chapter 1

Introduction to Networking

After reading this chapter and completing the exercises, you will be able to:

- Identify types of applications and protocols used on a network
- Distinguish between the client-server and peer-to-peer models used to control access to a network
- Describe various networking hardware devices and the most common physical topologies
- Describe the seven layers of the OSI model
- Explore best practices for safety when working with networks and computers
- Describe the seven-step troubleshooting model for solving a networking problem

On the Job

This story is about a client who visited our PC Clinic, a free service offered by our students to the community. Mrs. Jones is an elderly woman who had visited our PC Clinic several times with a variety of PC issues. This visit, she came in with a brand new Dell mini desktop PC.

At home, Mrs. Jones had hooked up all of the cables. Everything worked except her Internet connection. When she called Dell, the technician said she needed a device that cost $40. When it arrived in the mail, she plugged the USB end into her computer. She then tried to plug her phone line into the other end of the device but it didn't fit.

We took a look at the device, or dongle, as a small piece of hardware is sometimes called. It was designed to create an Ethernet connection via USB, with a USB connector on one end and an RJ-45 port on the other. Mrs. Jones's PC also had a wireless card built into the motherboard, but she said that her home network was not wireless.

Next we asked her, "Which Internet service provider do you have?" She said, "I pay AT&T." "Ok, you have a DSL connection with AT&T," we explained. "Do you plug your phone line into the computer?" "No," she said. "When I do that, my phone doesn't work." "Do you have a dial-up service?" "No," she replied. "I use AOL."

Aha! Mrs. Jones had a dial-up service which required an RJ-11 connection, not an RJ-45 connection! And her new desktop PC contained no modem, which is necessary to access dial-up service.

After searching Dell's Web site, we were able to locate an External V.92 56K USB Fax/Modem, a modem that connects to the PC through a USB connection. Mrs. Jones was very grateful, and looking forward to being "connected" again.

June West
Program Director, Computer Technology
Spartanburg Community College

Loosely defined, a **network** is a group of computers and other devices (such as printers) that are connected by some type of transmission media. Variations on the elements of a network and the way it is designed, however, are nearly infinite. A network can be as small as two computers connected by a cable in a home office or the largest network of all, the Internet, made up of millions of computers connected across the world via a combination of cable, phone lines, and wireless links. Networks might link cell phones, personal computers, mainframe computers, printers, plotters, fax machines, and corporate phone systems. They might communicate through copper wires, fiber-optic cable, or radio waves. This chapter introduces you to the fundamentals of networks and how technicians support them.

How Networks Are Used

Network+ 1.6 1.10 5.10

The resources a network makes available to its users include applications and the data provided by these applications. Collectively, these resources are usually referred to as **network services**. Let's quickly survey several types of applications that are typically found on most networks.

Network+ 1.6 5.10

Client-Server Applications

A **client-server application** involves two computers. The first, a client computer, requests data or a service from the second computer, called the server. For example, in Figure 1-1, someone uses a Web browser to request a Web page from a Web server. How does the client know how to make the request in a way the server can understand and respond to? These networked devices use methods and rules for communication known as **protocols**. To handle the request for a Web page, the client computer must first find the Web server. Then, the client and server must agree on the protocols they will use to communicate. Finally, the client makes the request and the server sends its response, in the form of a Web page. Hardware, the operating system, and the applications on both computers are all involved in this process.

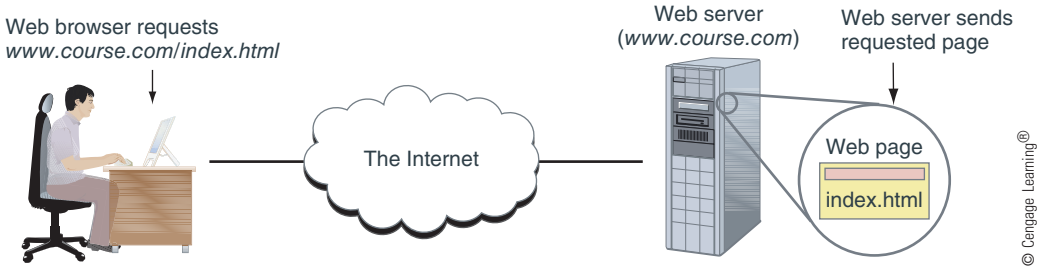


Figure 1-1 A Web browser (client application) requests a Web page from a Web server (server application); the Web server returns the requested data to the client

Here's a brief list of several popular client-server applications used on networks and the Internet:

- *Web service*—A Web server serves up Web pages to clients. Many corporations have their own Web servers, which are available privately on the corporate network. Other Web servers are public, accessible from anywhere on the Internet. The primary protocol used by Web servers and browsers (clients) is **HTTP (Hypertext Transfer Protocol)**. When HTTP is layered on top of an encryption protocol, such as **SSL (Secure Sockets Layer)** or **TLS (Transport Layer Security)**, the result is **HTTPS (HTTP Secure)**, which gives a secure transmission. The most popular Web server application is Apache (see *apache.org*), which primarily runs on UNIX systems, and the second most popular is Internet Information Services (IIS), which is embedded in the Windows Server operating system.

To verify that a Web-based transmission is secure, look for "https" in the URL in the browser address box, as in *https://www.wellsfargo.com*.

- *email services*—Email is a client-server application that involves two servers. The client uses **SMTP (Simple Mail Transfer Protocol)** to send an email message to the first server, which is sometimes called the SMTP server (see Figure 1-2). The first server sends the message on to the receiver's mail server, where it's stored until the recipient requests delivery. The recipient's mail server delivers the message to the receiving client using one of two protocols: **POP3 (Post Office Protocol, version 3)** or **IMAP4 (Internet Message Access Protocol, version 4)**. Using POP3, email is downloaded to the client computer. Using IMAP4, the client application manages the email stored on the server. An example of a

popular email server application is Microsoft Exchange Server. Outlook, an application in the Microsoft Office suite of applications, is a popular email client application.

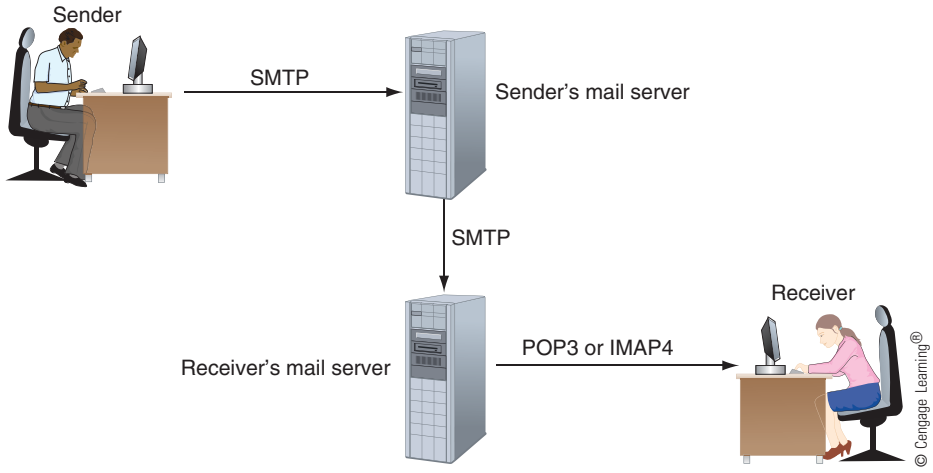


Figure 1-2 SMTP is used to send email to a recipient's email server, and POP3 or IMAP4 is used by the client to receive email

- *FTP service*—FTP is a client-server application that transfers files between two computers, and it primarily uses **FTP (File Transfer Protocol)**. FTP does not provide encryption and is, therefore, not secure. Web browsers can be FTP clients, although dedicated FTP client applications, such as CuteFTP by GlobalSCAPE (*cuteftp.com*), offer more features for file transfer than does a browser.

An encrypted and secure version of FTP is **SFTP (Secure File Transfer Protocol)**. In later chapters, you'll learn to set up an FTP server and client and an SFTP server and client.

- *Telnet service*—The **Telnet** protocol is used by the Telnet client-server command-line application to allow an administrator or other user to "remote in" or control a computer remotely. Telnet is included in many operating systems, but transmissions in Telnet are not encrypted, which has caused Telnet to be largely replaced by other more secure programs, such as the `ssh` command in the Linux operating system.

The `ssh` command in Linux uses the **Secure Shell (SSH)** protocol, which creates a secure channel or tunnel between two computers.

- *Remote Desktop*—In Windows operating systems, the Windows **Remote Desktop** application uses **RDP (Remote Desktop Protocol)** to provide secure, encrypted transmissions that allow a technician to remote in—that is, to access a remote computer from the technician's local computer, as shown in Figure 1-3. For example, when a vendor supports software on

your corporate network, the vendor's support technician at the vendor's site can use Remote Desktop to connect to a computer on your corporate network to troubleshoot problems with the vendor's software. The corporate computer serves up its Windows desktop from which the technician can access any resources on your corporate network. In this situation, the vendor's computer is running Remote Desktop as a client and the corporate computer is running Remote Desktop as a server or host.

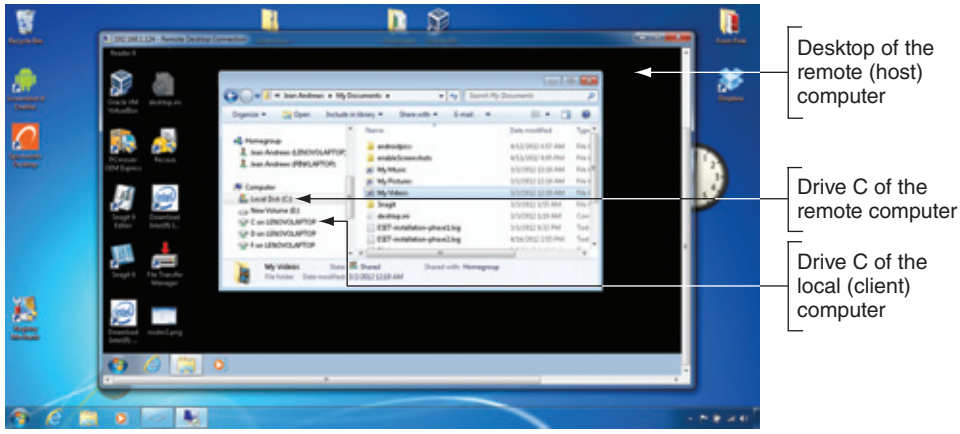


Figure 1-3 Using Remote Desktop, you can access the desktop of the remote computer on your local computer

Source: Microsoft LLC

Because they can be accessed from outside the local network, remote access servers necessitate strict security measures.

- *remote applications*—A **remote application** is an application that is installed and executed on a server and is presented to a user working at a client computer. Windows Server 2008 and later include **Remote Desktop Services** to manage remote applications, and versions of Windows Server prior to 2008 provided **Terminal Services**. Both use RDP to present the remote application and its data to the client. Remote applications are becoming popular because most of the computing power (memory and CPU speed) and technical support (for application installations and updates and for backing up data) are focused on the server in a centralized location, which means the client computers require less computing power and desk-side support.

Network+ 1.6

File and Print Services

The term **file services** refers to a server's ability to share data files and disk storage space. A computer that provides file services is called a **file server**, and serves up data to users, in contrast to users keeping copies of the data on their workstations. Data stored at a central location is typically more secure because a network administrator can take charge of backing up this data, rather than relying on individual users to make their own backups.

Using **print services** to share printers across a network saves time and money. A high-capacity printer can cost thousands of dollars, but can handle the printing tasks of an entire department, thereby eliminating the need to buy a desktop printer for each employee. With one printer, less time is spent on maintenance and management. If a shared printer fails, the network administrator can sometimes diagnose and solve the problem from a workstation anywhere on the network.

Network+ 1.6 1.10

Communications Services

Using the same network to deliver multiple types of communications services, such as video, voice, and fax, is known as **convergence**. A similar term, **unified communications (UC)**, refers to the centralized management of multiple network-based communications. For example, a company might use one software program to manage intraoffice phone calls, long-distance phone calls, cell phone calls, voice mail, faxes, and text messaging for all the users on your network.

Let's consider three types of communication services your network might support and the protocols and models they use:

- *conversational voice*—**VoIP (Voice over IP)** allows two or more people to have voice conversations over a network. VoIP voice is fast replacing traditional telephone service in homes and businesses. For conversational voice, VoIP applications, such as Skype and Google Talk, use a **point-to-point model** rather than a client-server model, which means that each computer involved is independent of the other computers. Additionally, computers engaged in a conference call would use a **point-to-multipoint model**, which involves one transmitter and multiple receivers.
- *streaming live audio and video*—A **video teleconference (VTC)** application, such as Skype or Google Talk, allows people to communicate in video and voice, primarily using the point-to-point model. On the other hand, when you watch a live sports event on your computer, the application is using a client-server model with one server and many clients, called a **multicast distribution**. The Session layer protocol that is specifically designed to transmit audio and video and that works in conjunction with VoIP is **RTP (Real-time Transport Protocol)**.
- *streaming stored audio and video*—When you watch a video on Youtube.com, you're using a client-server model, as the movie stored on the *Youtube.com* server is streamed to your client computer.

Voice and video transmissions are **delay-sensitive**, meaning you don't want to hear breaks in your conversation or see a buffering message when you watch a movie over the Internet. On the other hand, occasional loss of data (skipping video frames, for example) can be tolerated; for that reason, voice and video transmissions are considered **loss-tolerant**. Network administrators must pay attention to the **quality of service (QoS)** a network provides for voice and video.

Network administrators must be aware of the applications used on a network, including the application protocols they use and the amount of bandwidth they require. **Bandwidth**, as the term is used here, means the amount of traffic, or data transmission activity, on the network.

Another important consideration for administrators is the methods used to control access to the network.

Controlling Network Access

Network+ 1.6

A **topology** describes how the parts of a whole work together. When studying networking, you need to understand both the physical topology and the logical topology:

- The term **physical topology**, or network topology, mostly applies to hardware and describes how computers, other devices, and cables fit together to form the physical network.
- The term **logical topology** has to do with software and describes how access to the network is controlled, including how users and programs initially gain access to the network and how specific resources, such as applications and databases, are shared on the network.

In this part of the chapter, you learn about controlling network access. Later in the chapter, you'll learn about the physical topologies.

Controlling how users and programs get access to the resources on a network is a function of the operating systems used on the network. Each operating system (OS) is configured to use one of two models to connect to network resources: the peer-to-peer model or the client-server model. The peer-to-peer model can be achieved using any assortment of desktop, mobile devices, or tablet operating systems, but the client-server model requires one or more **network operating systems (NOSs)**, which controls access to the entire network. Examples of NOSs are Windows Server 2012 R2, Ubuntu Server, and Red Hat (Ubuntu and Red Hat are versions of Linux).

The peer-to-peer model and the client-server model are sometimes referred to as the peer-to-peer topology and the client-server topology. The CompTIA Network+ exam expects you to know how to use the word *topology*.

Peer-to-Peer Network Model

Network+ 1.6

Using a **peer-to-peer (P2P) network model**, the operating system of each computer on the network is responsible for controlling access to its resources without centralized control. The computers, called nodes or hosts on the network, form a logical group of computers and users that share resources (see Figure 1-4). Administration, resources, and security on a computer are controlled by that computer.

When looking at the diagrams in Figure 1-4 and later in Figure 1-5, keep in mind that the connecting lines describe the logical arrangement or topology of the group of computers, as opposed to the physical arrangement. The physical arrangement in both diagrams may be the same, but the model the OSs use to logically connect differs.

Examples of operating systems that might be installed on computers in a peer-to-peer network are Windows 7, Windows 8.1, Linux, and Mac OS X on desktop and laptop computers and iOS, Android, and BlackBerry on mobile devices.

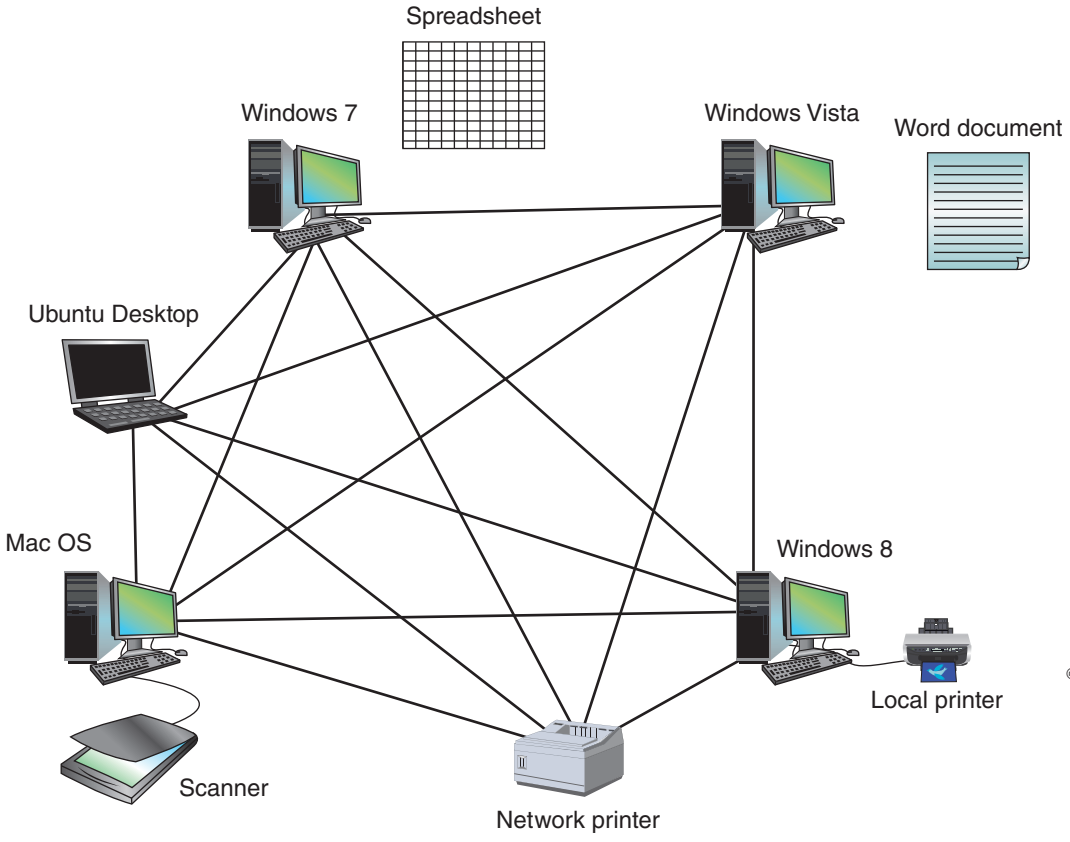


Figure 1-4 In a peer-to-peer network, no computer has more authority than another; each computer controls its own resources, and communicates directly with other computers

If all computers in a peer-to-peer network are running a Windows operating system, each computer user has a Windows **local account** that works only on that one computer. Resources can be shared in these ways:

- Using Windows folder and file sharing, each computer maintains a list of users and their rights on that particular PC. Windows allows a user on the network to access local resources based on these assigned rights.
- Using a homegroup, each computer shares files, folders, libraries, and printers with other computers in the homegroup. A homegroup limits how sharing can be controlled for individual users because any user of any computer in the homegroup can access homegroup resources.

You can also use a combination of folder and file sharing and homegroups on the same network and even using the same computers. That can get confusing, so it's best to stick with one method or the other.

This book assumes you are already aware of the knowledge and skills covered in the CompTIA A+ certification objectives. Using and supporting homegroups and sharing folders and files are part of this content. If you need to learn how homegroups and folder and file sharing are configured and supported, see *CompTIA A+ Guide to Managing and Maintaining Your PC*, by Jean Andrews.

Generally, if the network supports fewer than 15 computers, a peer-to-peer network is the way to go. The following are advantages of using peer-to-peer networks:

- They are simple to configure. For this reason, they may be used in environments in which time or technical expertise is scarce.
- They are often less expensive to set up and maintain than other types of networks. A network operating system, such as Windows Server 2012 R2, is much more expensive than a desktop operating system, such as Windows 8.1 Professional.

The following are disadvantages of using traditional peer-to-peer networks:

- They are not **scalable**, which means, as a peer-to-peer network grows larger, adding or changing significant elements of the network may be difficult.
- They are not necessarily secure—meaning that in simple installations, data and other resources shared by network users can be easily discovered and used by unauthorized people.
- They are not practical for connecting more than a few computers because it becomes too time consuming to manage the resources on the network. For example, suppose you set up a file server with a folder named \SharedDocs and create 12 local accounts on the file server, one for each of 12 users who need access to the folder. Then you must set up the workstations with the same local accounts, and the password to each local account on the workstation must match the password for the matching local account on the file server. It can be an organizational nightmare to keep it all straight! If you need to manage that many users and shared resources, it's probably best to implement Windows Server or another NOS.

Network+ 1.6

Client-Server Network Model

In the **client-server network model** (which is sometimes called the client-server architecture or client-server topology), resources are managed by the NOS via a centralized directory database. The database can be managed by one or more servers, so long as they each have a similar NOS installed (see Figure 1-5).

When Windows Server controls network access to a group of computers, this logical group is called a Windows **domain**. The centralized directory database that contains user account information and security for the entire group of computers is called **Active Directory (AD)**. Each user on the network has his own domain-level account called a **global account**, also called a global username or network ID, which is assigned by the network administrator and is kept in Active Directory. A user can sign on to the network from any computer on the network and get access to the resources that Active Directory allows. The process is managed by **Active Directory Domain Services (AD DS)**.

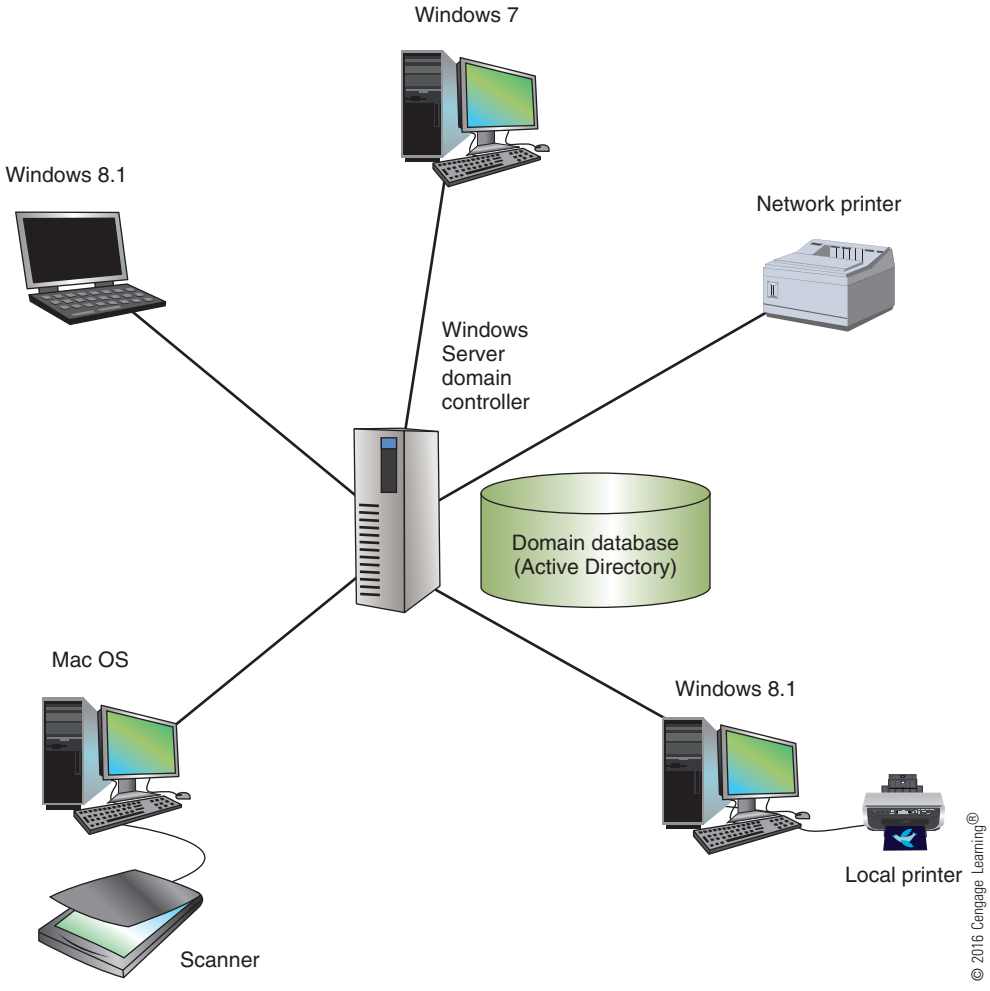


Figure 1-5 A Windows domain uses the client-server model to control access to the network, where security on each computer or device is controlled by a centralized database on a domain controller

Clients on a client-server network can run applications installed on the desktop and store their own data on local storage devices. Clients don't share their resources directly with each other; instead, access is controlled by entries in the centralized domain database. A client computer accesses resources on another computer by way of the servers controlling this database.

In summary, the NOS (for example, Windows Server 2012 R2, Ubuntu Server, or Red Hat Linux) is responsible for:

- Managing data and other resources for a number of clients
- Ensuring that only authorized users access the network
- Controlling which types of files a user can open and read
- Restricting when and from where users can access the network

- Dictating which rules computers will use to communicate
- In some situations, supplying applications and data files to clients

Servers that have a NOS installed require more memory, processing power, and storage capacity than clients because servers are called on to handle heavy processing loads and requests from multiple clients. For example, a server might use a RAID (redundant array of independent disks) configuration of hard drives, so that if one hard drive fails, another hard drive automatically takes its place.

Although client-server networks are typically more complex in their design and maintenance than peer-to-peer networks, they offer many advantages over peer-to-peer networks, including:

- User accounts and passwords to the network are assigned in one place.
- Access to multiple shared resources (such as data files or printers) can be centrally granted to a single user or groups of users.
- Problems on the network can be monitored, diagnosed, and often fixed from one location.
- Client-server networks are also more scalable than peer-to-peer networks. In other words, it's easier to add computers and other devices to a client-server network.

Regardless of the logical topology or the OSs used, the OSs on a network are able to communicate with each other via the protocols they have in common. The two primary protocols are TCP (Transmission Control Protocol) and IP (Internet Protocol) and the suite of all the protocols an OS uses for communication on a network is the **TCP/IP** suite of protocols.

You can think of applications and their data as the payload traveling on a network and the operating systems as the traffic controllers managing the traffic. The road system itself is the hardware on which the traffic flows. Let's now look at the basics of networking hardware and the physical topologies they use.

Networking Hardware and Physical Topologies

Network+ 1.6 1.7

Two computers connected by an ad hoc Wi-Fi connection are technically a network; however, let's start our discussion of networking hardware with the slightly more complex network shown in Figure 1-6. Keep in mind that every host or node on a network needs a network address so that other hosts or nodes can find it.

Notice the two printers in Figure 1-6. A network printer has a network port and connects directly to the switch. A local printer connects directly to a computer on the network.

LANs and Their Hardware

Network+ 1.6

The network in Figure 1-6 is a **local area network (LAN)** because each node on the network can communicate directly with others on the network. LANs are usually contained

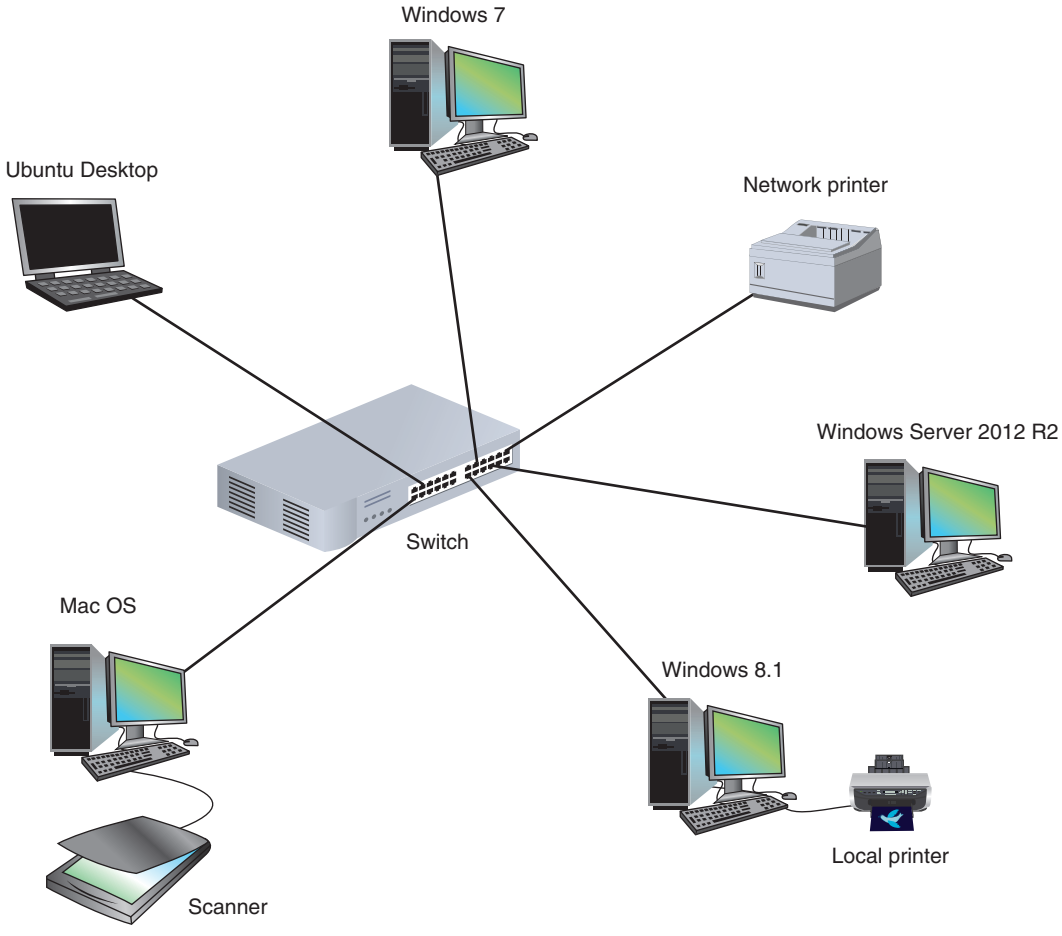
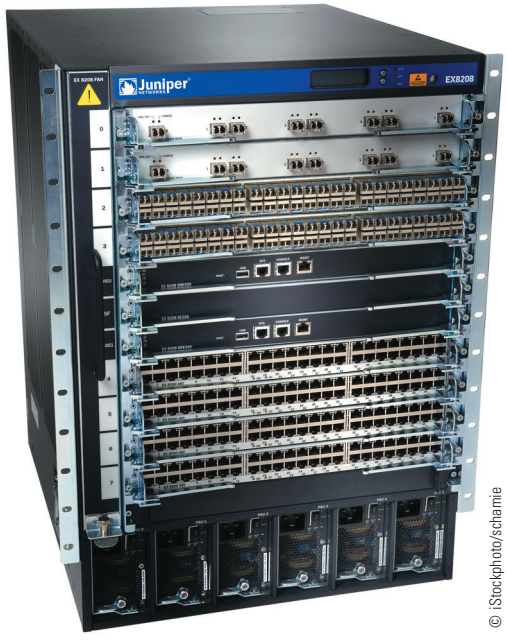


Figure 1-6 This LAN has five computers, a network printer, a local printer, a scanner, and a switch, and is using a star topology

in a small space, such as an office or building. The five computers and a network printer all connect to the switch by way of wired connections. A **switch** (see Figure 1-7) receives incoming data from one of its ports and redirects (switches) it to another port or multiple ports that will send the data to its intended destination(s). The physical topology used by the network is called a **star topology** because all devices connect to one central device, the switch.

Computers, network printers, switches, and other network devices have network ports into which you plug a network cable. A network port can be an **onboard network port** embedded in the computer's motherboard, such as the port on the laptop in Figure 1-8. Another type of port is provided by a **network interface card (NIC)**, also called a **network adapter**, installed in an expansion slot on the motherboard (see Figure 1-9).

A LAN can have several switches. For example, the network in Figure 1-10 has three switches daisy-chained together. The two yellow lines in the figure connecting the three



Courtesy of Juniper Networks, Inc

Figure 1-7 Industrial-grade and consumer-grade switches

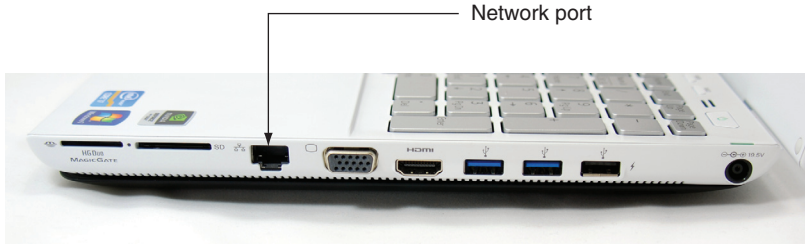


Figure 1-8 A laptop provides an onboard network port to connect to a wired network

switches represent the backbone of this network. A **backbone** is a central conduit that connects the segments (pieces) of a network and is sometimes referred to as "a network of networks." The backbone might use higher transmission speeds and different cabling than network cables connected to computers because of the heavier traffic and the longer distances it might span.

Because the three switches are daisy-chained together in a single line, the network is said to use a **bus topology**. However, each switch is connected to its computers via a star topology. Therefore, the topology of the network in Figure 1-10 is said to be a **star-bus topology**. A topology that combines topologies in this way is known as a **hybrid topology**.

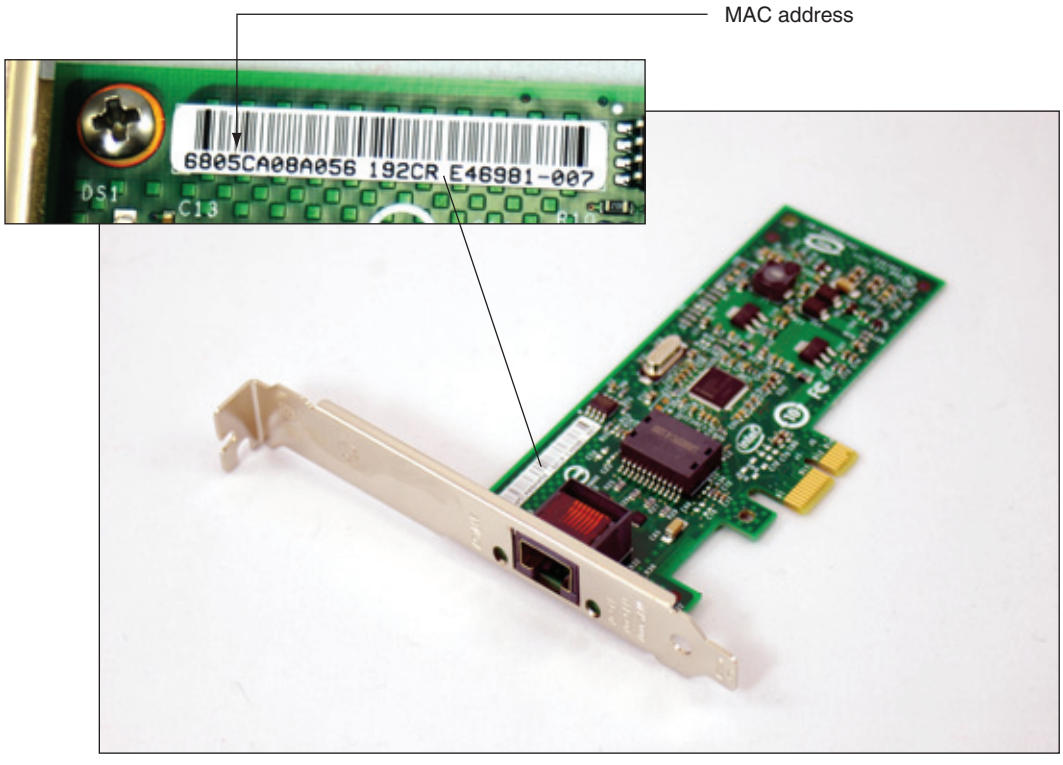


Figure 1-9 This Intel Gigabit Ethernet adapter, also called a network interface card or NIC, uses a PCIe x1 slot on a motherboard

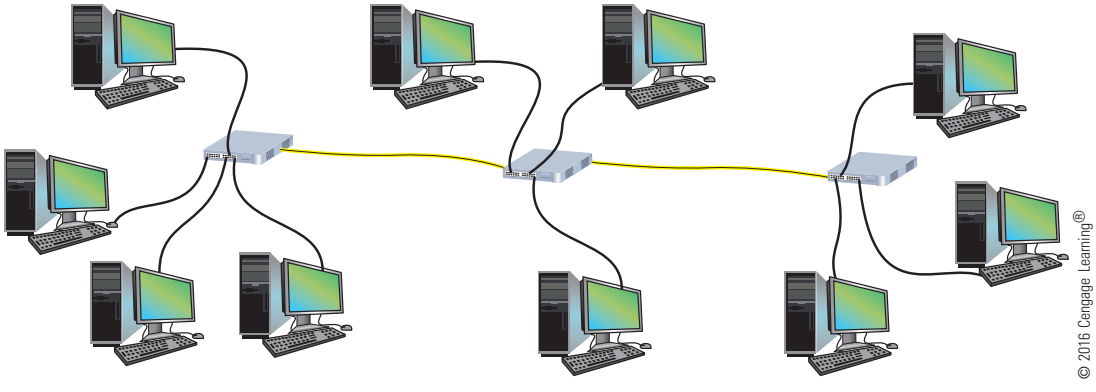


Figure 1-10 This local network has three switches, and is using a star-bus topology

Network+ 1.6

Legacy Networking

Ring Topology

1

In addition to the bus, star, and hybrid topologies, the CompTIA Network+ exam expects you to know about the ring topology, which is seldom used today. In a **ring topology**, nodes are connected in a ring, with one node connecting only to its two neighboring nodes (see Figure 1-11). A node can put data on the ring only when it holds a token, which is a small group of bits passed around the ring. This is similar to saying "I hold the token, so I get to talk now." The ring topology is rarely used today primarily because of its slow speed.

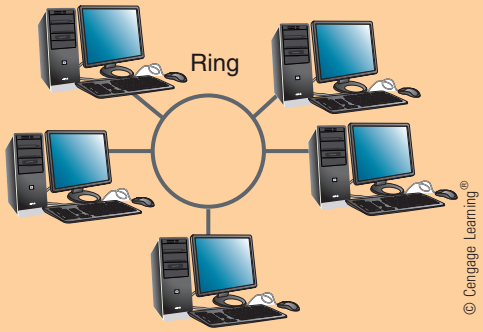


Figure 1-11 Using a ring topology, a computer connects to the two computers adjacent to it in the ring

A LAN needs a way to communicate with other networks, and that's the purpose of a router. A **router** is a device that manages traffic between two or more networks and can help find the best path for traffic to get from one network to another. In small home networks, a consumer-grade router is used to connect the LAN to the Internet (see Figure 1-12a).

A home network might use a combo device, which is both a router and a switch, and perhaps a wireless access point that creates a Wi-Fi hot spot. For example, the device may provide three network ports and a Wi-Fi hot spot that are part of the local network and one network port to connect to the Internet service provider (ISP) and on to the Internet. In this situation (see Figure 1-12b), the three ports are provided by a switch embedded in the device. The home router belongs to the home's local network and the ISP's local network. Don't confuse this combo device with an industrial-grade router in which each port connects to a different LAN.

Industrial-grade routers can have several network ports, one for each of the networks it connects to. In that case, the router belongs to each of these networks. For example, in Figure 1-13, the router connects three LANs and has a network address that belongs to Network A, another network address that belongs to Network B, and a third network address for Network C.

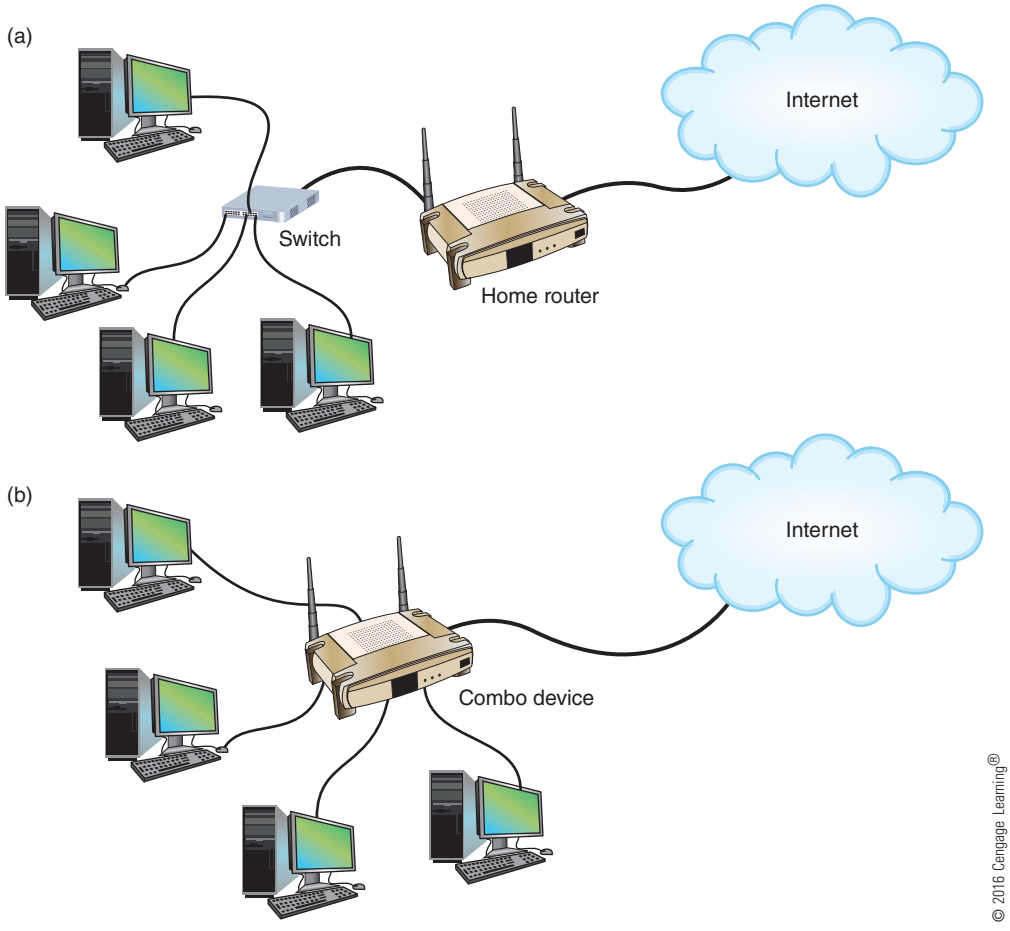


Figure 1-12 (a) A router stands between the LAN and the Internet, connecting the two networks; (b) home networks often use a combo device that works as both a switch and a router

The fundamental difference between a switch and a router is that a switch belongs only to its local network and a router belongs to two or more local networks. Recall that nodes on a local network communicate directly with one another. However, a host on one LAN cannot communicate with a host on another LAN without a router to manage that communication and stand as a gateway between the networks.

Let's make the distinction now between the two terms, *host* and *node*. A **host** is any computer on a network that hosts a resource such as an application or data, and a **node** is any computer or device on a network that can be addressed on the local network. A client computer or server is both a node and a host, but a router or switch does not normally host resources and is, therefore, merely a node on the network.

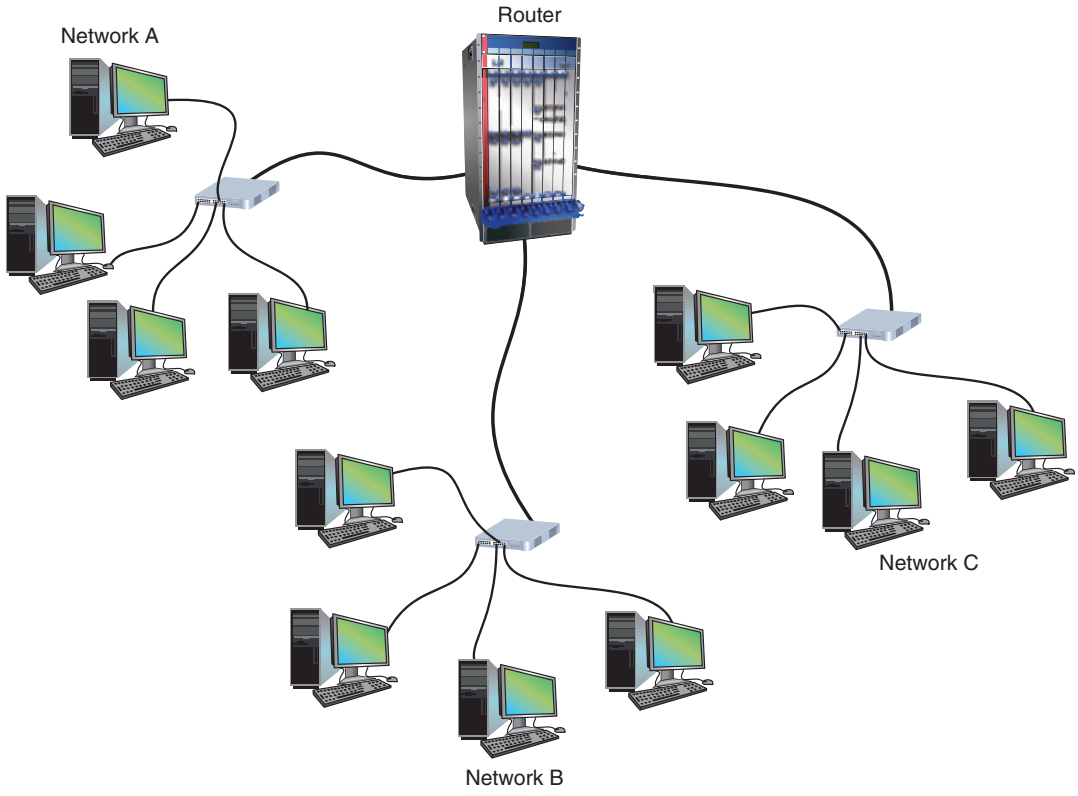


Figure 1-13 Three LANs connected by a router

As you might have already guessed, networked hardware devices such as NICs, switches, and routers can communicate with each other because of the protocols they have in common. In Chapters 3 and 4, you'll learn about the protocols used by NICs, switches, and routers.

Network+ 1.7

MANs and WANs

A group of connected LANs in the same geographical area—for example, a handful of government offices surrounding a state capitol building—is known as a **MAN (metropolitan area network)** or **CAN (campus area network)**. A group of LANs that spread over a wide geographical area is called a **WAN (wide area network)**. MANs and WANs often use different transmission methods and media than LANs. The Internet is the largest and most varied WAN in the world. The smallest network is a **PAN (personal area network)**, which is a network of personal devices, such as the network you use when you sync your cell phone and your computer.

Figure 1-14 shows a WAN link between two local networks bound by routers. For example, a corporation might have an office in San Francisco and another in Philadelphia. Each office has a LAN, and a WAN link connects the two LANs. The WAN link is most likely provided by a third-party service provider.

You've just learned how applications, operating systems, and hardware create, manage, and use a network. Now let's see, from a bird's-eye view, how they all work together.

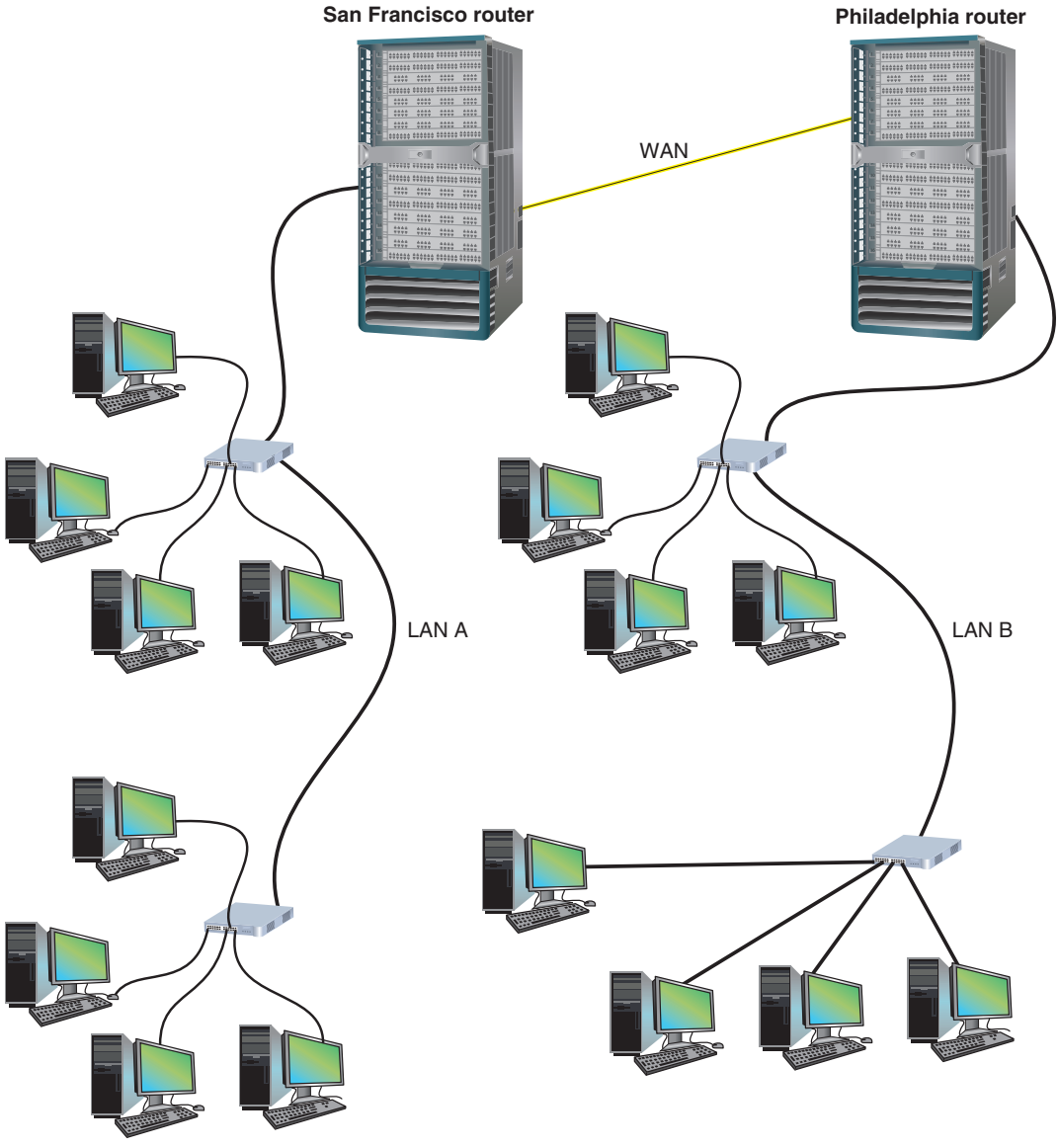


Figure 1-14 A WAN connects two LANs in different geographical areas

The Seven-Layer OSI Model

Network+ 2.5 5.1 5.2 5.9

Recall that an application, such as a browser, depends on the operating system to communicate across the network. Operating systems, meanwhile, depend on hardware to communicate across the network (see the left side of Figure 1-15). Throughout the entire process, protocols govern each layer of communication.

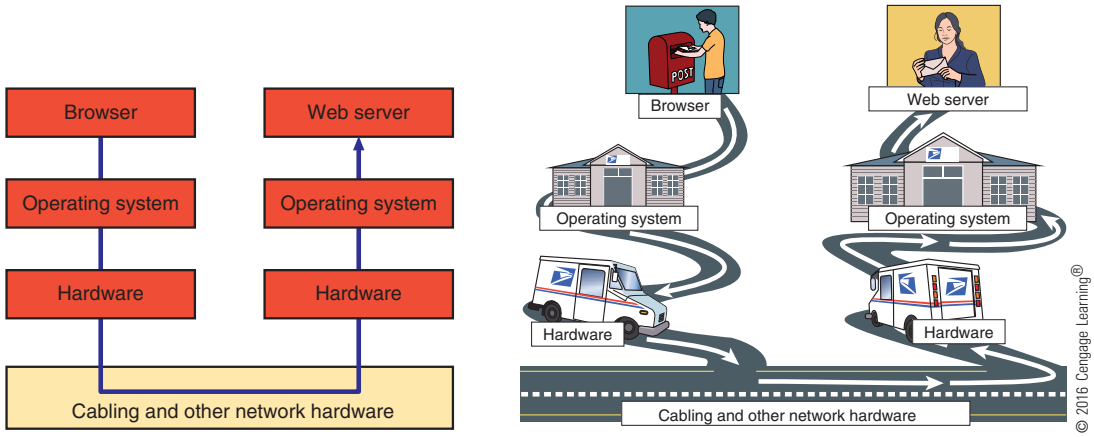


Figure 1-15 A browser and Web server communicate by way of the operating system and hardware, similar to the way a letter is sent through the mail using the U.S. Postal Service and the road system

To get a better sense of how this works, it's helpful to think of a different type of communication: two people communicating by way of the U.S. Postal Service (see the right side of Figure 1-15). The sender depends on the mailbox to hold her letter until a postal worker picks it up and takes it to the post office. The people at the post office, in turn, depend on truck drivers to transport the letter to the correct city. The truck drivers, for their part, depend on the road system. Throughout the entire process, various protocols govern how people behave. For example, the sender follows basic rules for writing business letters, the mail carriers follow U.S. Postal Service regulations for processing the mail, and the truck drivers follow traffic laws. Think of how complex it might be to explain to someone all the different rules or protocols involved if you were not able to separate or categorize these activities into layers.

Early in the evolution of networking, a seven-layer model was developed to categorize the layers of communication. This model, which is called the **OSI (Open Systems Interconnection) reference model**, is illustrated on the left side of Figure 1-16. It was first developed by the International Organization for Standardization, also called the ISO. (Its shortened name, *ISO*, is derived from a Greek word meaning *equal*.) Network engineers, hardware technicians, programmers, and network administrators still use the layers of the OSI model to communicate about networking technologies. In this book, you'll learn to use the OSI model to help you understand networking protocols and troubleshoot network problems.

The CompTIA Network+ exam expects you to know how to apply the OSI model when troubleshooting network problems.

As you study various protocols used in networking, it will help tremendously to map each protocol onto the OSI model. By doing so, you'll better understand the logistics of which

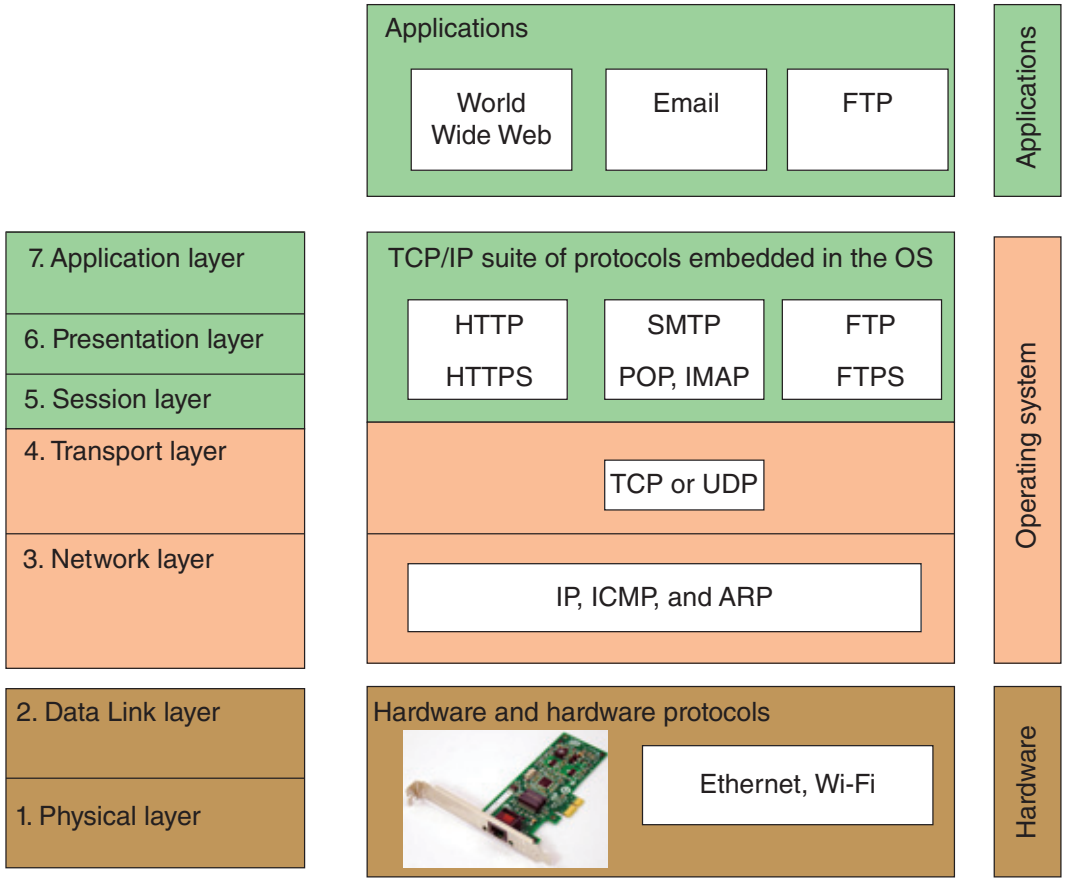


Figure 1-16 How software, protocols, and hardware map to the seven-layer OSI model

software program or device is initiating and/or receiving the protocol or data and how other protocols are relating to it.

Now let's take a brief look at each layer in the OSI model. The layers are numbered in descending order, starting with Layer 7, the Application layer, at the top. Figure 1-16 guides you through the layers.

You need to memorize the seven layers of the OSI model. Here's a seven-word mnemonic that can help: All People Seem To Need Data Processing.

Network+ 5.1 5.2

7 APPLICATION
6 PRESENTATION
5 SESSION
4 TRANSPORT
3 NETWORK
2 DATA LINK
1 PHYSICAL

Layer 7: Application Layer

The **Application layer** in the OSI model describes the interface between two applications, each on separate computers. Earlier in this chapter, you learned about several protocols used at this layer, including HTTP, SMTP, POP3, IMAP4, FTP, Telnet, and RDP. Application layer protocols are used by programs that fall into two categories:

- Application programs that provide services to a user, such as a browser and Web server using the HTTP Application layer protocol
- Utility programs that provide services to the system, such as SNMP (Simple Network Management Protocol) programs that monitor and gather information about network traffic and can alert network administrators about adverse conditions that need attention

Data that is passed between applications or utility programs and the operating system is called a **payload** and includes control information. The two end-system computers that initiate sending and receiving data are called hosts.

Network+ 5.1 5.2

Layer 6: Presentation Layer

In the OSI model, the **Presentation layer** is responsible for reformatting, compressing, and/or encrypting data in a way that the application on the receiving end can read. For example, an email message can be encrypted at the Presentation layer by the email client or by the operating system.

Network+ 5.1 5.2

Layer 5: Session Layer

The **Session layer** of the OSI model describes how data between applications is synced and recovered if messages don't arrive intact at the receiving application. For example, the Skype application works with the operating system to establish and maintain a session between two end points for as long as a voice conversation or video conference is in progress.

The Application, Presentation, and Session layers are so intertwined that, in practice, it's often difficult to distinguish between them. Also, tasks for each layer may be performed by the operating system or the application. Most tasks are performed by the OS when an application makes an API call to the OS. In general, an **API (application programming interface) call** is the method an application uses when it makes a request of the OS.

Network+ 5.1 5.2 5.9

Layer 4: Transport Layer

The **Transport layer** is responsible for transporting Application layer payloads from one application to another. The two main Transport layer protocols are TCP, which guarantees delivery, and UDP, which does not:

- ***TCP (Transmission Control Protocol)***—Makes a connection with the end host, checks whether the data is received, and resends it if it is not. TCP is, therefore, called a **connection-oriented protocol**. TCP is used by applications such as Web browsers and email. Guaranteed delivery takes longer and is used when it is important to know that the data reached its destination.
- ***UDP (User Datagram Protocol)***—Does not guarantee delivery by first connecting and checking whether data is received; thus, UDP is called a **connectionless protocol** or **best-effort protocol**. UDP is used for broadcasting, such as streaming video or audio over the Web, where guaranteed delivery is not as important as fast transmission. UDP is also used to monitor network traffic.

The protocols add their own control information in an area at the beginning of the payload called the **header** to create a message ready to be transmitted to the Network layer. The process of adding a header to the data inherited from the layer above is called **encapsulation**. The Transport layer header addresses the receiving application by a number called a **port number**. If the message is too large to transport on the network, TCP divides it into smaller messages called **segments**. In UDP, the message is called a **datagram**.

In our Post Office analogy, you can think of a message as a letter. The sender puts the letter in an envelope and adds the name of the sender and receiver, similar to how the Transport layer encapsulates the payload into a segment or datagram that identifies both the sending and destination applications.

Network+ 5.1 5.2

Layer 3: Network Layer

7 APPLICATION
6 PRESENTATION
5 SESSION
4 TRANSPORT
3 NETWORK
2 DATA LINK
1 PHYSICAL

The **Network layer**, sometimes called the Internet layer, is responsible for moving messages from one node to another until they reach the destination host. The principal protocol used by the Network layer is **IP (Internet Protocol)**. IP adds its own Network layer header to the segment or datagram, and the entire Network layer message is now called a **packet**. The Network layer header identifies the sending and receiving hosts by their IP addresses. An **IP address** is an address assigned to each node on a network, which the Network layer uses to uniquely identify them on the network. In our Post Office analogy, the Network layer would be the trucking system used by the Post Office and the IP addresses would be the full return and destination addresses written on the envelope.

IP relies on several routing protocols to find the best route for a packet when traversing several networks on its way to its destination. These routing protocols include **ICMP (Internet Control Message Protocol)** and **ARP (Address Resolution Protocol)**.

Along the way, if a Network layer protocol is aware that a packet is larger than the maximum size for its network, it will divide the packet into smaller packets in a process called **fragmentation**.

Network+ 2.5 5.1 5.2

Layer 2: Data Link Layer

7 APPLICATION
6 PRESENTATION
5 SESSION
4 TRANSPORT
3 NETWORK
2 DATA LINK
1 PHYSICAL

Layers 2 and 1 are responsible for interfacing with the physical hardware only on the local network. The protocols at these layers are programmed into the firmware of a computer's NIC and other networking hardware. Layer 2, the **Data Link layer**, is more commonly called the **Link layer**. The type of networking hardware or technology used on a network determines the Link layer protocol used. Examples of Link layer protocols are Ethernet and Wi-Fi. (Ethernet works on wired networks and Wi-Fi is wireless.) As you'll learn in later chapters, several types of switches exist. The least intelligent (nonprogrammable) switches, which are called **Link layer switches** or **Layer 2 switches**, operate at this layer.

The term *firmware* refers to programs embedded into hardware devices and that do not change unless a firmware upgrade is performed.

The Link layer puts its own control information in a Link layer header and also attaches control information to the end of the packet in a **trailer**. The entire Link layer message is then called a **frame**. The frame header contains the hardware addresses of the source and destination NICs. This address is called a **MAC (Media Access Control) address**, **physical address**, **hardware address**, or **Data Link layer address** and is embedded on every network adapter on the globe (refer back to Figure 1-9). The physical addresses are short-range addresses that can only find nodes on the local network.

In our Post Office analogy, a truck might travel from one post office to the next en route to its final destination. The address of a post office along the route would be similar to the physical address of a NIC that a frame reaches as it traverses only one LAN on its way to its destination.

Network+ 5.1 5.2

Layer 1: Physical Layer

7 APPLICATION
6 PRESENTATION
5 SESSION
4 TRANSPORT
3 NETWORK
2 DATA LINK
1 PHYSICAL

Layer 1, the **Physical layer**, is the simplest layer of all and is responsible only for sending bits via a wired or wireless transmission. These bits can be transmitted as wavelengths in the air (for example, Wi-Fi), voltage on a copper wire (for example, Ethernet with twisted-pair cabling), or light (for example, Ethernet with fiber-optic cabling).

It's interesting to consider that the top layers of the OSI model work the same for both wired and wireless transmissions. In fact, the only layers that must deal with the details of wired versus wireless transmissions are the Link layer and Physical layer on the firmware of the NIC. Finally, in our Post Office analogy, the Link layer and Physical layer compare with the various road systems a truck might use, each with its own speed limits and traffic rules.

Network+ 5.1 5.2

Protocol Data Unit or PDU

There are several different names for a group of bits as it moves from one layer to the next and from one LAN to the next. Although technicians loosely call this group of bits a message or a transmission, the technical name is a **protocol data unit (PDU)**. Table 1-1 can help you keep all these names straight.

Memorize the details of Table 1-1. You'll need them for the CompTIA Network+ exam.

Table 1-1 Names for a PDU or message as it moves from one layer to another

OSI model	Name	Extremely technical name
Layer 7, Application layer Layer 6, Presentation layer Layer 5, Session layer	Payload or data	L7PDU
Layer 4, Transport layer	Segment (TCP) or datagram (UDP)	L4PDU
Layer 3, Network layer	Packet	L3PDU
Layer 2, Data Link layer	Frame	L2PDU
Layer 1, Physical layer	Bit	L1PDU

Network+ 5.1 5.2

Summary of How the Layers Work Together

Now let's tie the layers together, as shown in Figure 1-17. This transmission involves a browser and Web server on their respective hosts, a switch, and a router. As you follow the red line from browser to Web server, notice the sending host encapsulates the payload in headers and a trailer before sending it, much like an assistant would place the boss's business letter in an envelope before putting it in the mail.

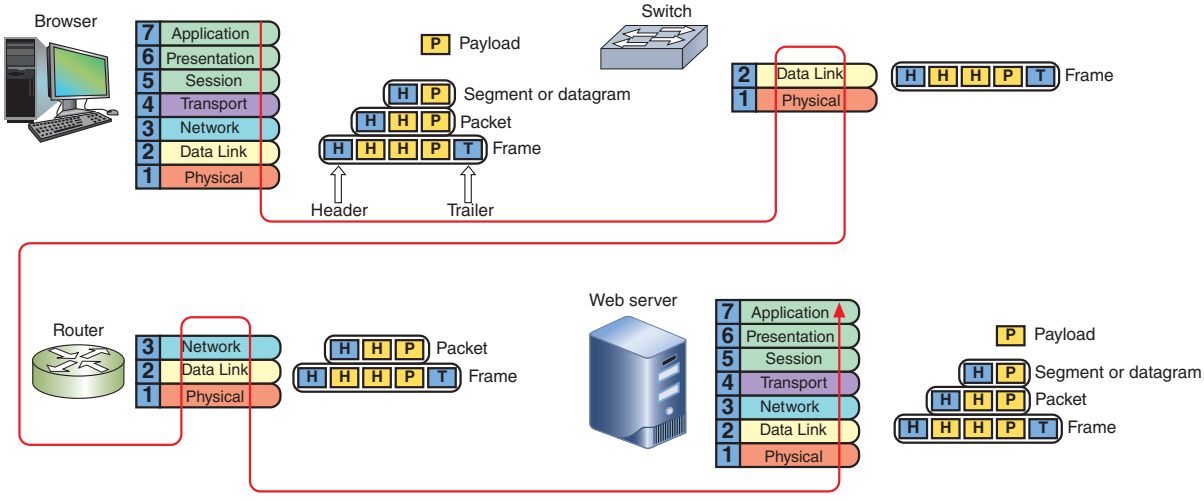


Figure 1-17 Follow the red line to see how the OSI layers work when a browser makes a request to a Web server

In the reverse order, the receiving host removes the headers and trailer before the message reaches the Web server application, just as the receiver's assistant would remove the letter from the envelope before handing it to the receiver. Removing a header and trailer from a layer below is called **decapsulation**.

In conceptual drawings and network maps, symbols are used for switches and routers. In the figure, notice the square symbol representing a switch, and the round symbol, which stands for a router.

The steps listed in Table 1-2 summarize the process illustrated in Figure 1-17.

A four-layer model similar to the OSI model is the TCP/IP model. Using the TCP/IP model, the Application, Presentation, and Session layers are wrapped together and called the Application layer. The Physical layer is so simple, it's ignored, which makes for four layers: Application layer, Transport layer, Internet layer (the Network layer in the OSI model), and Network Interface layer (the Data Link layer in the OSI model).

So now you have the big picture of networking and how it works. Let's turn our attention to staying safe when working around networks and computers.

Table 1-2 Steps through the OSI layers during a browser-to-Web server transmission

Sending host	1. The browser, involving the Application, Presentation, and Session layers, creates an HTTP message or payload on its source computer and passes it down to the Transport layer.
	2. The Transport layer (TCP, which is part of the OS) encapsulates the payload by adding its own header and passes the segment down to the Network layer.
	3. IP at the Network layer in the OS receives the segment (depicted as two yellow boxes in the figure), adds its header, and passes the packet down to the Data Link layer.
	4. The Data Link layer on the NIC firmware receives the packet (depicted as three yellow boxes in the figure), adds its header and trailer, and passes the frame to the Physical layer.
	5. The Physical layer on the NIC hardware puts bits on the network.
Switch	6. The network transmission is received by a Data Link layer switch, which passes the frame up to the Data Link layer (firmware on the switch), which looks at the destination MAC address to decide where to send the frame.
	7. The pass-through frame is sent to the correct port on the switch and on to the router.
Router	8. The router has two NICs, one for each of the two networks to which it belongs. The Physical layer of the first NIC receives the frame and passes it up to the Data Link layer (NIC firmware), which removes the frame header and trailer and passes the packet up to IP at the Network layer (firmware program or other software) on the router.
	9. This Network layer IP program looks at the destination IP address and determines the next node en route for the packet and passes the packet back down to the Data Link layer on the second NIC. The Data Link layer adds a new frame header and trailer appropriate for this second NIC's LAN, including the MAC address of the next destination node. It passes the frame to its Physical layer (NIC hardware), which sends the bits on their way.
Destination host	10. When the frame reaches the destination host NIC, the Data Link layer NIC firmware receives it, removes the frame header and trailer, and passes the packet up to IP at the Network layer, which removes its header and passes the segment up to TCP at the Transport layer.
	11. TCP removes its header and passes the payload up to HTTP at the Application layer. HTTP presents the message to the Web server.

Staying Safe When Working with Networks and Computers

Network+ 5.6

As a network and computer technician, you need to know how to protect yourself and sensitive electronic components as you work. Let's look at some best practices for safety.

Emergency Procedures

Network+ 5.6

In case of an emergency, such as a fire alert, you'll need to know the best escape route or emergency exit for you and others around you. Look in the lobby and hallways at your place of work for a posted building layout and fire escape plan so that you are prepared in an emergency. You also need to be aware of emergency exit doors, which are usually labeled with battery-powered, lighted Exit signs and clearly marked on the posted building layout.

Fire Suppression Systems A company is likely to have a **fire suppression system** in its data center that includes the following:

- ***emergency alert system*** —These systems vary, but they typically generate loud noise and flashing lights. Some send text and voice message alerts to key personnel, and post alerts by email, network messages, and other means.
- *portable fire extinguishers*—Note that electrical fires require a Class C fire extinguisher, as shown in Figure 1-18.
- *emergency power-off switch*—Don't use a power-off switch unless you really need to; improper shutdowns are hard on computers and their data.
- *suppression agent*—This can consist of a foaming chemical, gas, or water that sprays everywhere to put out the fire.

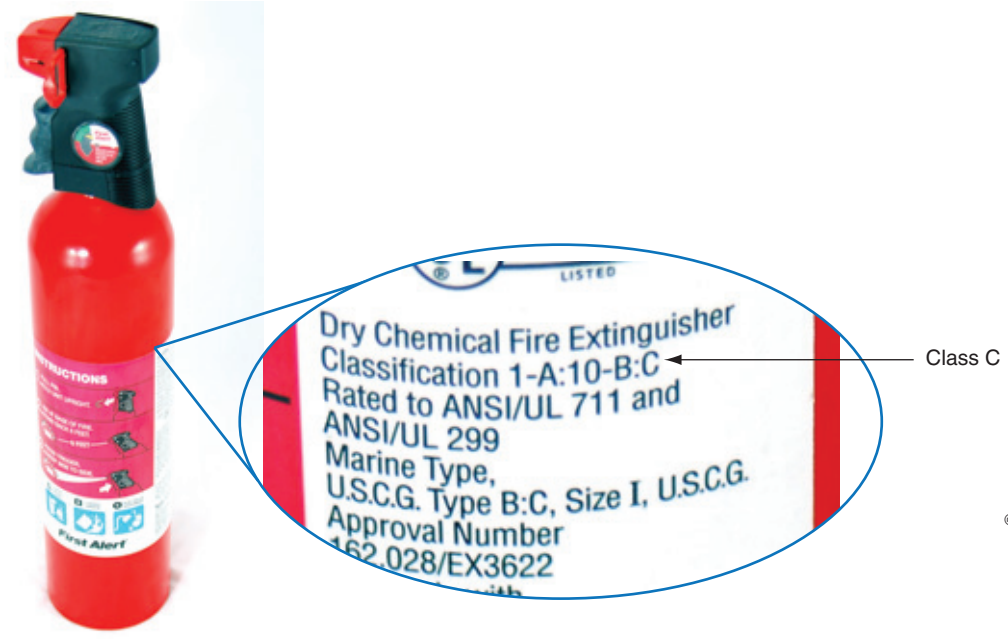


Figure 1-18 A Class C fire extinguisher is rated to put out electrical fires

In the United States, the national Emergency Alert System can only be activated by the president at the national level. It requires TV, radio, cable TV, satellite, and cellular service providers to broadcast the alert. The system can also be used at the state and local level to alert about missing children (AMBER alert) and dangerous weather conditions.

Fail Open or Fail Close What happens to security when a system responsible for security fails? Does the system allow access during the failure (**fail open**) or deny access during the failure (**fail close**)? For example, during a fire alert, using a fail-open policy, all exit

doors stay unlocked so that people can safely leave the building and firefighters can enter the building, even though this might present a security risk for thieves entering the building. On the other hand, if firewall software protecting access to a database of customer credit card numbers fails, it might be configured to fail close and to deny access to the database until the software is back up.

A fail-open policy is often based on common sense so as to ensure that, in an emergency, no one is harmed when a system is not working. A fail-close policy is usually based on the need for security to protect private data or other resources.

The term *open* or *close* takes on the opposite meaning when talking about electrical circuits. When a circuit breaker fails, there is a break in the circuit and the circuit is said to be open. The breaker opens the circuit to protect it from out-of-control electricity. Although this sounds like double-talk, an open circuit is, therefore, a fail-close system.

Material Safety Data Sheet (MSDS) You might need to use cleaning solutions to clean optical discs, tapes and tape drivers, and other devices. Most of these cleaning solutions contain flammable and poisonous materials. Take care when using them so that they don't get on your skin or in your eyes. To find out what to do if you are accidentally exposed to a dangerous solution, look on the instructions printed on the can or check out the material safety data sheet (see Figure 1-19). A **material safety data sheet (MSDS)** explains how to properly handle substances such as chemical solvents and how to dispose of them.

Figure 1-19 Each chemical you use should have a material safety data sheet available

An MSDS includes information such as physical data, toxicity, health effects, first aid, storage, shipping, disposal, and spill procedures. It typically comes packaged with the chemical,

but if you can't locate it, you can order one from the manufacturer, or you can find one on the Web (see *ilpi.com/msds*).

Network+ 5.6

HVAC Systems

The **heating, ventilation, and air conditioning (HVAC) system** controls the environment in a data center, including the temperature, humidity, airflow, and air filtering. The HVAC system must provide acceptable temperature and humidity ranges for devices that might overheat or fail due to high humidity. HVAC systems and network cabling often occupy the space above the ceiling or below the floor in a data center; this space is called the **plenum**. For older buildings that don't have structured plenums, the data center might instead have a raised floor.

It's important that the HVAC system and fire suppression system are compatible. For example, the fluid used in the HVAC system should not be a type that can trigger a false alert by the fire suppression system if the fluid leaks.

Network+ 5.6

Protecting Against Static Electricity

Computer components are grounded inside a computer case, and computer power cables all use a three-prong plug for this purpose. The third prong is grounded. **Grounding** means that a device is connected directly to the earth, so that, in the event of a short, the electricity flows into the earth, rather than out of control through the device and back to the power station, which can cause an electrical fire.

In addition, sensitive electronic components (for example, a NIC, motherboard, and memory modules) can be damaged by **electrostatic discharge (ESD)**, commonly known as **static electricity**. Static electricity is an electrical charge at rest. When your body and a component have different static charges and you touch the component, you can discharge up to 1500 volts of static electricity without seeing a spark or feeling the discharge. However, it only takes 10 volts to damage the component.

Static electricity can cause two types of damage in an electronic component: catastrophic failure and upset failure. A **catastrophic failure** destroys the component beyond use. An **upset failure** can shorten the life of a component and/or cause intermittent errors. Before touching a component, first ground yourself using one of these methods:

- Wear an ESD strap around your wrist that clips onto the chassis or computer case, which eliminates any ESD between you and the chassis and its components (see Figure 1-20).
- If you don't have an ESD strap handy, be sure to at least touch the case before you touch any component inside the case. This is not as effective as wearing an ESD strap, but can reduce the risk of ESD.
- To protect a sensitive component, always store it inside an antistatic bag when it's not in use.

In addition to protecting against ESD, always shut down and unplug a computer before working inside it.

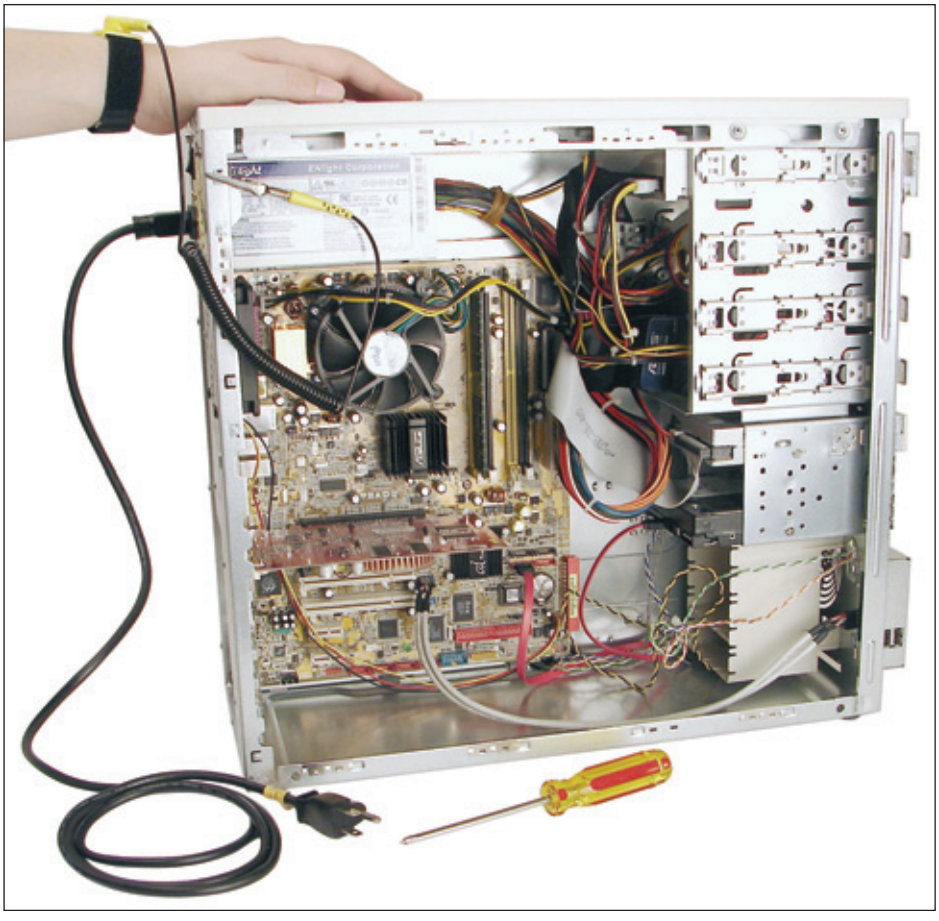


Figure 1-20 An ESD strap, which protects computer components from ESD, can clip to the side of the computer chassis and eliminate ESD between you and the chassis

Network+ 5.6

Installation Safety

When installing equipment, you need to pay special attention to protecting yourself and the equipment.

Lifting Heavy Objects Back injury, caused by lifting heavy objects, is one of the most common injuries that happen at work. Whenever possible, put heavy objects, such as a large laser printer, on a cart to move them. If you do need to lift a heavy object, follow these guidelines to keep from injuring your back:

1. Decide which side of the object to face so that the load is the most balanced.
2. Stand close to the object with your feet apart.
3. Keeping your back straight, bend your knees and grip the load.
4. Lift with your legs, arms, and shoulders, and not with your back or stomach.
5. Keep the load close to your body and avoid twisting your body while you're holding it.

6. To put the object down, keep your back as straight as you can and lower the object by bending your knees.

Don't try to lift an object that is too heavy for you. Because there are no exact guidelines for when heavy is too heavy, use your best judgment as to when to ask for help.

Rack Installations Switches, routers, servers, and **patch panels** (a panel, such as the one shown in Figure 1-21, where cables converge in one location) can be installed in a data center in **racks**, which can be open all around or enclosed in cabinets (see Figure 1-22). When selecting racks and installing devices in racks, it's important to follow the device manufacturer's guidelines for the requirements for the rack and the directions for installation.

Figure 1-21 This patch panel can be installed in a rack and is used where cables converge. Courtesy of Siemon

© iStockphoto/alacatr

© Sashkin/Shutterstock.com

Figure 1-22 Open racks on the left and an enclosed cabinet on the right

Here are some general directions for safely installing rack-mountable devices, such as a rack-mountable server, router, or switch:

- Some racks have wheels. Before you begin the installation, engage the brakes on the rack wheels so the rack doesn't roll.
- To protect against ESD, be sure to wear an ESD strap during the installation.
- Place the device in the rack for good airflow to help keep it cool. It's best for the front of a device to face the colder aisle in the data center. Also, keep in mind that you must be able to access the device from the front and the rear.
- The device must be well grounded, following the manufacturer's directions.
- Pay attention to your tools as you work so they don't accidentally fall into a rack of expensive equipment. For example, remove that little screwdriver from your shirt pocket.
- Some rack-mountable devices that generate a lot of heat have fan trays that install in the rack slot under the device to provide extra airflow. Be sure to install the fan tray oriented in the rack so that air flows in the same direction as the fans inside the device, which are part of the device's power supply.

Figure 1-23 shows one step in the installation: attaching brackets and sliders to the side of the device before sliding it into the rack. After an industrial-grade switch or router has been installed in a rack, the next steps are to use network cables to connect it to the network, power it up, and configure it. Most often, you can configure the device by using a computer on the network to access a utility program in the device's firmware. In Chapter 10, you'll learn how to configure an industrial-grade switch. Configuring and programming routers is beyond the scope of this book.

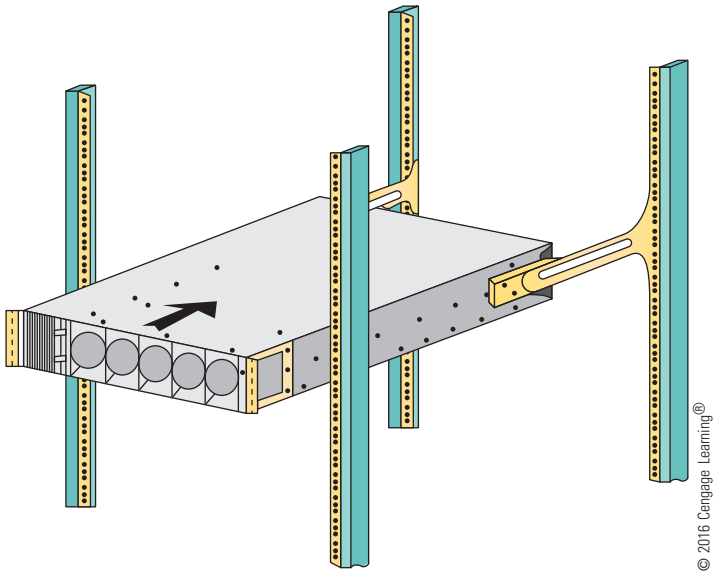


Figure 1-23 This switch uses brackets and sliders to install in a rack

Network+ 5.6

Electrical and Tool Safety in Data Centers

Electrical and tool safety in workplaces is generally regulated by **OSHA (Occupational Safety and Health Administration)**, which is the main federal agency charged with safety and health in the workplace. See *osha.gov*.

OSHA regulations for electrical safety require that electrical devices be turned off and the electrical supply locked out before employees work near these devices. For example, OSHA requires that all devices in a data center cabinet, rack, or panel be turned off and the power locked out before employees work inside of or with these units.

Following are some general OSHA guidelines when using power (electric) tools or other hand tools in the workplace. Your employer can give you more details specific to your work environment:

- Wear **personal protective equipment (PPE)** to protect yourself as you work. For example, wear eye protection where dust or fumes are generated by power tools.
- Keep all tools in good condition and properly store tools not in use. Examine a tool for damage before you use it.
- Use the right tool for the job and operate the tool according to the manufacturer's instructions and guidelines. Don't work with a tool unless you are trained and authorized to use it.
- Watch out for **trip hazards**, so you and others don't stumble on a tool or cord. For example, keep power tool electrical extension cords out from underfoot, and don't leave hand tools lying around unattended.

Troubleshooting Network Problems

Network+ 4.1

As a network technician, you'll be called on to troubleshoot problems with networking hardware, operating systems, applications that use the network, and other network resources. The flowchart in Figure 1-24 illustrates the method used by most expert networking troubleshooters to solve networking problems.

Here are the steps:

Step 1: Identify the problem and its symptoms—As you gather information about the problem, begin by identifying the symptoms, questioning the user, finding out what has recently changed, and determining the scope of the problem. If possible, duplicate the problem. For multiple problems, approach each problem individually. Solve it before moving on to the next.

Step 2: Establish a theory of probable cause—As you observe the extent of the problem, make your best guess as to the source of the problem. Troubleshooters generally follow the bottom-to-top OSI model by first suspecting and eliminating hardware (for example, a loose cable or failed NIC), before moving on to software as the cause of a problem. As you question the obvious and check simple things first, such as a loose network cable, you might solve the problem right on the spot.

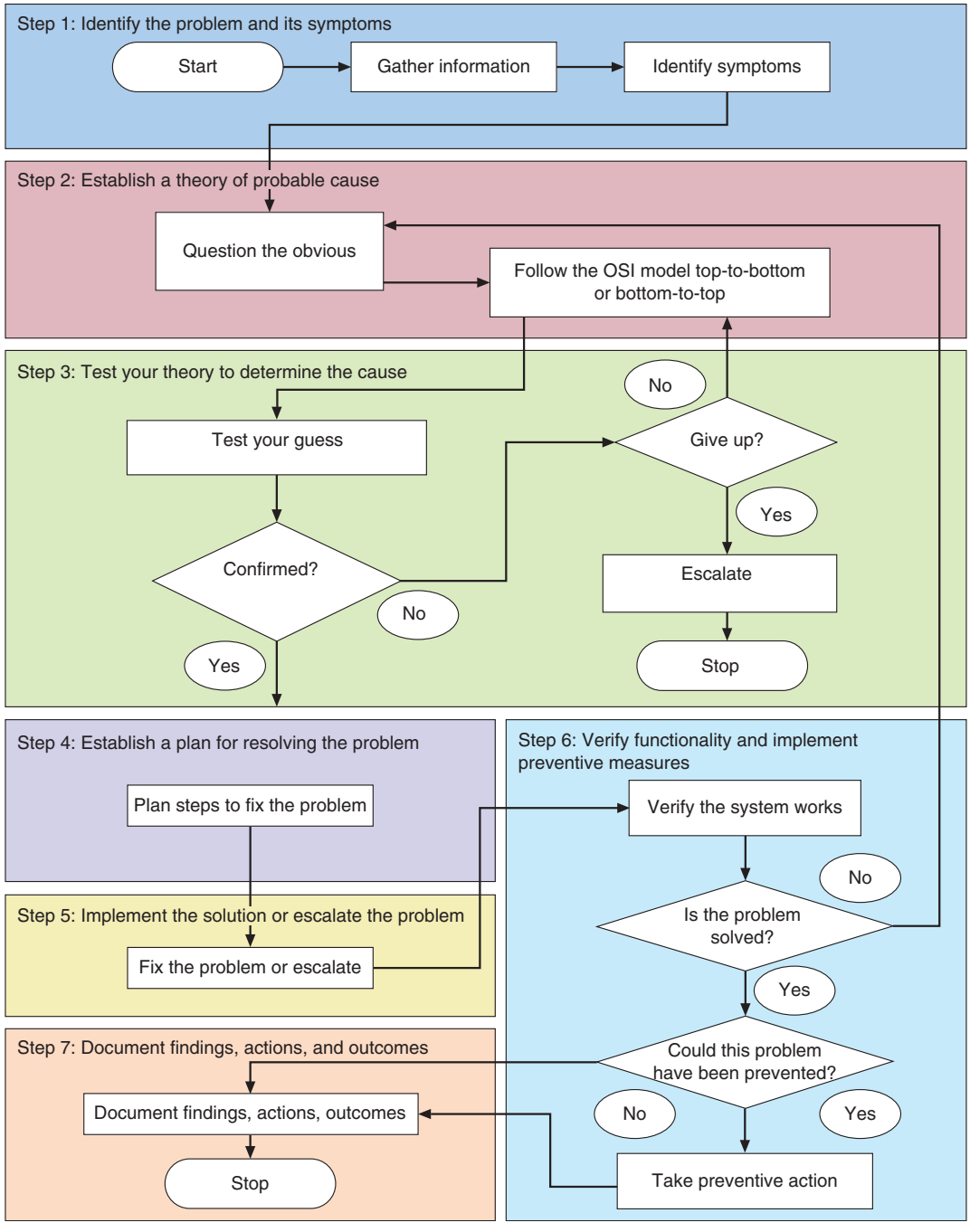


Figure 1-24 General approach to solving network problems

Some situations are obviously software related, such as when a user cannot log on to the network and gets an invalid password message. Here, it makes more sense to follow the top-to-bottom OSI model, beginning at the Application layer, and suspect the user has forgotten his or her password.

As you work, use a divide-and-conquer approach by eliminating parts of the whole until you zero in on the source of the problem.

Step 3: Test your theory to determine the cause—For more complicated or expensive solutions, test your theory to assure yourself that it will indeed solve the problem before you implement the solution. If your test proves your theory is wrong, move on to another guess or escalate the problem to the next tier of support in your organization.

As with any computer-related troubleshooting, be sure you choose the least invasive and least expensive solution first before moving on to more drastic or expensive changes to a computer or the network.

Step 4: Establish a plan for resolving the problem—Changes to a network have the potential for disrupting a lot of people's work. Before you implement a fix, consider the scope of your change, especially how it will affect users, their applications, and their data. Unless the problem poses an emergency, make your changes when the least number of users are on the network.

Step 5: Implement the solution or escalate the problem—Before you make the change, be sure to alert all affected users in advance, create backups of software and data as needed, and save or write down current settings before you change them. Keep good notes as you work, so you can backtrack as necessary. Test your solution thoroughly, and clean up after yourself when you're done. For major changes, it's often best to roll out changes in stages so as to make sure all is working for a few users before you affect many users.

For complex problems, you might need to escalate the problem to someone with access to more technical resources or with more authority to test or implement a solution. An organization might require that major changes to a network be documented in a change management system. You learn about these systems in Chapter 12.

Step 6: Verify functionality and implement preventive measures—At the time you implement your solution, you'll test the system for full system functionality. It's also a good idea to return a few days later and make sure all is working as you expected. Also consider what you can do to make sure the problem doesn't reappear. For example, is more preventive maintenance required? Do you need to implement network monitoring software?

Step 7: Document findings, actions, and outcomes—Most organizations use a **call tracking system** (also called help desk software) to document problems and their resolutions. Your organization is likely to expect you to document the name,

department, and contact information of the person who originated the call for help; when the call first came in; information about the problem; the symptoms of the problem; the resolution of the problem; the name of the technician who handled the problem; and perhaps the amount of time spent resolving the problem. Your company may also require you to document unique or insightful solutions to problems in your company's knowledge base for you and others to draw from in the future. A **knowledge base** is a collection of accumulated insights and solutions to the problems encountered on a particular network.

Network+ 4.1

Applying Concepts

Troubleshoot a Failed Network Connection

Suppose your computer cannot connect to the Internet. Here's a simple process for troubleshooting this problem that demonstrates all seven steps in the troubleshooting model:

Step 1: *Identify the problem and its symptoms*—You open your browser on your desktop computer and discover you can't reach any Web site and you see an error message on the browser screen. You open Windows Explorer or File Explorer and find that you can't navigate to resources normally available on your local network.

Step 2: *Establish a theory of probable cause*—Because a network technician was working near your desk when you left the evening before, you suspect your network cable might have been left unplugged. In the OSI model, you've started at the bottom by suspecting the problem is hardware related.

Step 3: *Test your theory to determine the cause*—You check the cable and discover it is lying on the floor, not connected to your desktop.

Step 4: *Establish a plan for resolving the problem*—You decide to plug in the network cable. This is a very simple resolution that does not affect other users. In other situations, your plan might involve informing coworkers of what is about to happen.

Step 5: *Implement the solution or escalate the problem*—You plug in the cable.

Step 6: *Verify functionality and implement preventive measures*—You open your browser and find you can surf the Web. You verify local network resources are available from Windows Explorer or File Explorer.

Step 7: *Document findings, actions, and outcomes*—This simple problem and solution doesn't require documentation. However, network technicians are generally expected to document troubleshooting tasks and solutions.

In almost every chapter in this book, you'll build your network troubleshooting skills. Many times, the resolution of a problem boils down to the question of where your company's network begins and ends. For most situations, the **demarcation point** (or **demarc**) is the device that marks where a telecommunications service provider's network ends and the organization's network begins. For example, an Internet service provider might be responsible for fiber-optic cable to your building to connect to your LAN. The device where the WAN ends and the LAN begins is the demarc. The service provider is responsible for its network beyond the demarc.

Chapter Summary

How Networks Are Used

- Networks provide a wide range of network services, including client-server applications, such as Web services, email services, FTP services, Telnet services, Remote Desktop, remote applications, file and print services, and communication services, such as conversational voice and streaming audio and video.
- Web servers and browsers primarily use HTTP and HTTPS for communication. Email services primarily use SMTP, POP3, and IMAP4 for communication. FTP services use the FTP protocol, and Telnet uses the Telnet protocol. Remote Desktop and Windows Remote Applications use the RDP protocol.
- File and print services enable multiple users to share data, storage areas, and printers.
- Streaming voice and video can use a point-to-point communication model or a multicast distribution model. The RTP protocol is used with multicast distribution. Video and voice is delay-sensitive and loss-tolerant.

Controlling Network Access

- The peer-to-peer model for controlling access to a network allows every computer to share resources directly with every other computer. By default, no computer on a peer-to-peer network has more authority than another. However, each computer can be configured to share only some of its resources, while keeping other resources inaccessible.
- Traditional peer-to-peer networks are usually simple and inexpensive to set up. However, they are not necessarily scalable or secure.
- The client-server model for access control relies on a centrally administered server (or servers) using a network operating system (NOS) that manages shared resources for multiple clients. In a Windows NOS, the group of networked computers is called a domain and the directory database that contains user account information is called Active Directory.
- Client-server networks are more complex and expensive to install than peer-to-peer networks. However, they are more easily managed, more scalable, and typically more secure. They are by far the most popular type of network access control in use today.
- Servers require more processing power, hard disk space, and memory than client computers.

Networking Hardware and Physical Topologies

- A LAN (local area network) is a network of computers and other devices that can directly address all other nodes. A LAN is typically confined to a relatively small space, such as one building or one floor in a large building.
- In a star topology, all computers and network devices connect to one central device, which is likely to be a switch.
- A computer or other device connects to a wired network via a network port and a network cable. The port is provided by a network interface card (NIC) or is an onboard port embedded in the device's motherboard.

- A backbone is a central conduit that connects parts of a network and might use the bus topology, in which devices are daisy-chained together in a single line.
- A star-bus topology is a type of hybrid typology that contains elements of both the star and bus topologies.
- A router manages traffic between two or more LANs and belongs to each network to which it directly connects.
- A MAN is made up of several LANs that cover multiple buildings in the same geographical area.
- LANs can be interconnected to form WANs (wide area networks), which traverse longer distances in two or more geographical areas and may use different transmission methods and media than LANs. The Internet is the largest example of a WAN.

The Seven-Layer OSI Model

- The seven layers of the OSI model are the Application (Layer 7), Presentation (Layer 6), Session (Layer 5), Transport (Layer 4), Network (Layer 3), Data Link (Layer 2), and Physical (Layer 1).
- At Layers 7, 6, and 5, a transmission of data and its control information is known as the payload.
- A message at the Transport layer is called a segment in TCP and a datagram in UDP.
- IP is the primary protocol used at the Network layer, although several routing protocols are also used. An IP transmission is called a packet.
- A message at the Data Link layer is called a frame. The protocol used depends on the technology of the networking hardware, for example, Ethernet or Wi-Fi.
- Some switches operate at the Data Link layer and routers operate at the Network layer.

Staying Safe When Working with Networks and Computers

- Emergency procedures can include designated emergency exits, building layouts, and fire escape plans to help aid people in an emergency alert.
- A fire suppression system can include an emergency alert system, portable fire extinguishers, an emergency power-off switch, and suppression agents.
- To ensure a system's security, it's important to have a fail-open or fail-close policy that determines how security is handled when the system fails.
- A material safety data sheet (MSDS) explains how to properly handle substances that can be destructive to humans.
- A heating, ventilation, and air conditioning (HVAC) system is responsible for controlling humidity and temperature in a data center, and is necessary to protect equipment.
- When working with sensitive components, you can protect against ESD by using an electrostatic discharge (ESD) strap.
- For rack installations, protect against ESD, ground the device, place it in the rack for good airflow, and pay attention to tool safety as you work.

Troubleshooting Network Problems

- The seven troubleshooting steps used in networking are: (1) Identify the problem and its symptoms, (2) establish a theory of probable cause, (3) test your theory, (4) establish a plan to fix the problem, (5) implement the solution or escalate the problem, (6) verify functionality and implement preventive measures, and (7) document findings, actions, and outcomes.
- Troubleshooting can follow the top-to-bottom OSI model or the bottom-to-top OSI model, depending on the nature of the problem.
- Troubleshooting problems and their solutions are documented in a call tracking system. An organization might require that major changes to a network be documented in a change management system.

Key Terms

For definitions of key terms, see the Glossary near the end of the book.

Active Directory (AD)
Active Directory Domain Services (AD DS)
API (application programming interface) call
Application layer
ARP (Address Resolution Protocol)
backbone
bandwidth
best-effort protocol
bus topology
call tracking system
CAN (campus area network)
catastrophic failure
client-server applications
client-server network model
connectionless protocol
connection-oriented protocol
convergence
Data Link layer
Data Link layer address
datagram
decapsulation
delay-sensitive
demarc
demarcation point
domain
electrostatic discharge (ESD)
emergency alert system
encapsulation
fail close
fail open
file server
file services
fire suppression system
fragmentation
frame
FTP (File Transfer Protocol)
global account
grounding
hardware address
header
heating, ventilation, and air conditioning (HVAC) system
host
HTTP (Hypertext Transfer Protocol)
HTTPS (HTTP Secure)
hybrid topology
ICMP (Internet Control Message Protocol)
IMAP4 (Internet Message Access Protocol, version 4)
IP (Internet Protocol)
IP address
knowledge base
Layer 2 switch
Link layer
Link layer switch
local account
local area network (LAN)
logical topology
loss-tolerant
MAC (Media Access Control) address
MAN (metropolitan area network)
material safety data sheet (MSDS)
multicast distribution
network
network adapter
network interface card (NIC)
Network layer
network operating system (NOS)
network services
node
onboard network port

OSHA (Occupational Safety and Health Administration)
OSI (Open Systems Interconnection) reference model
Packet
PAN (personal area network)
patch panel
payload
peer-to-peer (P2P) network model
personal protective equipment (PPE)
physical address
Physical layer
physical topology
plenum
point-to-multipoint model
point-to-point model
POP3 (Post Office Protocol, version 3)
port number
Presentation layer
print services
protocol
protocol data unit (PDU)
quality of service (QoS)
rack
RDP (Remote Desktop Protocol)
remote application
Remote Desktop
Remote Desktop Services
ring topology
router
RTP (Real-time Transport Protocol)
scalable
Secure Shell (SSH)
segment
Session layer
SFTP (Secure File Transfer Protocol)
SMTP (Simple Mail Transfer Protocol)
SSL (Secure Sockets Layer)
star topology
star-bus topology
static electricity
switch
TCP (Transmission Control Protocol)
TCP/IP
Telnet
Terminal Services
TLS (Transport Layer Security)
topology
trailer
Transport layer
trip hazard
UDP (User Datagram Protocol)
unified communications (UC)
upset failure
video teleconference (VTC)
VoIP (Voice over IP)
WAN (wide area network)

Review Questions

1. In the client-server model, what is the primary protocol used for communication between a browser and Web server?
   a. FTP
   b. TCP
   c. HTTP
   d. SSL
2. Which two encryption protocols might be used to provide secure transmissions for browser and Web server communications?
   a. HTTP and HTTPS
   b. SSL and TLS
   c. SSL and HTTP
   d. TCP and UDP
3. Apache is a popular example of what type of networking software?
   a. Web server
   b. Browser

c. Email server

d. Email client

4. Which email protocol allows an email client to download email messages to the local computer?

a. IMAP4

b. SMTP

c. TCP

d. POP3

5. Which email protocol allows an email client to read mail stored on the mail server?

a. IMAP4

b. SMTP

c. TCP

d. POP3

6. Which client-server application allows an administrator to control a remote computer, but does not encrypt or secure the communication between client and server?

a. Telnet

b. Remote Desktop

c. FTP

d. SSH

7. Which application embedded in Windows operating systems allows remote control of a computer and uses the RDP secure protocol for transmissions?

a. Telnet

b. Remote Desktop

c. FTP

d. SSH

8. What service provided by Windows Server 2012 R2 allows a computer to serve up applications to other computers on the network?

a. Remote Desktop Services

b. Windows 8.1

c. File Transfer Protocol

d. Active Directory

9. List three types of services a network might support that are considered part of unified communications or convergence.

a. File transfers, print services, and conversational voice

b. User authentication, streaming live audio and video, and print services

c. Web services, email services, and file services

d. Conversational voice, streaming live audio and voice, and streaming stored audio and voice

10. Which Session layer protocol is a streaming live video teleconference likely to use on the network?

a. UDP

b. SMTP

c. RTP

d. TCP

11. A network consists of 10 computers, all running Windows 7 Professional. One computer acts as a file server and serves up data to other computers on the network. Which networking model does the network use?

12. In Question 11, suppose one computer is upgraded from Windows 7 Professional to Windows Server 2012 R2. Which networking model can the network now support that it could not support without the upgrade?

13. What is the name of the domain controller database that Windows Server 2012 R2 uses to store data about user access and resources on the network?

14. A network consists of seven computers and a network printer all connected directly to one switch. Which network topology does this network use?

15. In Question 14, suppose a new switch is connected to the first switch by way of a network cable and three computers are connected to the new switch. Which network topology is now used?

16. What is the fundamental distinction between a Layer 2 switch and a router?

17. What is the fundamental distinction between a node and a host?

18. What is the fundamental distinction between a MAN and a WAN?

19. What is a message called that is delivered by TCP? What is a message called that is delivered by UDP? At which layer do the two protocols work?

20. Which type of address is used at the Transport layer to identify the receiving application?

21. Is TCP or UDP normally used when streaming live video? Why?

22. At the Network layer, what is a message called?

23. What is the primary protocol used at the Network layer?

24. At the Network layer, what type of address is used to identify the receiving host?

25. What is a PDU called at the Link layer?

26. At the Link layer, which type of network address is used to identify the receiving node?

27. Why is it important to wear an ESD strap when installing a server in a rack?

28. A computer is unable to access the network. When you check the LED lights near the computer's network port, you discover the lights are not lit. Which layer of the OSI model are you using to troubleshoot this problem? At which two layers does the network adapter work?
29. A user complains that he cannot access a particular Web site, although he is able to access other Web sites. At which layer of the OSI model should you begin troubleshooting the problem?
30. A user complains that Skype drops her videoconference calls and she must reconnect. At which layer of the OSI model should you begin troubleshooting? Which OSI layer is responsible for not dropping the Skype connection?

Hands-On Projects

Project 1-1: Set Up a Small Network

For this project, you'll need two Windows 7 or Windows 8.1 computers, a small consumer-grade switch (one that does not require its firmware to be configured), and two regular network cables (a regular network cable is also called a straight-through cable or patch cable). Do the following to set up a small network:

1. Use the network cables to connect each computer to the switch. Make sure the switch has power. Verify the LED lights on the network ports of the computers and switch are lit and/or blinking to verify network connectivity and activity.
2. Open the Network and Sharing Center of each computer to verify that Windows sees the computer connected to the network. (In Windows 7, click **Start**, **Control Panel**, and make sure Control Panel is set to **Small icons** view. Then click **Network and Sharing Center**. In Windows 8.1, to open Control Panel, right-click the **Start** button and click **Control Panel**.)
3. If you don't see connectivity, reset the connection by restarting the computer. In Chapter 2, you'll learn about easier methods to verify and reset a network connection.
4. Open Windows Explorer or File Explorer and look in the Network group in the navigation pane. You should see the other computer listed. You won't be able to access resources on the other computer unless you share these resources in a homegroup or share a specific folder or file.
5. Answer the following questions:
   a. Does your network use a client-server or peer-to-peer model?
   b. What is the topology of your network?
   c. If the lights on the switch ports were not lit or blinking, what is the best theory of probable cause? At what layer of the OSI model would this theory be?

As you work your way through this book, you will continue to build your small network and its resources.

Project 1-2: Guidelines for Installing a Switch

While working as an intern in a corporate data center, you are asked to research the guidelines for installing a Cisco Nexus 5000 series switch in a rack. Search the Cisco Web site and other sites and answer the following questions:

1. Find a photo of any Nexus 5000 series switch. How much does the switch cost? Create a screenshot showing a photo of the switch and its price.
2. What are the two types of racks Cisco recommends for the switch? Find a rack of each type that meets these qualifications. Create screenshots showing a photo of each rack, its manufacturer, and price.
3. Create a screenshot showing the required equipment for installing the switch.
4. Create a screenshot showing the additional items needed to ground the switch.
5. Why does Cisco recommend you keep the shipping container?
6. Which installs first, the brackets or the sliders?
7. Create a document and insert into it the screenshots you made and the answers to the questions. Include in the document your name and course information and email the document to your instructor.

Project 1-3: Research Network Operating Systems

The client-server network at Scoops, a chain of ice cream stores, currently depends on one server machine running Windows Server 2008 as its NOS. However, the system was installed five years ago, and the chain is growing. The company's general manager has heard a lot of good things about Linux operating systems—in particular, a type of Linux called Fedora. He asks you to find out how these two NOSs differ in their file sharing, remote access, and mail service capabilities. Also, he wonders how the two compare in their ease of use, reliability, and support. He remarks that he doesn't want to spend a lot of time looking after the server, and reminds you that he is not a technical expert. After some research, what can you tell him about the similarities and differences between these two NOSs? Do you advise the Scoops chain to change its server's NOS to Linux? Why or why not?

Project 1-4: IT and Networking Certifications

This book prepares you to take the CompTIA Network+ N10-006 exam, which is considered a fundamental benchmark toward a career in IT. Many other IT certifications apply to IT and networking. Use the Web to research and answer the following questions:

1. Which certification does CompTIA recommend a candidate for the CompTIA Network+ exam already have?
2. How long does CompTIA recommend you work in networking before you take the CompTIA Network+ exam?
3. Cisco offers a full range of certifications focused on all aspects of networking. How long does Cisco recommend you work in networking before you take the CCNA Routing and Switching exam for certification?

4. How long does Cisco recommend you work in networking before you take the CCIE Routing and Switching exam?
5. Microsoft offers a group of certifications collectively called the Microsoft Certified Solutions Expert (MCSE). What are the eight MCSE certifications?
6. Search online for a job opening in IT networking in your geographical area and save or print the job description and requirements. (Excellent sites that post IT jobs are Indeed.com and Monster.com.) Answer the following questions about the job:
   a. Which degrees are required or recommended?
   b. What types of skills are required or recommended?
   c. Which IT certifications are required or recommended?

Case Projects

In Case Project 1-1, you set up a virtual machine (VM) using Client Hyper-V, and in Case Project 1-2, you set up a VM using Oracle VirtualBox. You only need to do one of these case projects. However, you'll need to do one because we'll continue to build your virtual network of VMs in later chapters. Client Hyper-V and VirtualBox are client hypervisors, which is software used to manage VMs installed on a workstation. If you don't want to use Client Hyper-V or VirtualBox as your hypervisor of choice, you can substitute another client hypervisor, such as VMware Player, which can be downloaded free from *vmware.com*. Note that Windows Hyper-V and Oracle VirtualBox don't play well on the same computer, and can cause problems, such as failed network connectivity. For that reason, don't install Hyper-V and VirtualBox on the same computer.

Case Project 1-1: Set Up a Virtual Machine Using Hyper-V

In this project, you use Hyper-V, which is software embedded in Windows 8.1 Professional, 64-bit version, to create and manage virtual machines (VM) and virtual networks on a single workstation. You'll first enable the workstation BIOS to support virtualization and enable Hyper-V and then create a VM in Hyper-V. Then you will install an OS in the VM. Your instructor will provide access to the Windows operating system installation files used in the VM.

Using a Windows 8.1 Pro, 64-bit version computer, follow these steps to enable virtualization in BIOS, enable Hyper-V, and configure a virtual switch for the virtual network:

1. For Hyper-V to work, hardware-assisted virtualization (HAV) must be enabled in BIOS setup. If you are not sure it is enabled, power down your computer, turn it on, press a key during start-up to access BIOS setup, and make sure hardware-assisted virtualization is enabled. For one system, that's done on the Security BIOS screen shown in Figure 1-25. Also make sure that any subcategory items under HAV are enabled. Save your changes, exit BIOS setup, and allow the system to restart to Windows 8.1.
2. Hyper-V is disabled in Windows 8.1 Pro by default. To enable it, right-click **Start** and click **Programs and Features**. Then click **Turn Windows features on or off**. Check **Hyper-V** and close all windows. You'll need to restart the computer for the change to take effect.

Figure 1-25 Virtualization must be enabled in BIOS setup for Client Hyper-V to work

3. Launch the **Hyper-V Manager** application. In the Hyper-V Manager left pane, select the host computer.
4. To make sure your VMs have access to the network or the Internet, you need to first install a virtual switch in Hyper-V. To create a new virtual network switch, click **Virtual Switch Manager** in the Actions pane.
5. In the Virtual Switch Manager dialog box, verify **New virtual network switch** is selected in the left pane. To bind the virtual switch to the physical network adapter so the VMs can access the physical network, select **External** in the right pane. Then click **Create Virtual Switch**. In the next dialog box, make sure **Allow management operating system to share this network adapter** is checked and click **Apply**. Click **Yes**. Your virtual LAN now has a virtual switch. Close the Virtual Switch Manager dialog box.

To create a VM, follow these steps:

6. In the Actions pane, click **New** and then click **Virtual Machine**. The New Virtual Machine Wizard launches. Use these parameters for the new VM:
   - Select a name for your VM, for example VM1 or VM_Lab_B.
   - Make sure **Generation 1** is selected in the Specify Generation box.
   - Set the amount of RAM for the VM. Be sure to specify at least the minimum requirement for the OS you plan to install in the VM.
   - Check **Use Dynamic Memory for this virtual machine**.
   - Specify the VM can use the new virtual switch you created earlier.
   - Specify a new dynamically expanding virtual hard drive.
   - Specify how you will install an OS in the VM, which depends on the method your instructor used to provide you these setup files.

7. After the VM is created, it's listed in the middle pane of the Hyper-V Manager window. When you select it, its thumbnail appears in the middle pane of the Hyper-V Manager window.

Now you're ready to install an OS in the VM. The OS setup files are likely to come bundled in a single ISO file. An ISO file is a Disc Image File, which is a virtual DVD or CD. Follow these steps to mount an ISO file or a physical CD or DVD to the VM's virtual optical drive and install Windows:

8. Select the VM in the middle pane of the Hyper-V Manager window and click **Settings** near the bottom of the Actions pane. In the left pane of the Settings dialog box, select the **DVD Drive**. In the right pane, select **Image file**. Click **Browse** and browse to the ISO file. Select it and click **Open**. Click **OK** to mount the ISO file to the virtual DVD drive.
9. To boot the VM to the DVD drive, select **BIOS** in the left pane of the Settings box to verify the boot priority order of the VM begins with CD. Click **Apply** to apply your changes.
10. To boot up the selected VM, click **Start** in the Actions pane of the Hyper-V Manager window. To see the VM in its own window, double-click the thumbnail, as shown in Figure 1-26, where a Windows 8 installation has begun.

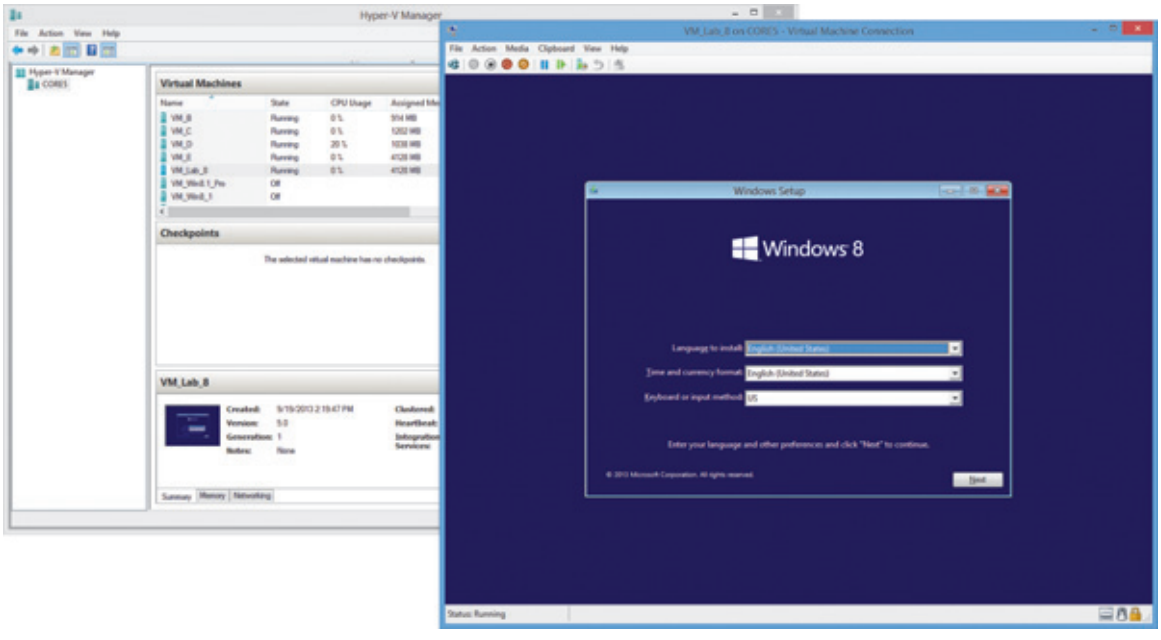


Figure 1-26 Windows 8 setup is running in the VM managed by Hyper-V

Source: Microsoft LLC

11. After you have installed Windows in the VM, open Internet Explorer to confirm the VM has a good Internet connection.

In future chapters, you'll continue to build your virtual network and install resources in the VMs on your network.

Case Project 1-2: Set Up a Virtual Machine Using Oracle VirtualBox

Using Windows 7 or Windows 8.1, you can download and install Oracle VirtualBox and use this free hypervisor to create virtual machines and a virtual network. Have available an ISO file to install the Windows operating system in the VM. Follow these steps:

1. Go to **virtualbox.org/wiki/Downloads** and download **VirtualBox for Windows hosts x86/amd64** to your desktop or other folder on your hard drive. Install the software, accepting default settings during the installation. The Oracle VM VirtualBox Manager window opens (see Figure 1-27).

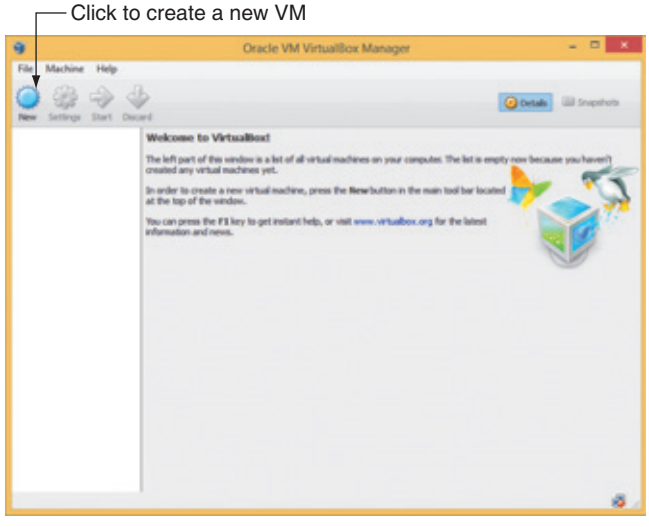


Figure 1-27 Use the VirtualBox Manager to create and manage virtual machines

Source: Oracle VirtualBox

2. To create a virtual machine using VirtualBox, click **New** in the toolbar and follow the wizard to create a VM. Name the virtual machine **VM10** and select the Windows OS you will install in it. You can accept all default settings for the VM.
3. With the VM selected, click **Settings** in the VirtualBox Manager window. In the VM10-Settings box, click **Storage** in the left pane.

4. In the Storage Tree area, to the right of Controller: IDE, click **Add CD/DVD Device**, which is represented by the single CD icon, as shown in Figure 1-28.

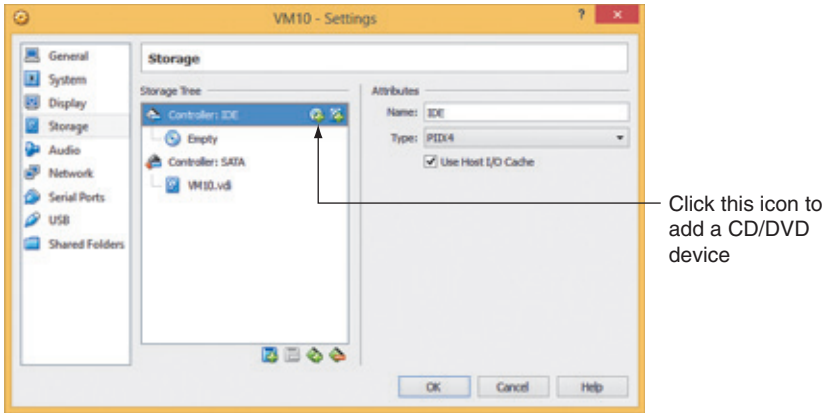


Figure 1-28 Storage Tree options allow you to mount an ISO image as a virtual CD in the VM

Source: Oracle VirtualBox

5. A dialog box appears. Click **Choose disk**. Browse to the location of the ISO file that contains the Windows operating system setup files made available by your instructor, click **Open**, and then click **OK**. You return to the VirtualBox Manager window.
6. Click **Start** on the toolbar. Your VM starts up and begins the process of installing the operating system.