New employees can be hired. But it is difficult to re-create large amounts of data. The network administrator must establish a schedule for backing up all critical data. Separate storage area network (SAN) or networked attached storage (NAS) may be needed to provide added storage protection. Critical software may not necessarily be replaced and should be backed up as well. Configuration files on all servers should be backed up.

Security

Once computers become accessible to other individuals, security issues need to be considered. In a networked environment, users will need user IDs and passwords. If security is extremely important, then encryption of data may also need to be implemented. Software like PGP can be used for encrypting e-mail and data on hard drives. If the local area network is attached to another network, then a firewall or a virtual private network (VPN) may be necessary to control access to critical data between the two networks.

LAN SECURITY

In today's world of ubiquitous local area networks, security is of the utmost importance. This is true whether the LAN

is a peer-to-peer or client-server network. Security is all about confidentiality, integrity, and availability. Where necessary, information should be confidential. The information should be only available to those who are authorized to access it. The integrity of the information must be maintained. We need to be assured that the information has not been altered. The availability of the information must be preserved. Authorized users need to be able to access the information and computing resources when needed.

Securing a LAN requires a multilayered approach. One of the main themes in security is “defense in depth” where multiple layers of technology and multiple procedures need to be implemented to minimize the threats to the local area network. This includes the physical security protecting the devices, database security protecting the data, and network security protecting the transmission of the data.

Physical Security

“I touch it, I own it!” Without physical security, there is no security. Having physical access to the devices and computers on a network is the greatest vulnerability in network security. No matter how strong other facets of security, if an attacker can physically access computers and other devices, the LAN can be easily compromised.

All LAN servers must be locked in a physically secure area. Network devices and network cable need to be protected from intentional and unintentional disruption. To avoid inadvertent compromise, servers should not be used as client workstations. It is too easy for client-based vulnerabilities to be compromised and to affect the server software running on the same computer. Securing a LAN includes more than preventing attacks. An inadvertent loss of power to the computers and network devices can be catastrophic. All devices should be protected by surge protectors. Power to servers and other critical hardware needs to be stabilized using uninterruptible power supplies (UPS). The UPS battery needs to be checked regularly. An alternate power supply, such as a generator or second utility grid should be available for mission-critical LANs. Temperature controls need to be in place for any LANs and devices that are mission-critical. Wherever feasible, redundant network connections need to be installed in case of a network disruption. Redundant servers should be available in case a server is compromised or malfunctions.

Access Security

The first line of defense is access control. Access to servers and the data needs to be controlled. This can be implemented by instituting controls at the network level as well as individual controls at the directory and file levels. Connections to all servers and the network should be controlled through authentication procedures. All users must be registered and authenticated. There should be no guest accounts. Minimally the use of user IDs and strong passwords should be required for all connections to the network. All users need to use nontrivial passwords that are difficult to “guess.” This includes using passwords that are sufficiently long and not using words that

would be found in dictionaries or other wordlists. These passwords should be frequently changed and checked. Unfortunately, too many passwords can create operational issues. Oftentimes, users forget their passwords. A mechanism needs to be in place to address this problem. One mechanism is to use a secure password vault where users can securely store their passwords. All default passwords for servers, operating systems, and applications must be changed immediately. All obsolete user accounts need to be terminated immediately. It may also be necessary to restrict user access to certain days and times to better control access to sensitive data.

There should be several levels of access to directories and files. These typically would include read, write, and execute. Users need to be given the minimum privileges to access all of their files and directories. All data must be protected from access by unauthorized users. It is important that authorization be carefully planned. Audit logs of successful and unsuccessful access to systems and files may need to be kept to allow for tracking of problems that arise.

Data Security

Where necessary, critical data needs to be protected. In addition to those mechanisms discussed above, additional layers of security may be necessary. In the case of databases, views need to be provided to permit users to access only the minimum that is necessary.

Data confidentiality is especially important. Where necessary, encryption software needs to be used to protect confidential and sensitive data. Controls need to be implemented to protect all confidential and sensitive data stored and/or processed on the LAN. These controls should include any removable media associated with the LAN. It is important that all confidential and sensitive data be removed before disposing of the media that the data resides on. Remember that simply deleting a file that contains the data may not be enough. Be sure to delete any copies of the files stored on backup media and “empty the trash.” Removable storage like disks and flash drives, as well as permanent storage like hard disks need to be thoroughly erased before being recycled. If necessary, use software that overwrites every track of the storage device.

Backup procedures need to be implemented. All file servers need to be automatically backed up on a regularly scheduled basis. The backup media needs to be kept onsite for immediate recovery. Copies of the backup media need to be kept offsite in case the onsite backups are compromised. Both sets of backups need to be tested and audited to ensure recovery.

Network Security

There are two major approaches to securing a local area network: host-based security and network-based security. Typically, both approaches are combined to provide multiple levels of security.

In host-based security, selected hosts are separately protected. This could range from installing antivirus software and personal firewalls on each computer in the network, to installing a host-based intrusion detection

system on each server. Minimally, every server should be protected with antivirus software, antispyware, and a personal firewall. If possible, the important servers should also be shielded by a host-based intrusion detection system.

Network-based security is equally important. Hardware-based security devices such as firewalls and intrusion detection devices are generally placed at the perimeter of the network, typically inside the router where they can monitor all traffic coming in and out of the local area network. Intrusion detection and intrusion protection devices can also be set up with agents installed on those hosts needing the most protection. These agents can then be monitored and managed from a central location. In more secure environments, there may be layers of network-based security both at the perimeter of the LAN as well as internal to the network. One layer of security is the placement of a firewall device (Figure 1.32) between the LAN (trusted network) and the outside (untrusted networks). Devices that require access to the Internet or other untrusted networks are often placed outside the firewall in a subnetwork often referred to as the DMZ (demilitarized zone). This provides an additional layer of security if one of these devices is compromised.

The network should be audited for the use of software for illicit purposes (e.g., sniffers, traffic monitors). Although network monitoring software, when used properly, are powerful tools for network management, they have the potential for misuse by others. No unauthorized connections to the network should be permitted. This would include rogue wireless access points and modem connections.

Malware

Malware includes programs like viruses, worms, and spyware. To protect against most malware attacks, antivirus and antispyware software needs to be installed on all servers and clients. It is imperative that this software be kept up-to-date on all computers. Most antivirus software vendors have procedures for automatically updating the software. The autoupdate feature should be configured to the shortest time that is tolerable by the users. All

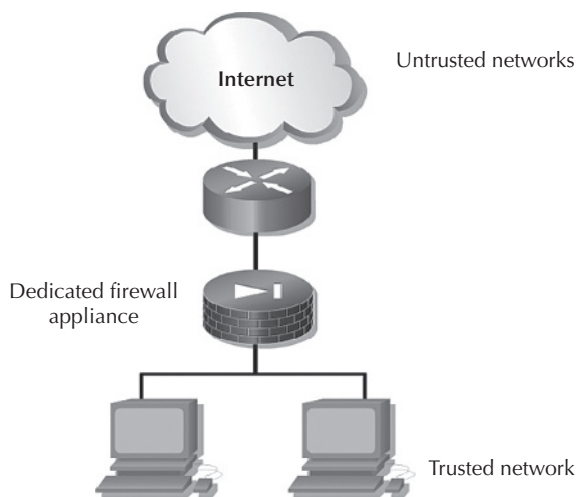


Figure 1.32: Placement of a Firewall

foreign media and all files downloaded from the Internet must be scanned for malware. The antivirus software needs to be running continuously. In addition to updating the antivirus software, it is mandatory that all operating systems and applications running on all computers in the network be patched. "Patching host software is probably the single most important thing companies can do to improve their security" (Panko 2004). Software vulnerabilities are constantly being exposed. Threats that exploit these vulnerabilities are rapidly developed and can best be prevented from compromising the system's security by downloading security patches as soon as the patches are available. Users should be trained in how to disconnect their device from the network in the event of a virus attack to isolate their host. One vulnerability in an operating system or application can destroy the entire network of computers.

Policy, Procedures, and Awareness

"Security is not a product, it's a process" (Schneier 1999). Using any security product without understanding what it does, and what it does not protect against is a recipe for disaster. Keep in mind that added security features tend to increase the complexity of the system and may decrease the degree of usability of the systems. Usability needs to be balanced with the increased need for security.

Any organization implementing or using a LAN must have a well-documented security policy. The policy should incorporate physical security procedures, e-mail, Internet acceptable usage, and network usage procedures. The policy should include procedures for incident response and a LAN risk analysis. The policy should include a focus on software use to ensure compliance with license agreements. All unauthorized copies of software should be removed from workstations and servers. The policy needs to outline what additional response is necessary when unauthorized software is discovered.

The policy must include procedures for ensuring that all software is patched on a regular basis. This is especially important for all security software including antivirus software and any intrusion detection and prevention software protecting the LAN and its resources.

As mentioned earlier, audit logs need to be invoked. These logs should not only document successful and unsuccessful access to resources on the LAN, but should record any and all anomalies. These audit logs must be reviewed regularly with procedures in place for addressing any security alerts or identified anomalies. All attacks and breaches of security need to be investigated immediately and followed up with appropriate responses.

"The most potent tool in any security arsenal isn't a powerful firewall or a sophisticated intrusion detection system. When it comes to security, knowledge is the most effective tool . . ." (Schweizer 2003). There needs to be a regular training program for administration and users. Administrators need to be trained on their responsibilities in managing the security of the LAN and its components. Regular security awareness sessions need to be scheduled and required for all employees including training against social engineering attacks. An important policy is to train before deploying any component in the network.

CONCLUSION

LANs play a very important role in providing computer resources to large numbers of users. They allow users to share hardware, software, and most importantly data. LANs also provide access to the Internet as well as organization intranets and extranets. With the continued emergence of WANs, the applications of LANs will continue to expand. It is imperative that we secure the LAN to ensure confidentiality, integrity, and availability of the data.

GLOSSARY

Access point: is a hardware device consisting of one or more antennae, a radio transmitter, and a wired network interface. Used as a bridge between a wireless network and a wired network. The access point acts a hub for the wireless network.

Attenuation: is a loss of energy from a signal because of resistance in the medium.

Bridge: is a network device for connecting two or more local area networks that typically use different media but the same network protocol.

Bus network: refers to a network where the nodes are connected to the same wire. Data is broadcast from one node to all other nodes in the LAN, even though the data may be intended for only one node.

Collision domain: is the segment of the physical network where data packets collide in an Ethernet network.

Ethernet: is a common data-link layer technology for networking computers in a LAN using the CSMA/CD access method.

Extranet: is a private portion of the Internet treated as an extension of an organization's intranet and allowing access to the organization's data by the organization's partners, customers, and so on.

Fiber-distributed data interface (FDDI): data link layer standard based on token ring for extended data communications using optical fiber.

Hub: is the central device in a star network for connecting multiple nodes to a network. It functions as a multiport repeater.

IEEE 802.3: is a collection of standards for CSMA/CD (Ethernet)-based LANs.

IEEE 802.5: is a collection of standards for token ring-based LANs.

IEEE 802.11: is a collection of standards for wireless-based LANs.

Internet: is a worldwide collection of networks linked together and built around the TCP/IP suite of protocols. It was originally conceived in 1969 by the Advanced Research Projects Agency (ARPA) of the U.S. government.

Intranet: is an organization's private internal network based on the TCP/IP suite of protocols.

Local area network (LAN): is a data communication network of computers, peripheral devices, and other network devices allowing data to be communicated at high speeds over short distances.

Logical topology or electrical topology: is based on how the devices of the network are electrically configured.

Network: is an interconnection of two or more computers or devices.

Network interface card (NIC): is an adapter for connecting a computer or device to the network media.

Personal area network (PAN): is a communication network of computing devices within close proximity of a person, typically a few meters.

Physical topology: is based on the way the nodes are physically configured in the network.

Repeater: is a network device that retransmits the communication signal and is used for extending the radius of a network. It operates at the OSI physical layer.

Ring network: refers to a network where the nodes are arranged in a closed loop where each device is connected directly to two adjacent devices.

Router: is a special-purpose network device that connects two or more networks at the OSI network layer.

Server: is a computer or other device that provides services or applications to other users. Examples include webserver and file server.

Segmented network: is a network that is broken into groups of devices and connections to improve performance and contain the broadcast traffic.

Social engineering: is the process of compromising a computer system and/or its data by manipulating the users.

Star network: has the nodes arranged so that each device is connected to a central device, typically a hub or a switch.

Switch: is a network device operating at the OSI data-link layer that connects multiple network segments. It functions as a multiport bridge featuring microsegmentation that allows two devices to communicate only with each other at that moment.

Wide area network (WAN): is a data communication network spanning geographically dispersed areas.

WiFi: is the trademark name for wireless technology used in networks.

WiMax (Worldwide Interoperability for Microwave Access): provides for the wireless transmission of data using a variety of transmission modes. WiMax is an alternative to cable and DSL enabling the delivery of the last mile of wireless broadband access.

CROSS REFERENCES

Client/Server Computing; Home Networking: Technologies and Management; Network Management; Wide Area and Metropolitan Area Networks; Wireless Wide Area Network Technologies and Implementations.

REFERENCES AND SUGGESTED READINGS

- Bautts, T., T. Dawson, and G. Purdy. 2005. *Linux Network administrator's guide*. 3rd ed., O'Reilly Media. Sebastopol, CA.
- Bishop, M. 2005. *Introduction to computer security*. Boston, MA: Addison-Wesley.
- Brain, M. 2008. How WiFi works. computer.howstuffworks.com/wireless-network.htm (accessed November 29, 2008).

- Burke, R. 2004. *Network management concepts and practice: A hands-on approach*. Englewood Cliffs, NJ: Prentice Hall.
- Cisco Systems, Inc. 2002. Token Ring/IEEE 802.5, Available at www.cisco.com/en/US/docs/internetworking/technology/handbook/Token-Ring.html (posted February 20, 2002; accessed November 29, 2008).
- Cisco Systems, Inc. 2006. Fiber distributed data interface, Available at www.cisco.com/en/US/docs/internetworking/technology/handbook/FDDI.html (posted October 12, 2006; accessed November 29, 2008).
- Comer, D., and R. Droms. 2003. *Computer networks and internets with internet applications*, 4th ed. Englewood Cliffs, NJ: Prentice-Hall.
- Ethernet Codes master page. (2008. Available at www.mit.edu/~map/Ethernet/ (accessed November 29, 2008).
- Forouzan, Behrouz. 2007. *Data communications and networking*, 4th ed. New York, NY: McGraw-Hill.
- Gast, Matthew. 2005. *802.11 wireless networks: The definitive guide*, 2nd ed. Chapter 15: A peek ahead at 802.11n: MIMO-OFDM) Sebastopol, CA: O'Reilly Media.
- Goldman, J. 2004. *Applied data communications: A business-oriented approach*, 4th ed. Hoboken, NJ: John Wiley & Sons, Inc.
- Guide to Network Cabling Standards (2008). Available at www.siemon.com/us/standards/ (accessed November 29, 2008).
- IEEE 802.3 CSMA/CD (ETHERNET).2008. Available at <http://grouper.ieee.org/groups/802/3/index.html> (accessed November 29, 2008).
- Local area networks. 2008. Available at http://compnetworking.about.com/cs/lanvlanwan/g/bldef_lan.htm (accessed November 29, 2008). New York Times Company.
- Link-layer technologies. 2008. Available at www.cs.columbia.edu/~hgs/internet/ethernet.html (accessed November 29, 2008).
- Metcalf, R., and R. Boggs 1976. Ethernet: Distributed packet switching for local computer networks. *Communications of the ACM* 19(5): 395–404.
- Official Internet Protocol Standards. 2006. Available at www.rfc-editor.org/rfcxx00.html (accessed November 29, 2008).
- Olenewa, J., and M., Ciama 2007. *Wireless# guide to wireless communications*, 2nd ed. Boston, MA: Course Technology.
- Panko, R. 2004. *Corporate computer and network security*. Englewood Cliffs, NJ: Prentice-Hall.
- _____. 2007. *Business data networks and telecommunications*, 6th ed. Prentice-Hall Englewood Cliffs, NJ.
- Pfleeger, C. 2006. *Security in computing*, 4th ed. Englewood Cliffs, NJ: Prentice-Hall.
- Schneier, B. 1999. Crypto-gram newsletter, Available at www.schneier.com/crypto-gram-9912.html (posted December 15, 1999; accessed November 29, 2008).
- Schweizer, D. 2003. *The state of network security*. Processor.com, August 22, 2003.
- Spurgeon, C. 2008. Ethernet web site. Available at www.ethermanage.com/ethernet/ethernet.html (accessed November 29, 2008).
- Stallings, W. 2006. *Data & computer communications*, 8th ed. Englewood Cliffs, NJ: Prentice-Hall.
- Subramanian, M. 2000. *Network management: principles and practice*. Boston, MA: Addison-Wesley.
- Summers, W. 2004. Local area networks in *The internet encyclopedia*, vol. 2, 515–526. Hoboken, NJ: John Wiley & Sons, Inc.
- _____. 2006. Local area networks in *The handbook of information security*, vol. 2, 428–443. Hoboken, NJ: John Wiley & Sons, Inc.
- _____. 2008. Local area networks in *Handbook of computer networks*, vol. 2, 3–18. Hoboken, NJ: John Wiley & Sons, Inc.
- Taylor, E. 2000. *Networking handbook*. New York, NY: McGraw Hill.