

# Chapter 1

## Computer Networking Fundamentals

---

**THE FOLLOWING CWTS EXAM OBJECTIVES  
ARE COVERED IN THIS CHAPTER:**

- ✓ 1.4 Explain the role of Wi-Fi as a network access technology





It is important to have an understanding of basic computer networking concepts before you begin exploring the world of over-the-air (wireless) networking technology, wireless terminology, and mobility. This chapter looks at various topics surrounding foundational computer networking, including computer network types, computer topologies, the OSI model, and network device addressing. It is intended to provide an overview of basic computer networking concepts as an introduction for those who need to gain a basic understanding or for those already familiar with this technology and want a review of these concepts.

You will learn about the various types of wireless networks—including wireless personal area networks (WPANs), wireless local area networks (WLANs), wireless metropolitan area networks (WMANs), and wireless wide area networks (WWANs)—in Chapter 2, “Wireless Local Area Networking, Standards, and Certifications.”

## Network Types

Computer networking technology has evolved at a tremendous pace over the past couple of decades, and many people across the world now have some type of exposure to the technology. Initially, personal computers were connected, or networked, to share files and printers and to provide central access to the users’ data. This type of network was usually confined to a few rooms or within a single building and required some type of cabled physical infrastructure. As the need for this technology continued to grow, so did the types of networks. Computer networking started with the local area network (LAN) and grew on to bigger and better types, including wide area networks (WANs), metropolitan area networks (MANs), and others. The following are some of the common networking types in use today:

- Local area networks (LANs)
- Wide area networks (WANs)
- Metropolitan area networks (MANs)
- Campus area networks (CANs)
- Personal area networks (PANs)



You may also come across the term *storage area network (SAN)*. The SAN is basically a separate subnet for offloading large amounts of data used within an enterprise network. High-speed connections are used, so the data is easily accessible because it appears to be part of the network. The connections are commonly Fibre Channel or iSCSI utilizing the TCP/IP protocol.

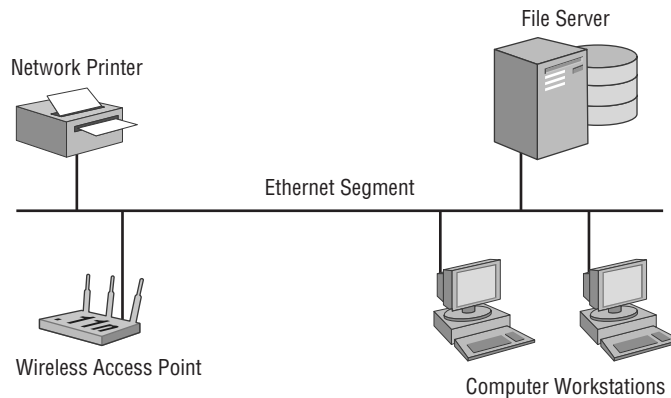
Most computer networks today contain some type of wireless connectivity or may consist of mostly wireless connectivity. The need for wireless networking and mobility continues to be in great demand and is growing at a rapid pace.

## The Local Area Network

A *local area network (LAN)* can be defined as a group of devices connected in a specific arrangement called a *topology*. The topology used depends on where the network is installed. Some common legacy topologies (such as the bus and ring) and more modern topologies (such as the star and mesh) are discussed later in this chapter. LANs are contained in the same physical area and usually are bounded by the perimeter of a room or building. In some cases, however, a LAN may span a group of buildings in close proximity that share a common physical connection.

Early LANs were used primarily for file and print services. File services enabled users to store data securely and provided a centralized location of data for accessibility even when the user was physically away from the LAN. This central storage of data also gave a network administrator the ability to back up and archive all the saved data for disaster recovery purposes. As for print services, it was not cost effective to have a physical printer at every desk or for every user, so LANs allowed the use of shared printers for any user connected to the LAN. Figure 1.1 illustrates a LAN that includes both wired and wireless networking devices.

**FIGURE 1.1** Example of a local area network (LAN)

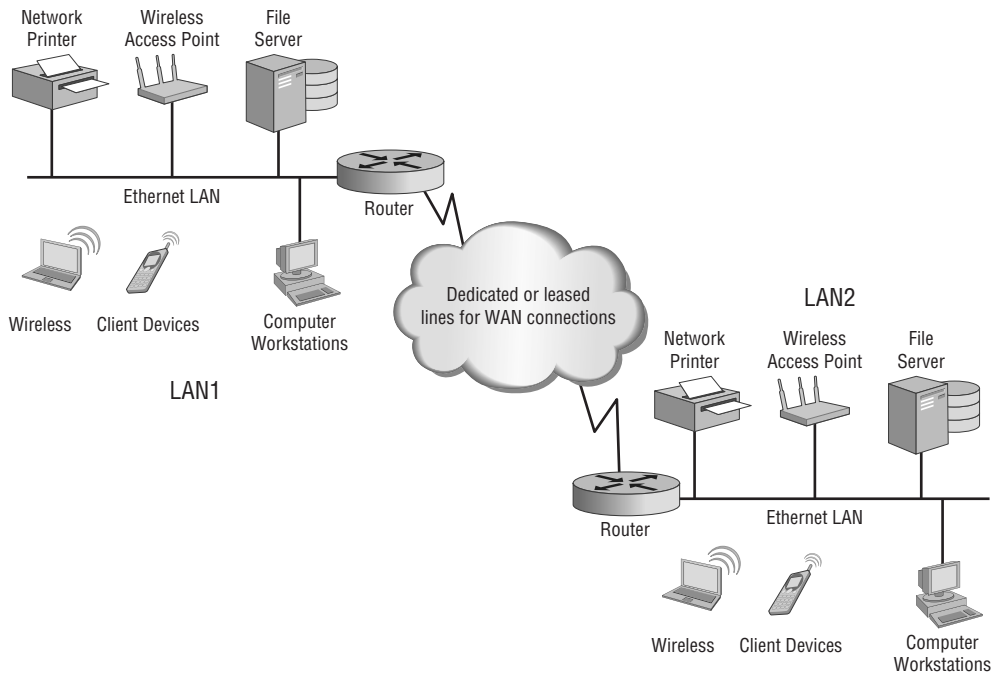


## The Wide Area Network

As computer networking continued to evolve, many businesses and organizations that used this type of technology needed to expand the LAN beyond the physical limits of a single room or building. These networks covered a larger geographical area and became known as *wide area networks (WANs)*. As illustrated in Figure 1.2, WAN connectivity

mostly consists of point-to-point or point-to-multipoint connections between two or more LANs. The LANs may span a relatively large geographical area. (Point-to-point and point-to-multipoint connections are discussed later in this chapter.) The WAN has allowed users and organizations to share data files and other resources with a much larger audience than a single LAN would.

**FIGURE 1.2** Example of a wide area network (WAN) connecting two LANs



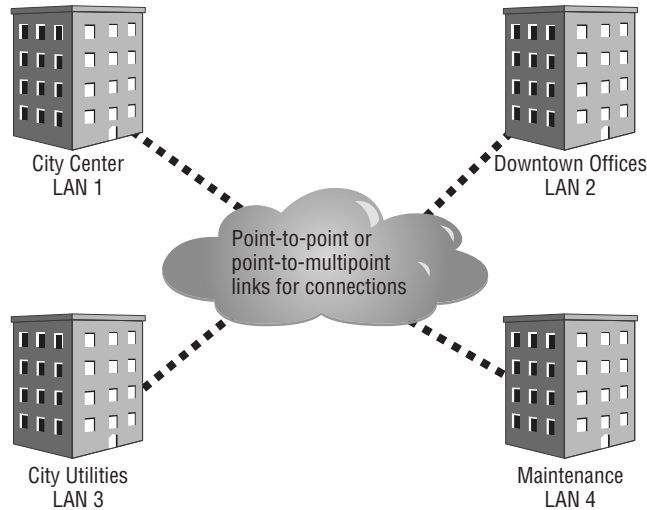
WANs can use leased lines from telecommunication providers (commonly known as *telcos*), fiber connections, and even wireless connections. The use of wireless for bridging LANs is growing at a fast pace because it can often be a cost-effective solution for connecting LANs.

## The Metropolitan Area Network

The *metropolitan area network (MAN)* interconnects devices for access to computer resources in a region or area larger than that covered by LANs but yet smaller than the areas covered by WANs. A MAN consists of networks that are geographically separated and can span from several blocks of buildings to entire cities (see Figure 1.3). MANs include fast

connectivity between local networks and may include fiber optics or other wired connectivity that is capable of longer distances and higher capacity than those in a LAN.

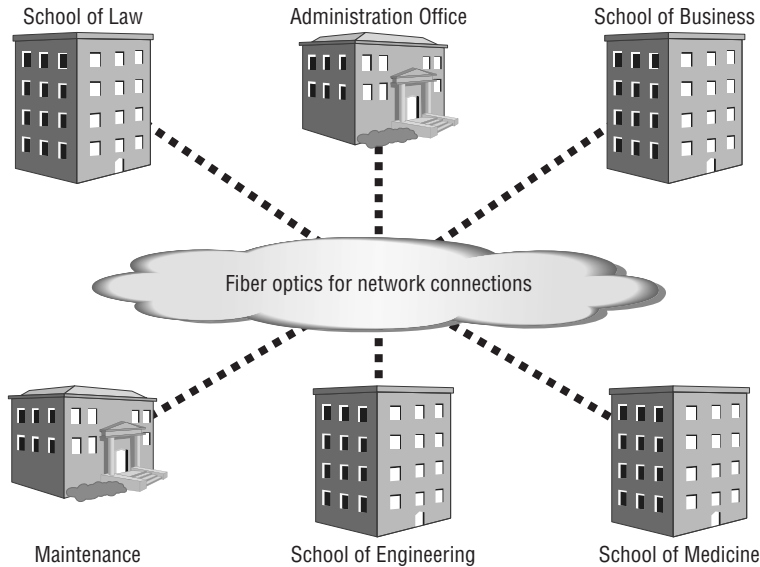
**FIGURE 1.3** Example of a metropolitan area network (MAN) connecting a small town



MANs allow for connections to outside larger networks such as the Internet. They may include cable television, streaming video, and telephone services. Devices and connectivity used with MANs may be owned by a town, county, or other locality, and may also include the property of individual companies. Wireless MANs are also becoming a common way to connect the same type of areas but without the physical cabling limitations.

## The Campus Area Network

A *campus area network (CAN)* includes a set of interconnected LANs that basically form a smaller version of a WAN within a limited geographical area, usually an office or school campus. Each building within the campus generally has a separate LAN. The LANs are often connected using fiber-optic cable, which provides a greater distance than copper wiring using IEEE 802.3 Ethernet technology. However, using wireless connections between the buildings in a CAN is an increasingly common way to connect the individual LANs. These wireless connections or wireless bridges provide a quick, cost-effective way to connect buildings in a university campus, as shown in Figure 1.4.

**FIGURE 1.4** Example of a campus area network (CAN) connecting a school campus

In a university campus environment, a CAN may link many buildings, including all the various colleges—such as the College of Business, College of Law, College of Engineering, and so on—as well as the university library, administration buildings, and even residence halls. Wireless LAN deployments are now commonplace in university residence halls. With the rapidly increasing number of wireless mobile devices on university campuses, the number of wireless access points and the capacity of each need to be considered.

As in the university campus environment, a corporate office CAN may connect all the various building LANs that are part of the organization. This type of network will have the characteristics of a WAN but be confined to the internal resources of the corporation or organization. Many organizations are deploying wireless networks within the corporate CAN as a way to connect various parts of the business. As with the university CAN, in the corporate world a wireless CAN is a quick, cost-effective way to provide connectivity between buildings and departments.

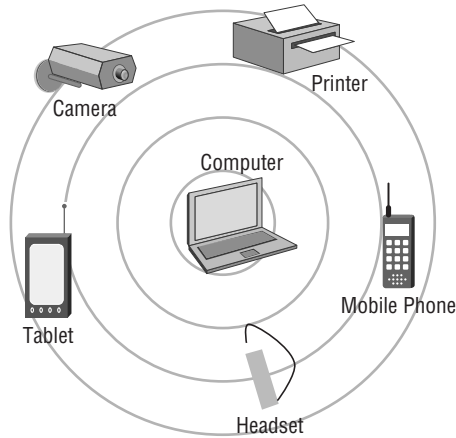
All the physical connection mediums and devices are the property of the office or school campus, and responsibility for the maintenance of the equipment lies with the office or campus as well.

## The Personal Area Network

*Personal area networks (PANs)* are networks that connect devices within the immediate area of individual people. PANs may consist of wired connections, wireless connections, or both. On the wired side, this includes universal serial bus (USB) devices such as printers, keyboards, and computer mice that may be connected with a USB hub. With wireless

technology, PANs are short-range computer networks and in many cases use Bluetooth wireless technology. Wireless Bluetooth technology is specified by the IEEE 802.15 standard and is not IEEE 802.11 wireless LAN technology. Bluetooth will be discussed in more detail in Chapter 2. Like wired PANs, wireless PANs are commonly used in connecting an individual's wireless personal communication accessories, such as phones, headsets, computer mice, keyboards, tablets, and printers, and are centered on the individual personal workspace without the need for physical cabling. Figure 1.5 illustrates a typical wireless PAN configuration.

**FIGURE 1.5** Example of a wireless Bluetooth network connecting several personal wireless devices



## Network Topologies

A computer's physical network topology is the actual layout or physical design and inter-connection of a computer network. A topology includes the cabling and devices that are part of the network. In the following sections you will learn about several different types of network topologies:

- Bus
- Ring
- Star
- Mesh
- Ad hoc
- Point-to-point
- Point-to-multipoint

The bus, ring, star, mesh, and ad hoc topologies are typically what make up the LAN you learned about previously. Point-to-point and point-to-multipoint topologies can be commonly used for connecting LANs but are mostly used for WAN connections. The size of your network will determine which topologies will apply. If your network is a single building and not part of a larger corporate network, the LAN topologies may be the extent of the technologies used. Once that LAN connects to a different LAN, however, you are moving up and scaling to a WAN.

## The Bus Topology

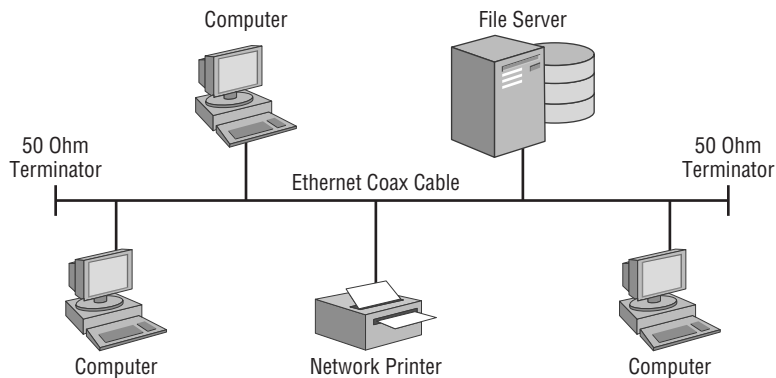
A *bus* topology consists of multiple devices connected along a single shared medium with two defined endpoints. It is sometimes referred to as a *high-speed linear bus* and is a single collision domain in which all devices on the bus network receive all messages. Both endpoints of a bus topology have a 50-ohm termination device, usually a Bayonet Neill-Concelman (BNC) connector with a 50-ohm termination resistor. The bus topology was commonly used with early LANs but is now considered a legacy design.

One disadvantage to the bus topology is that if any point along the cable is disconnected, damaged, or broken, the entire LAN will cease to function. This is because the two endpoints communicate only across the single shared medium; there is no alternative route for them to use in the event of a problem.

Troubleshooting a bus network is performed by a technique known as the *half-split method*. A network engineer “breaks” or separates the link at about the halfway point and measures the resistance of the link on both ends. If the segment measures 50 ohms of resistance, there is a good chance that side of the LAN segment is functioning correctly. If the resistance measurement is not 50 ohms, it signals a problem with that part of the LAN segment. The engineer continues with this method until the exact location of the problem is identified. Depending on the length of the segment and the type of installation, this can be a time-consuming and tedious process.

Figure 1.6 illustrates an example of the bus topology.

**FIGURE 1.6** Example of the bus topology







## Real World Scenario

### Troubleshooting the Bus Topology

Many years ago I was called to troubleshoot a problem on a small LAN using a bus topology. The network consisted of a network file server, about 20 client stations, and a few network printers. The users complained of intermittent connection problems with the network. After spending some time looking over the network, I decided to test the bus using the half-split method and checked to verify that the cable was reporting the correct resistance using a volt-ohm-milliammeter (VOM) meter. Sure enough, one side of the network cable reported the correct resistance reading, but the other side was giving intermittent results.

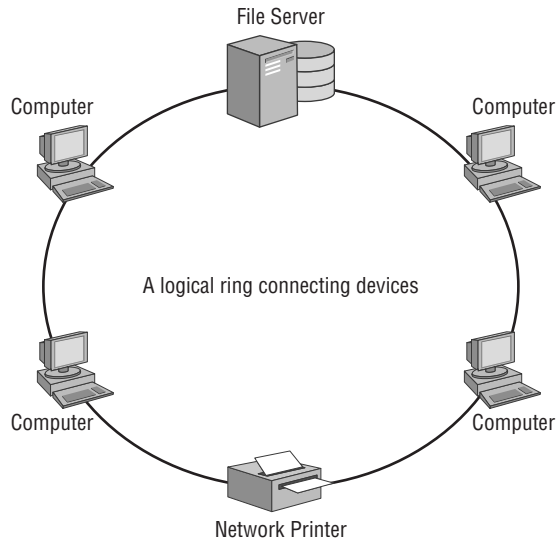
After spending some time repeating the troubleshooting method, I was able to determine the problem. Someone had run the coax (bus) cable underneath a heavy plastic office chair mat, and one of the little pegs used to protect the flooring was causing the intermittent connection as it struck the cable when the user moved their chair around the mat. I quickly replaced and rerouted the section of cable in question. It is a good thing I was there during the normal business operating hours when the person was moving around in the chair, or I might have never found the problem. Ah, the joys of troubleshooting a bus topology.

## The Ring Topology

In the *ring* topology, each device connects to two other devices, forming a logical ring pattern. The ring topology is rarely used with LANs today, but it is still widely used by Internet service providers (ISPs) for high-speed, resilient backhaul connections over fiber-optic links.

Ring topologies in LANs may use a token-passing access method in which data travels around the ring in one direction. Only one device at a time will have the opportunity to transmit data. Because this access method travels in one direction, it does not need to use collision detection and often outperforms the bus topology, achieving higher data transfer rates than are possible using a collision detection access method. Each computer on the ring topology can act as a repeater, a capacity that allows for a much stronger signal.

The IEEE standard for LANs is IEEE 802.5, specifying Token Ring technology. IEEE 802.5 Token Ring technology used in LANs was a very efficient method used to connect devices, but it was usually more expensive than the bus or star topologies. Because of the token-passing method used, early 4 Mbps Token Ring networks could sometimes outperform a 10 Mbps IEEE 802.3 collision-based Ethernet network. Token Ring technology speeds increased to 16 Mbps but decreased in popularity as Ethernet speeds increased. Even though this is a ring topology, devices are connected through a central device and appear to be similar to devices on an Ethernet hub or switch. Figure 1.7 shows an example of the ring topology.

**FIGURE 1.7** Example of the ring topology

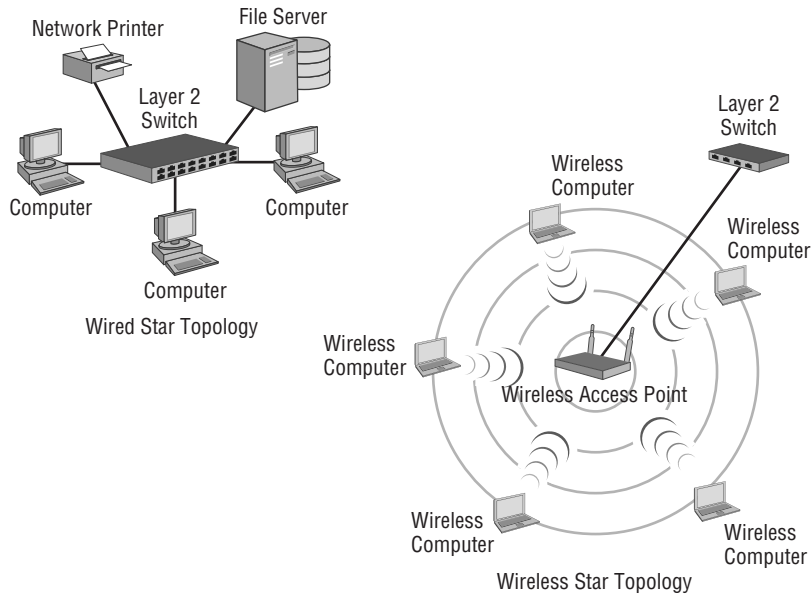
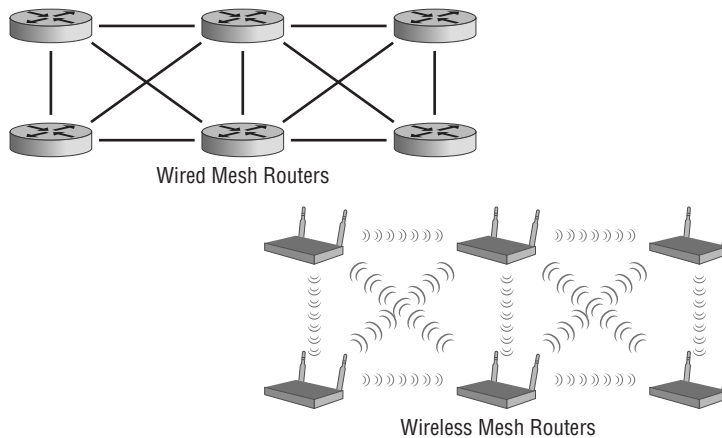
## The Star Topology

The *star* topology, as shown in Figure 1.8, is the most commonly used method of connecting devices on a LAN today. It consists of multiple devices connected by a central connection device. Hubs, switches, and wireless access points are all common central connection devices, although hubs are rarely used today. The hub provides a single collision domain similar to a bus topology. However, the Ethernet switch and wireless access point both have more intelligence—the capability to decide which port specific network traffic can be sent to. Note that in Figure 1.8, the wireless star topology includes an Ethernet switch, which could also have extended devices connected to it with wires. In that sense, it is possible to have a wired/wireless hybrid topology.

A big advantage to the star over the bus and some ring topologies is that if a connection is broken or damaged, the entire network does not cease to function; only a single device in the star topology is affected. The central connection device, such as a switch or wireless access point, can be considered a potential central point of failure.

## The Mesh Topology

A device in a mesh network will process its own data as well as serving as a communication point for other mesh devices. Each device in a *mesh* topology (see Figure 1.9) has one or more connections to other devices that are part of the mesh network. This approach provides both network resilience in case of link or device failure and a cost savings compared to full redundancy. Mesh technology can operate with both wired and wireless infrastructure network devices. Wireless mesh networks continue to grow in popularity because of the potential uses in various deployment models and the cost savings they provide.

**FIGURE 1.8** Example of a common star topology using either wired or wireless devices**FIGURE 1.9** Mesh networks can include either wired or wireless devices.

From an IEEE 802.11 wireless perspective, wireless mesh technology has now been standardized, although most manufacturers continue to use their proprietary methods. The amendment to the IEEE 802.11 standard for mesh networking is 802.11s. This amendment was ratified in 2011 and is now part of the latest wireless LAN standard, IEEE 802.11-2016. In addition to IEEE 802.11 networks, mesh is also standardized in IEEE 802.15 personal

area networks for use with Zigbee and IEEE 802.16 wireless MAN networks. Wireless standards will be discussed in more detail in Chapter 2.

As mentioned earlier, IEEE 802.11 wireless device manufacturers commonly use proprietary Layer 2 routing protocols, forming a self-healing wireless infrastructure (mesh) in which edge devices can communicate. Manufacturers of enterprise wireless networking infrastructure devices provide support for mesh access points (APs) such that the mesh APs connect back to APs that are directly wired into the network backbone infrastructure. The APs, wireless LAN controllers or software-based cloud solutions in this case, are used to configure both the wired and mesh APs.

## Ad Hoc Connections

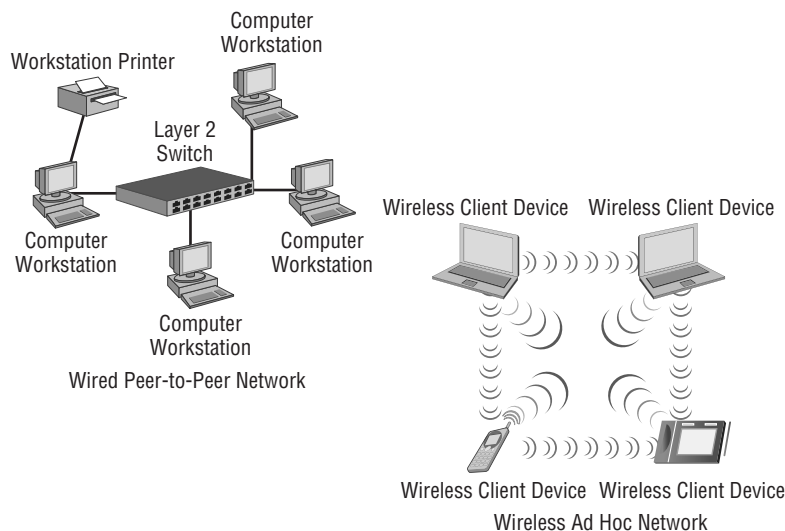
In the terms of computer networking, the *ad hoc* network is a collection of devices connected without a design or a plan for the purpose of sharing information or resources. Another term for an ad hoc network is *peer-to-peer network*.

In a wired peer-to-peer network, all computing devices are of equal status. In other words, no server manages the access to network resources. All peers can either share their own resources or access the resources of their devices on the network.

An ad hoc wireless network is one that does not contain a distribution system, which means no wireless access point is contained in the system to provide centralized communications.

Figure 1.10 shows an example of a wired peer-to-peer network and a wireless ad hoc network.

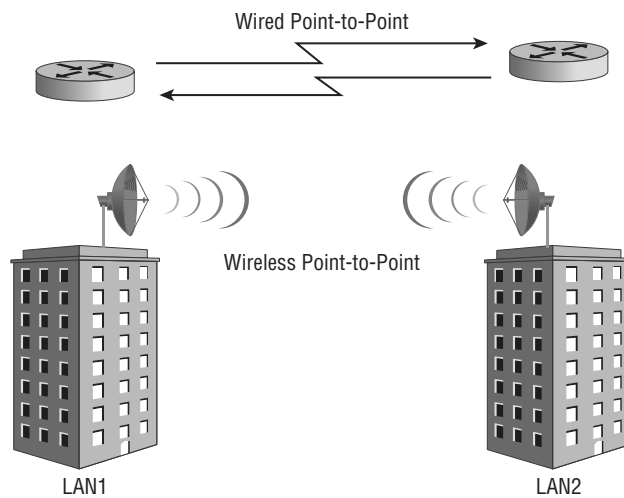
**FIGURE 1.10** Wired peer-to-peer and wireless ad hoc networks



## Point-to-Point Connections

When at least two LANs are connected, it is known as a *point-to-point connection* or link (see Figure 1.11). The connection can be made using either wired or wireless network infrastructure devices and can include bridges, wireless access points, and routers. Wireless point-to-point links can sometimes extend very long distances depending on terrain and other local conditions. Point-to-point links provide a connection between LANs, allowing users from one LAN to access resources on the other connected LAN.

**FIGURE 1.11** Point-to-point connections using either wired or wireless connections



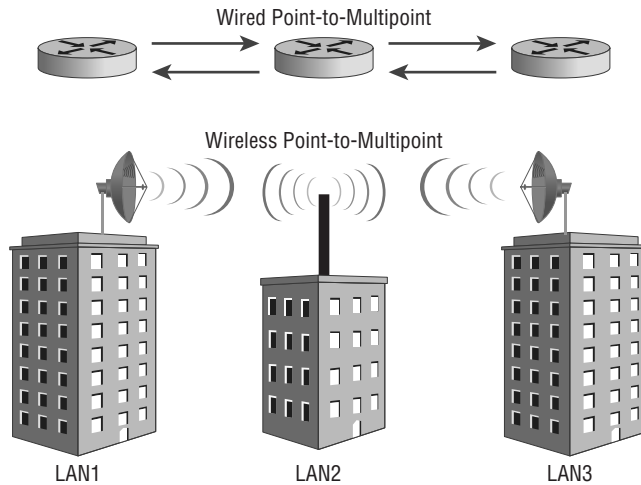
Wired point-to-point links consist of fiber-optic connections or leased lines from local telecommunication providers. Wireless point-to-point links usually call for semi-directional or highly directional antennas. Wireless point-to-point links include directional antennas and encryption to protect the wireless data as it propagates through the air from one network to the other. With some regulatory domains such as the Federal Communications Commission (FCC), when an omnidirectional antenna is used in this configuration it is considered a special case, called a point-to-multipoint link.

## Point-to-Multipoint Connections

A network infrastructure connecting more than two LANs is known as a *point-to-multipoint connection* or link (see Figure 1.12). When used with wireless, this configuration usually consists of one omnidirectional antenna and multiple semi-directional or highly

directional antennas. Point-to-multipoint links are often used in campus-style deployments, where connections to multiple buildings or locations may be required. Like point-to-point connections, wired point-to-multipoint connections can use either direct wired connections such as fiber-optic cables or leased line connectivity available from telecommunication providers.

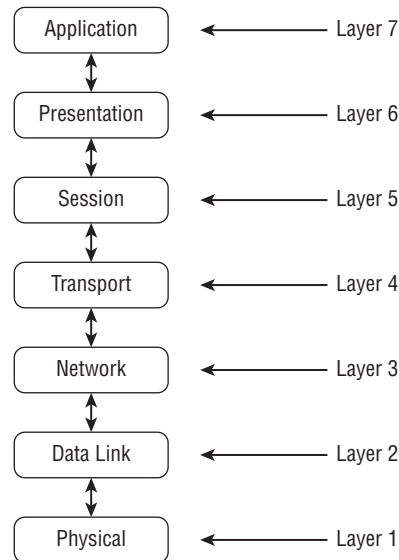
**FIGURE 1.12** Point-to-multipoint connections using either wired or wireless connections



## The OSI Model

Before we continue with other mobility topics, you should have some background on computer networking theory. The basics of a computer networking discussion start with the *Open Systems Interconnection (OSI)* model, a conceptual seven-layer model. The OSI model has been around for decades. It came about in the late 1970s and early 1980s, being published in 1984, and was developed by the International Organization for Standardization (ISO). The ISO is a worldwide organization that creates standards on an international scale. The OSI model describes the basic concept of communications in the computer network environment. Be careful not to confuse the two.

There are seven layers to the OSI model. Each layer is made up of many protocols and serves a specific function. You will take a quick look at all seven layers of the OSI model. Figure 1.13 illustrates the seven layers of the conceptual OSI model.

**FIGURE 1.13** Representation of the OSI Model

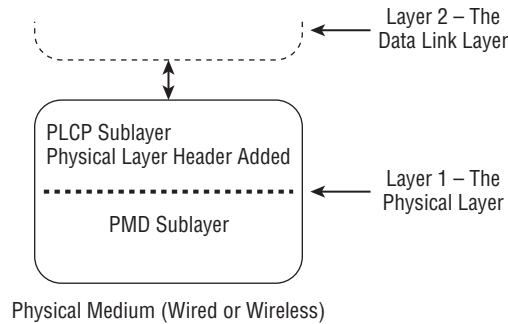
The following sections describe how each layer is used.

## Layer 1 – The Physical Layer

The *Physical layer* (sometimes referred as the *PHY*) is the lowest layer in the OSI model. The PHY consists of bit-level data streams and computer network hardware connecting the devices together. The hardware that connects devices includes network interface cards, cables, Ethernet switches, wireless access points, and bridges. Keep in mind that some of these hardware devices, such as Ethernet switches and bridges, actually have Data Link layer (Layer 2) functionally and operate at that layer but also make up the actual physical connections. In the case of wireless networking, radio frequency (RF) uses air as the medium for wireless communications. With respect to wireless networking, the Physical layer consists of two sublayers:

- Physical Layer Convergence Protocol (PLCP)
- Physical Medium Dependent (PMD)

The PLCP, the higher of the two layers, is the interface between the PMD and Media Access Control (MAC) sublayer of the Data Link layer. This is where the Physical layer header is added to the data. The PMD is the lower sublayer at the bottom of the protocol stack and is responsible for transmitting the data onto the wireless medium. Figure 1.14 shows the two sublayers that make up the Physical layer.

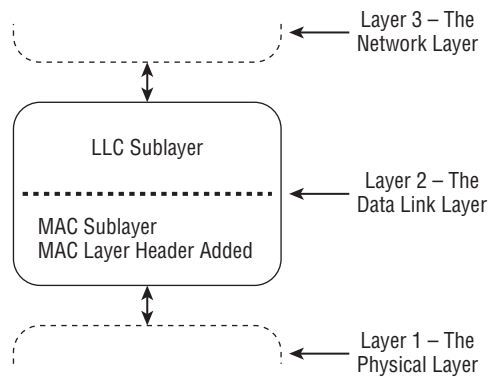
**FIGURE 1.14** Physical layer sublayers, PLCP and PMD

## Layer 2 – The Data Link Layer

The *Data Link layer* is responsible for organizing the bit-level data for communication between devices on a network and detecting and correcting Physical layer errors. This layer consists of two sublayers:

- Logical Link Control (LLC)
- Media Access Control (MAC)

The bit-level communication is accomplished through Media Access Control (MAC) addressing. A *MAC address* is a unique identifier of each device on the computer network and is known as the *physical address* or sometimes referred to as the *hardware address*. (MAC addresses are discussed later in this chapter.) Figure 1.15 illustrates the two sublayers of the Data Link layer, Layer 2.

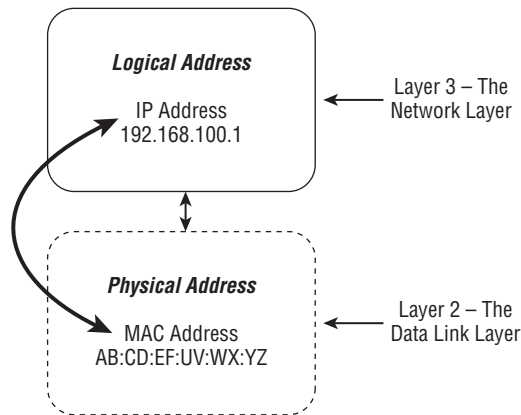
**FIGURE 1.15** Data Link layer sublayers, LLC and MAC



## Layer 3 – The Network Layer

The *Network layer* is responsible for addressing and routing data by determining the best route to take based on what it has learned or been assigned. The Internet Protocol (IP) resides at the Network layer. An IP address is defined as a numerical identifier or logical address assigned to a network device. The IP address can be static, manually assigned by a user, or dynamically assigned from a server using Dynamic Host Configuration Protocol (DHCP). (IP addresses are discussed later in this chapter.) Figure 1.16 illustrates the Layer 2 MAC address translation to a Layer 3 IP address.

**FIGURE 1.16** Data Link layer (Layer 2) to Network layer (Layer 3) address translation



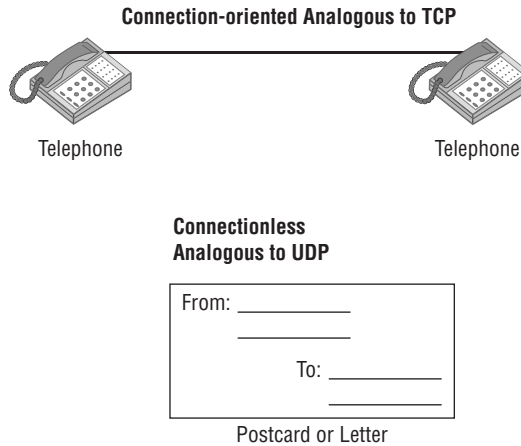
## Layer 4 – The Transport Layer

The *Transport layer* consists of both connection-oriented and connectionless protocols providing communications between devices on a computer network. Although several protocols operate at this layer, you should be familiar with two commonly used Layer 4 protocols:

- Transmission Control Protocol (TCP)
- User Datagram Protocol (UDP)

TCP is a connection-oriented protocol and is used for communications that require reliability, analogous to a circuit-switched telephone call.

UDP is a connectionless protocol and is used for simple communications requiring efficiency, analogous to sending a postcard through a mail service. You would not know if the postcard was received or not. UDP and TCP port numbers are assigned to applications for flow control and error recovery. Figure 1.17 represents the relationship between the Transport layer protocols TCP and UDP.

**FIGURE 1.17** Comparison between TCP and UDP protocols

## Layer 5 – The Session Layer

The *Session layer* opens, closes, and manages communications sessions between end-user application processes located on different network devices. The following protocols are examples of Session layer protocols:

- Network File System (NFS)
- Apple Filing Protocol (AFP)
- Remote Procedure Call Protocol (RPC)

## Layer 6 – The Presentation Layer

The *Presentation layer* provides delivery and formatting of information for processing and display. This allows for information that is sent from one device on a network (the source) to be understood by another device (the destination) on the network.

## Layer 7 – The Application Layer

The *Application layer* can be considered the interface to the user. Application is another term for a program that runs on a computer or other networking device, and that is not what we are looking at here. Protocols at this layer are for network operations such as transferring files, browsing web pages, and sending email. The following list includes some of the more common examples of Application layer protocols we use daily:

- File Transfer Protocol (FTP) for transferring data
- Hypertext Transfer Protocol (HTTP) for web browsing
- Post Office Protocol v3 (POP3) for email

## How the Layers Work Together

In order for computers and other network devices to communicate with one another using the OSI model, a communication infrastructure of some type is necessary. In a wired

network, such an infrastructure consists of cables, repeaters, bridges, and Layer 2 switches. In a wireless network, the infrastructure consists of access points, bridges, repeaters, radio frequency, and the open air. Some of these devices will be discussed in more detail in Chapter 3, “Infrastructure and Client Devices Used with Wireless Networking.”

Wireless network technology operates at the two lowest layers of the OSI model, Layer 1 (Physical) and Layer 2 (Data Link). However, to some degree Layer 3 (Network) plays a role as well, generally for the TCP/IP protocol capabilities. It is also important to note that wireless networking technology does use all seven layers for certain functionality.

### OSI Model Memorization Tip

One common method you can use to remember the seven layers of the OSI model from top to bottom is to memorize the following sentence: All people seem to need data processing. Take the first letter from each word and that will give you an easy way to remember the first letter that pertains to each layer of the OSI model.

- All (Application)
- People (Presentation)
- Seem (Session)
- To (Transport)
- Need (Network)
- Data (Data Link)
- Processing (Physical)

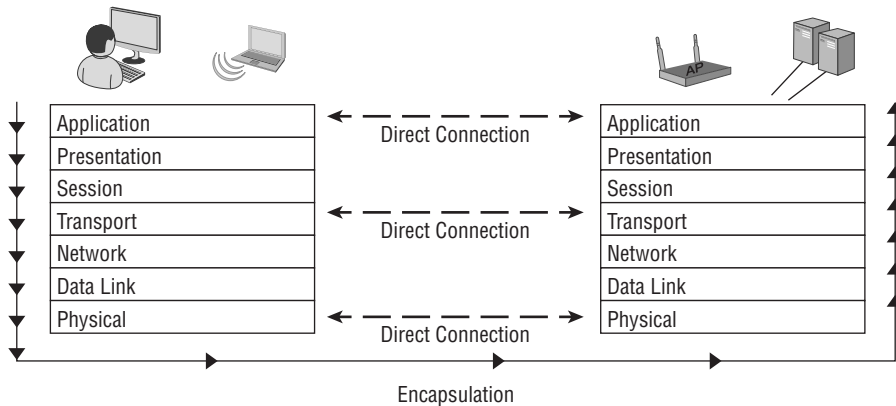
Here’s another one, this time from the bottom layer to the top layer:

- Please (Physical)
- Do (Data Link)
- Not (Network)
- Throw (Transport)
- Sausage (Session)
- Pizza (Presentation)
- Away (Application)

## Peer-Layer Communication

Peer layers communicate with other layers in the OSI model, and the layers underneath are their support systems. Peer-layer communication is the “horizontal” link between devices on the network. Figure 1.18 shows three examples of *peer-layer communication*. Keep in mind, however, that this principle applies to all seven layers of the OSI model. This allows for the layers to communicate with the layer to which a device is sending or receiving information.

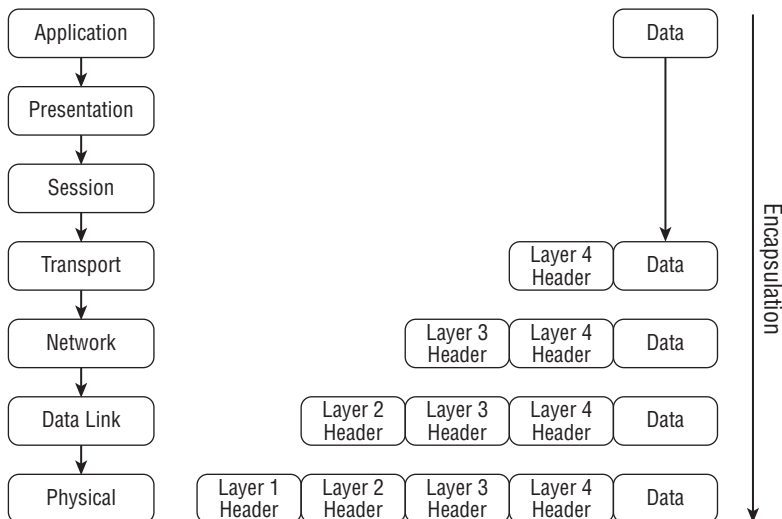
**FIGURE 1.18** Peer communication between three of the seven layers



## Data Encapsulation

The purpose of *encapsulation* is to allow Application layer data communication between two stations on a network using the lower layers as a support system. As data moves down the OSI model from the source to the destination, it is encapsulated. As data moves back up the OSI model from the source to the destination, it is de-encapsulated. Some layers will add a header and/or trailer when information is being transmitted and remove it when information is being received. Encapsulation is the method in which lower layers support upper layers. Figure 1.19 illustrates this process.

**FIGURE 1.19** Information is added at each layer of the OSI model as data moves between devices.



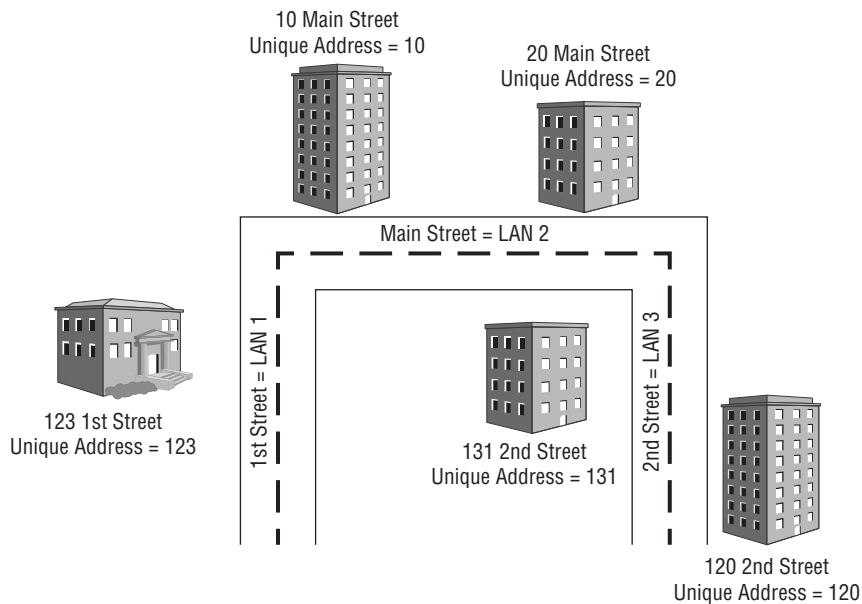
# Device Addressing

Every device on a network requires unique identification. This can be accomplished in a couple of ways:

- Physical addresses
- Logical addresses

The *physical address* of a network adapter is also known as the Media Access Control (MAC) address. As shown in Figure 1.20, every device on a network (like every street address in a city) must have a unique address. The physical address is required in order for a device to send or receive information (data). An analogy to this is sending a package to be delivered via a courier service. Before handing over the package to the courier, you would write the name and physical street address of the recipient on the package. This ensures that the package is delivered correctly to the recipient.

**FIGURE 1.20** The MAC address is analogous to the address of buildings on a street.



The streets shown—1st, Main, and 2nd—represent local area networks.  
The numbers 10, 20, 123, 131, and 120 represent the unique address of each structure on the streets just as MAC addresses would represent devices on a LAN.

The *logical address* is also known as the Internet Protocol (IP) address. Each device on a Layer 3 network or subnet must have a unique IP address (like every city's zip code). The IP address can be mapped to the physical address by using the Address Resolution Protocol (ARP).

The streets shown in Figure 1.20—1st, Main, and 2nd—represent LAN subnets. The street addresses—10, 20, and so on—represent the unique address of each structure on a street as a MAC address would a device on a LAN.

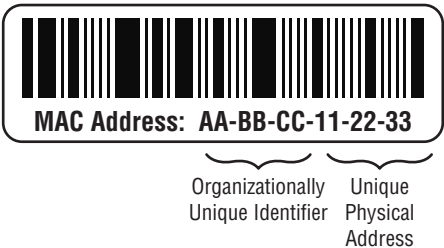
# Physical Addressing

The physical address of a network device is called a MAC address because the *MAC sub-layer* of the Data Link layer handles media access control. The MAC address is a 6-byte (12-character) hexadecimal address in the format AB:CD:EF:12:34:56. The first 3 bytes (or octets) of a MAC address are called the *organizationally unique identifier* (OUI). Some manufacturers produce many network devices and therefore require several OUIs. A table of all OUIs is freely available from the IEEE Standards Association website at

<http://standards.ieee.org/develop/regauth/oui/oui.txt>

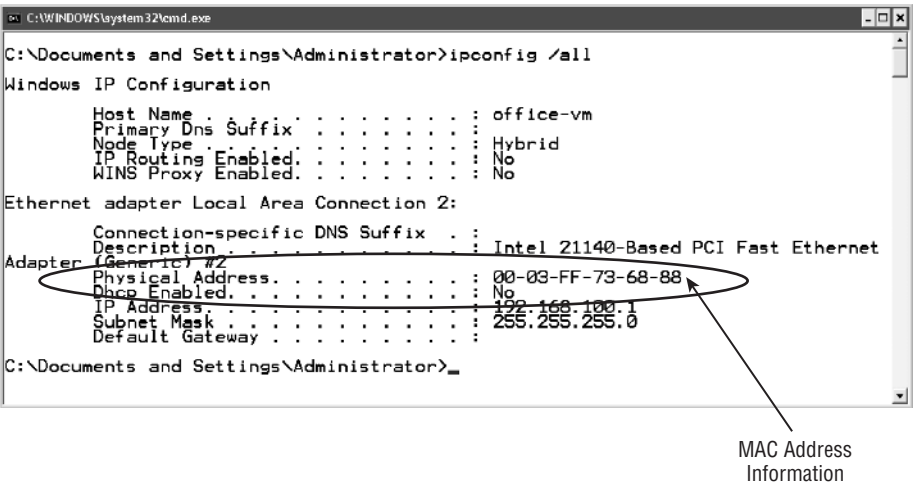
MAC addresses are globally unique; an example is shown in Figure 1.21. The first 3 bytes or octets (6 characters) are issued to manufacturers by the IEEE. The last 3 bytes or octets (6 characters) are incrementally assigned to devices by the manufacturer.

**FIGURE 1.21** Example of a Layer 2 MAC address showing the OUI and unique physical address



The MAC address of a device is usually stamped or printed somewhere on the device. This allows the device to be physically identified by the MAC address. By typing the simple command **ipconfig /all** in the command-line interface of some operating systems, you can view the physical address of the network adapter. Figure 1.22 shows an example of the information displayed by using this command-line utility in the Microsoft Windows operating system.

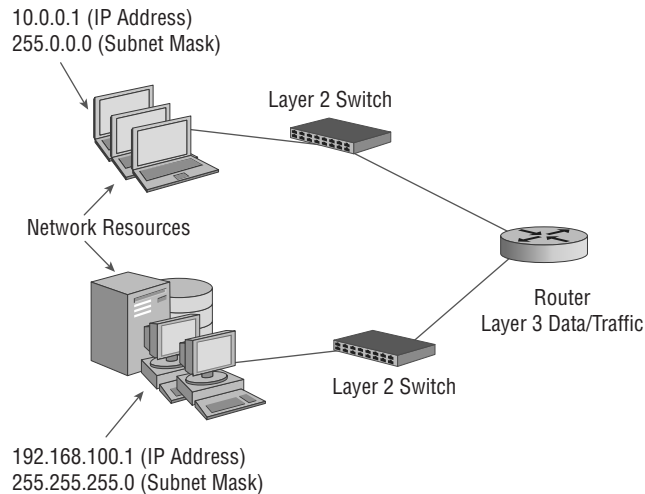
**FIGURE 1.22** The ipconfig command-line utility displaying a physical/MAC address in Microsoft Windows



## Logical Addressing

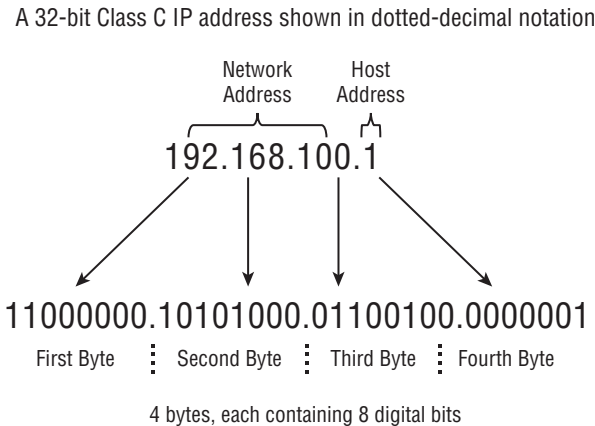
Network devices can also be identified by a logical address, known as the Internet Protocol (IP) address. The Layer 3 IP protocol works with a Layer 4 transport protocol, either User Datagram Protocol (UDP) or Transport layer Protocol (TCP). You learned earlier in this chapter that UDP is a connectionless protocol and using it is analogous to sending a postcard through the mail. The sender has no way of knowing if the card was received by the intended recipient. TCP is a connection-oriented protocol, used for communications analogous to a telephone call, and provides guaranteed delivery of data through acknowledgements. During a telephone conversation, communication between two people will be confirmed to be intact, with the users acknowledging the conversation. Routable logical addresses such as TCP/IP addresses became more popular with the evolution of the Internet and the Hypertext Transfer Protocol (HTTP) that is used with the World Wide Web (WWW) service. IP moves data through an internetwork such as the Internet one router (or hop) at a time. Each router decides where to send the data based on the logical IP address. Figure 1.23 shows a basic network utilizing Layer 3 data traffic.

**FIGURE 1.23** A network with Layer 3 network device logical addressing



Logical addresses (IP addresses) are 32-bit dotted-decimal addresses usually written in the form `www.xxx.yyy.zzz`. Figure 1.24 illustrates an example of a logical Class C, 32-bit IP address. Each of the four parts is a byte, or 8 digital bits. There are two main IP address types: private addresses and public addresses. Private addresses are unique to an internal network, and public addresses are unique to the Internet. These addresses consist of two main parts: the network (subnet) and the host (device). Logical addresses also require a subnet mask and may have a gateway address depending on whether the network is routed. IPv4 addresses fall under three classes: Class A addresses, Class B addresses, and Class C addresses.

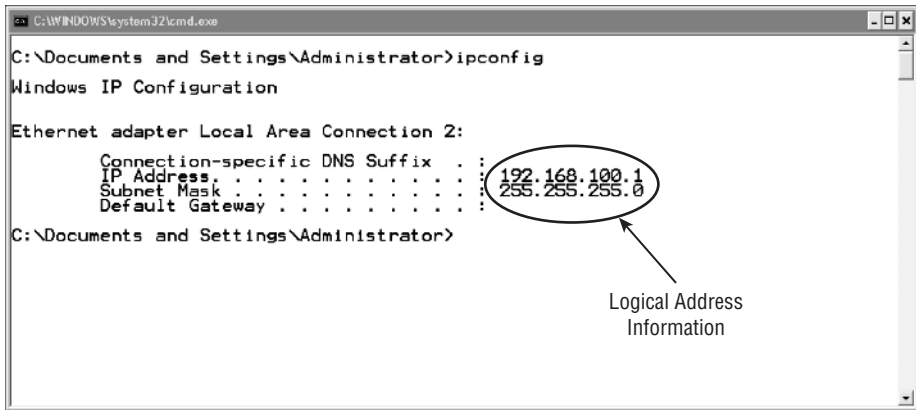
**FIGURE 1.24** Example of a Class C logical IP address



The logical IP addresses you just learned about are known as *IPv4 addresses*. Newer addresses, called *IPv6 addresses*, also exist and are discussed in the following section, “Network Address Translation.”

Unlike a MAC address, an *IP address* is logical and can be either specified as a static address assigned to the device manually by the user or dynamically assigned by a server. However, the same command-line utility used to identify the physical address of a device can be used to identify the logical address of a device. Typing **ipconfig** at a command prompt displays the logical address, including the IP address, subnet mask, and default gateway (router) of the device. The `ipconfig /all` command, illustrated earlier in the chapter, yields additional information, including the physical or MAC address of the device’s network adapter. This command is for a computer using the Microsoft Windows operating system. For some Apple and Linux devices, the `ifconfig` command will yield similar information. Figure 1.25 shows the `ipconfig` utility displaying the logical address information, including the IP address and subnet mask.

**FIGURE 1.25** The Microsoft Windows `ipconfig` command-line utility showing logical address information





In Exercise 1.1, you will use the `ipconfig` utility from a command prompt on a computer using the Microsoft Windows operating system. This will allow you to see the address information for any available network adapters within the device.



Exercise 1.1 was written using a computer with the Microsoft Windows 10 operating system. If you're using a different version of the operating system, the steps may vary slightly. Keep in mind that there are many different shortcuts and ways to get to a command prompt in the Microsoft operating systems. The steps in this exercise use one common method.

## EXERCISE 1.1

### Viewing Device Address Information on a Computer

1. Click the Start menu.
2. Click the All Apps icon near the bottom of the menu.
3. Navigate to and click the Windows System folder.
4. Click the Command Prompt. The command window will appear.
5. In the command window, type `ipconfig /all`.
6. View the results in the command window. Notice the physical address of the network adapter as well as other information. The results should look similar to that shown here for Microsoft Windows 10 but may vary slightly based on the OS version in use.

```

C:\WINDOWS\system32\cmd.exe
C:\Documents and Settings\Administrator>ipconfig /all
Windows IP Configuration

    Host Name . . . . . : office-vm
    Primary Dns Suffix . . . . . : 
    Node Type . . . . . : Hybrid
    IP Routing Enabled . . . . . : No
    WINS Proxy Enabled . . . . . : No

Ethernet adapter Local Area Connection 2:

    Connection-specific DNS Suffix . : 
    Description . . . . . : Intel 21140-Based PCI Fast Ethernet
    Adapter (Generic) #2
    Physical Address. . . . . : 00-03-FF-73-68-88
    Dhcp Enabled . . . . . : No
    IP Address. . . . . : 192.168.100.1
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 

C:\Documents and Settings\Administrator>
  
```

## Network Address Translation

In the mid-1990s, the use of the Internet along with the TCP/IP protocols was fueled by the release of the Hypertext Transfer Protocol (HTTP) and the World Wide Web. The heavily used Internet Protocol version 4 (IPv4) of assigning IP addresses was in jeopardy because

of the increased use of TCP/IP networks. Because the IPv4 mechanism has a finite number of addresses, there was a possibility of running out of IP addresses. Table 1.1 shows the number of IPv4 addresses available based on the IP address class.

**TABLE 1.1** IPv4 IP addresses

Class Type	1st Octet – Decimal	Max Number of Hosts
A	1–126	16,777,214
B	128–191	65,534
C	192–223	254

Newer technology, Internet Protocol version 6 (IPv6), was the answer to the IPv4 address limitation issue. As you learned earlier in this chapter, IPv4 uses 32-bit binary addresses; there is a limit to the number of possible public addresses, as shown in Table 1.1. Keep in mind that all the Class A addresses were reserved by organizations and companies early on and therefore not available to the general public. The IPv6 method of addressing new IP technology is what was going to solve the problem of IP address exhaustion. IPv6 uses 128 bits ( $2^{128}$ ), which equates to a potential  $3.4 \times 10^{38}$  IP addresses. That's a lot of IP addresses. The switch to IPv6 would not be an easy task. Computer operating systems, servers, and network infrastructure hardware lacked support for IPv6, causing delays in the implementation.

So why all this discussion about IP addresses or potential lack thereof? Well, this is where *Network Address Translation* (NAT) technology comes into action. NAT allows the use of a *private* IP address network for internal use and mapping it to a single *public* IP address connected to the Internet. This is accomplished by modifying the header in the IPv4 packet, which is where the term *address translation* comes in. NAT allows for a home network, a very small organization, or even a very large organization to be represented by a single public IP address on the Internet. It is addressed in RFC 2663 and allowed for the continued use of IPv4 addresses. NAT consists of different implementations. The following are two common implementations:

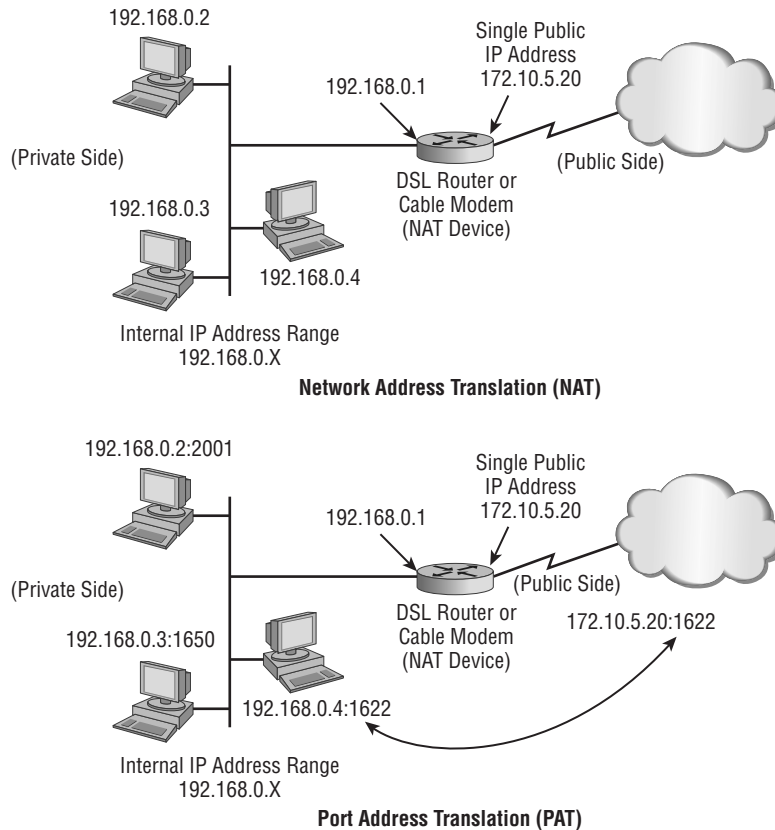
- One-to-one NAT
- One-to-many NAT

One-to-one NAT will map an IP address on the outside to an IP address on the inside. This can be accomplished through either a static assignment or a dynamic assignment. The static NAT entry is a permanent entry and needs to change manually. The dynamic process is useful when there are a limited number of addresses and the one-to-one assignment occurs when needed.

One-to-many NAT allows for the translation of one single public IP address on the outside of a network to service many devices with private IP addresses on the inside network.

This is accomplished by modifying the information in the IP packet. Figure 1.26 shows how NAT on a DSL router or cable modem will provide IP address translation. Notice that the private IP addresses on the private side of the router in this example are in the 192.168.0.X range. These private IP addresses will be translated to the single public IP address 172.10.5.20 on the public-facing side.

**FIGURE 1.26** Network Address Translation (NAT) and Port Address Translation (PAT). The IP addresses shown are examples.



## Summary

This chapter provided a simple review of computer networking topics. It began with an outline of the common network technology types:

- Local area networks (LANs)
- Wide area networks (WANs)

- Metropolitan area networks (MANs)
- Campus area networks (CANs)
- Personal area networks (PANs)

The next fundamental networking concept discussed was computer network topologies. You learned about network topologies ranging from the legacy high-speed linear bus and ring to the current star topology, the most common topology used today with both wired and wireless networks. You looked at the following various topologies:

- Bus
- Ring
- Star
- Mesh
- Ad hoc
- Point-to-point
- Point-to-multipoint

You then reviewed the basics and different layers of the OSI model, including a brief overview of each layer illustrating the different protocols and sublayers where applicable. Then the chapter discussed the basics of peer communications and data encapsulation.

The chapter's final topic was device addressing. You explored the concepts of physical (MAC sublayer) and logical (Network layer) addressing, including the IP address and subnet mask. A simple exercise using a computer with the Microsoft Windows operating system showed how to view device addressing information.

## Exam Essentials

**Understand the components of a local area network (LAN).** A LAN is a group of computers connected by a physical medium in a specific arrangement called a topology.

**Know the different types of networks.** The basic networks types are LAN, WAN, CAN, MAN, and PAN.

**Become familiar with various networking topologies.** Bus, star, ring, mesh, and ad hoc are some of the topologies used in computer networking. Bus is considered a legacy topology, whereas star is one of the most common topologies in use today.

**Understand point-to-point and point-to-multipoint connections.** These connect two or more LANs and can consist of both wired and wireless connections.

**Understand the basics of the OSI model.** Know that each of the seven layers of the OSI model serves a specific function.

**Remember the details of the lower two layers of the OSI model.** The Physical layer and Data Link layer are the two lowest layers of the OSI model. Wireless networking technology operates at these layers. The Data Link layer consists of two sublayers: the Logical Link Control (LLC) sublayer and the Media Access Control (MAC) sublayer. The Physical Layer consists of two sublayers: the Physical Layer Convergence Protocol (PLCP) sublayer and the Physical Medium Dependent (PMD) sublayer.

**Understand device addressing.** Devices are assigned a unique physical address by the manufacturer. This address is known as the MAC address. MAC addresses consist of two parts, the organizationally unique identifier (OUI) and the unique physical address. A logical address may also be assigned at the Network layer to identify devices on different inter-networks using the Internet Protocol (IP).

## Review Questions

1. At which two layers of the OSI model does wireless LAN technology operate? (Choose two.)
  - A. Session
  - B. Network
  - C. Physical
  - D. Application
  - E. Data Link
2. A high-speed linear topology is defined as a \_\_\_\_\_.
  - A. Ring
  - B. Mesh
  - C. Bus
  - D. Star
3. The lower three layers of the OSI model are the \_\_\_\_\_, \_\_\_\_\_ and the \_\_\_\_\_.
  - A. Data Link, Physical, Transport
  - B. Physical, Data Link, Network
  - C. Session, Physical, Application
  - D. Application, Presentation, Session
4. The IP address of a network adapter is also known as which address?
  - A. MAC address
  - B. Logical address
  - C. Layer 4 address
  - D. Mesh address
5. Which layer of the OSI model is responsible for organizing bit-level data for communication between devices on a network and detecting and correcting Physical layer errors?
  - A. Application
  - B. Transport
  - C. Network
  - D. Data Link
  - E. Physical
6. Which layer of the OSI model is responsible for addressing and routing?
  - A. Physical
  - B. Network
  - C. Transport
  - D. Application

7. \_\_\_\_\_ allows for Application layer data communication between two stations using lower layers as a support system.
- A. Logical addressing
  - B. Physical addressing
  - C. Data encapsulation
  - D. Peer communication
  - E. Point-to-point
8. Which topology may use a token-passing access method?
- A. Ring
  - B. Mesh
  - C. Bus
  - D. Star
9. Which layer of the OSI model provides an interface to the user?
- A. Physical
  - B. Network
  - C. Transport
  - D. Application
  - E. Data Link
  - F. Presentation
10. The physical address of a network adapter is the \_\_\_\_\_.
- A. MAC address
  - B. Logical address
  - C. Layer 3 address
  - D. Mesh address
11. The term encapsulation means to \_\_\_\_\_.
- A. Add an IP address to a network adapter
  - B. Add a MAC address to a network adapter
  - C. Add topology information to a frame
  - D. Add layer header and trailer information to a frame
12. Which of the following is an accurate description of peer communication?
- A. The horizontal link between devices on the network
  - B. The vertical link between devices on the network
  - C. The logical link between devices on the network
  - D. The physical link between devices on the network

13. Physical addresses on a network device are responsible for which of the following?
  - A. To identify the logical location on the network
  - B. To identify which device should receive the information
  - C. To identify the routing information on the network
  - D. To identify the protocol in use on the network
14. At which layer of the OSI model are bits compiled into frames?
  - A. Physical
  - B. Data Link
  - C. Network
  - D. Transport
  - E. Application
15. Which protocol is used to guarantee delivery of data?
  - A. UDP
  - B. IP
  - C. ARP
  - D. TCP
  - E. HTTP
16. Which protocol is responsible for addressing and routing?
  - A. IP
  - B. TCP
  - C. UDP
  - D. ARP
17. Which layer of the OSI model allows physical addresses to be converted to logical addresses?
  - A. Application
  - B. Session
  - C. Transport
  - D. Network
  - E. Data Link
18. The Data Link layer of the OSI model is divided into which two sublayers?
  - A. PLCP, PMD
  - B. LLC, MAC
  - C. TCP, UDP
  - D. HTTP, FTP



- 19.** Which layer of the OSI model uses physical addresses to deliver data to the destination?
- A.** Physical
  - B.** Data Link
  - C.** Network
  - D.** Transport
- 20.** Which is a valid logical IPv4 address?
- A.** 255.255.0.0
  - B.** 192.168.200.1
  - C.** AB.CD.EF12.34.56
  - D.** 12.34.56.AB.CD.EF

