CHAPTER 17

Networking Essentials

In this chapter, you will learn:

- About hardware devices used for networking
- About the different types of networks
- About the protocols and standards Windows uses for networking
- How to connect a computer to a network
- About troubleshooting tools and tips for network connections

In this chapter, you'll learn about the technologies and hardware used to build networks, and how Windows supports and manages a network connection, including how computers are identified and addressed on a network. You'll also learn to connect a computer to a network and what to do when that connection gives problems. In the next chapter, you'll learn how to set up, configure, and support a small network.

The focus in this and the next chapter is to prepare you so that you can assume total responsibility for supporting both wired and wireless networks in a small-office-home-office (SOHO) environment. Consider this chapter the introductory chapter toward that end.

A+ Exam Tip All the content in this chapter applies toward the networking objectives of the A+ 220-701 Essentials exam. The A+ 220-702 Practical Application exam networking objectives are covered in the next chapter. The A+ 220-701 Essentials exam expects you to know about networking terms, concepts, protocols, and hardware, and to know how to connect a computer to an existing network.

NETWORKING TECHNOLOGIES

A+
220-701
4.1
4.3

A computer network is created when two or more computers can communicate with each other. Networks can be categorized by several methods, including the technology used and the size of the network. When networks are categorized by size or physical area they cover, these are the categories used:

- *PAN*. A **PAN (personal area network)** consists of personal devices at close range such as a cell phone, PDA, and notebook computer in communication. PANs can use wired connections (such as USB or FireWire) or wireless connections (such as Bluetooth or infrared).
- *LAN*. A **LAN (local area network)** covers a small local area such as a home, office, other building, or small group of buildings. LANs can use wired (most likely Ethernet) or wireless (most likely 802.11, also called Wi-Fi) technologies. A LAN is used for workstations, servers, printers, and other devices to communicate and share resources.
- *Wireless LAN*. A **wireless LAN (WLAN)** covers a limited geographical area, and is popular in places where networking cables are difficult to install, such as outdoors, in public places, and in homes that are not wired for networks. They are also useful in hotel rooms.
- *MAN*. A **MAN (metropolitan area network)** covers a large campus or city. (A small MAN is sometimes called a CAN or campus area network.) Newer technologies used are wireless and Ethernet with fiber-optic cabling. Older technologies used are ATM and FDDI.
- *WAN*. A **WAN (wide area network)** covers a large geographical area and is made up of many smaller networks. The best-known WAN is the Internet. Some technologies used to connect a single computer or LAN to the Internet include DSL, cable modem, satellite, cellular WAN, and fiber optic.

A+ Exam Tip The A+ 220-701 Essentials exam expects you to know about a LAN and a WAN.

Networks are built using one or more technologies that provide varying degrees of bandwidth. **Bandwidth** (the width of the band) is the theoretical number of bits that can be transmitted over a network at one time, similar to the number of lanes on a highway. In practice, however, the networking industry refers to bandwidth as a measure of the maximum rate of data transmission in bits per second (bps), thousands of bits per second (Kbps), millions of bits per second (Mbps), or billions of bits per second (Gpbs). Bandwidth is the theoretical or potential speed of a network, whereas **data throughput** is the actual speed. In practice, network transmissions experience delays that result in slower network performance. These delays in network transmissions are called **latency**. Latency is measured by the round-trip time it takes for a data packet to travel from source to destination and back to source.

In this chapter, we focus on network technologies used for a local network (LAN) and those used to connect to the Internet. To connect to the Internet, a network first connects to an **Internet Service Provider (ISP)**, such as Earthlink or Comcast (see Figure 17-1). When connecting to an ISP, know that upload speeds are generally slower than download speeds. These rates differ because users generally download more data than they upload. Therefore, an ISP devotes more of the available bandwidth to downloading and less of it to uploading.

A+
220-701
4.1
4.3

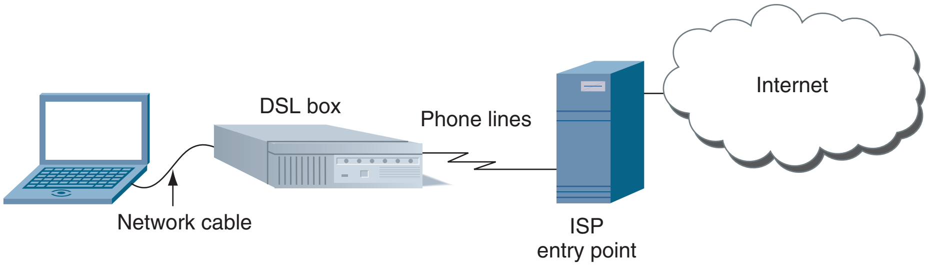


Figure 17-1 Use an ISP to connect to the Internet
Courtesy: Course Technology/Cengage Learning

Table 17-1 lists network technologies, their speeds, and their uses. Older technologies no longer widely used and not listed in the table include X.25, Frame Relay, ISDN, Token Ring, FDDI, and ATM. The table is more or less ordered from slowest to fastest maximum bandwidth, although latency can affect the actual bandwidth of a particular network.

Technology	Maximum Speeds	Common Uses
Wireless Networks		
Bluetooth 2.0 (BT2)	Up to 2 Mbps	Short-range wireless technology used for a PAN (personal area network).
GSM mobile phone service	Up to 3 Mbps	Cellular wireless technology used for voice and data transmissions over mobile phones; first became popular in Europe.
CDMA mobile phone service	Up to 3 Mbps	Cellular wireless technology used for mobile phones; losing popularity.
G3 mobile phone service	Up to 2.4 Mbps	Cellular mobile phone technology allows for transmitting data, video, and text.
Wi-Fi 802.11b wireless	Up to 11 Mbps	First 802.11 standard that was widely used, but is being replaced by 802.11g and n.
Bluetooth 3.0 (BT3)	Up to 24 Mbps	Latest Bluetooth standard just released that is not yet available in devices.
Wi-Fi 802.11a wireless	Up to 54 Mbps	Shorter range than 802.11b, but faster.
Wi-Fi 802.11g wireless	Up to 54 Mbps	Compatible with and replacing 802.11b.
802.16 wireless (WiMAX)	Up to 75 Mbps	Offers ranges up to 6 miles.
802.11n wireless	Up to 160 Mbps	Latest Wi-Fi technology.
Wired Networks		
Dial-up or regular telephone (POTS, for plain old telephone service)	Up to 56 Kbps	Slow access to an ISP using a modem and dial-up connection.
SDSL (Symmetric Digital Subscriber Line)	Up to 2.3 Mbps	Equal bandwidths in both directions. SDSL is a type of broadband technology. (**Broadband** refers to a networking technology that carries more than one type of signal, such as DSL and telephone.)

Table 17-1 Networking technologies (continued)

A+
220-701
4.1
4.3

Technology	Maximum Speeds	Common Uses
ADSL (Asymmetric DSL)	640 Kbps upstream and up to 8 Mbps downstream	Most bandwidth is from ISP to user. Slower versions of ADSL are called ADSL Lite or DSL Lite. ISP customers pay according to a bandwidth scale.
Ethernet	10 Mbps	Slowest Ethernet network, replaced by Fast Ethernet. Variations of Ethernet are used for almost all local networks.
Cable modem	4 to 16 Mbps, depends on the type of cable used	Connects a home or small business to an ISP; is usually purchased with a cable television subscription. Cable modem is a type of broadband technology that is used in conjunction with television on the same cable. Fiber-optic cable gives highest speeds.
Dedicated line using fiber optic	Up to 20 Mbps upstream and 50 Mbps downstream	Dedicated line from ISP to business or home. Speeds vary with price.
T3	45 Mbps	Dedicated lines used by large companies that require a lot of bandwidth and transmit extensive amounts of data.
VDSL (very-high-bit-rate DSL)	Up to 52 Mbps	This latest version of DSL is asymmetric DSL that works only a short distance.
Fast Ethernet	100 Mbps	Used for local networks.
Gigabit Ethernet	1 Gbps	Fastest Ethernet standard for a local network.
10-gigabit Ethernet	10 Gbps	Newest Ethernet standard expected to largely replace SONET, OC, and ATM because of its speed, simplicity, and lower cost.
OC-1, OC-3, OC-24, up to OC-3072	52 Mbps, 155 Mbps, 1.23 Gbps, 160 Gbps	Optical Carrier levels (OCx) used for Internet backbones; they use fiber-optic cabling.
SONET (Synchronous Optical Network)	Up to 160 Gbps	Major backbones built using fiber-optic cabling make use of different OC levels.

Table 17-1 Networking technologies

A+ Exam Tip The A+ 220-701 Essentials exam expect you to be able to compare and contrast these network types: Dial-up, DSL, cable, satellite, fiber, 802.11, Bluetooth, and cellular.

Notes The **Institute of Electrical and Electronics Engineers (IEEE)** creates standards for computer and electronics industries. Of those standards, IEEE 802 applies to networking. For example, IEEE 802.2 describes the standard for Logical Link Control, which defines how networks that use different protocols communicate with each other. (Remember that protocols are rules for communication.) For more information on the IEEE 802 standards, see the IEEE Web site, *www.ieee.org*.

A+
220-701
4.1
4.3

When two devices on a network communicate, they must use the same protocols, so that the communication makes sense. For almost all networks today, including the Internet, the protocol used is called TCP/IP (Transmission Control Protocol/Internet Protocol). TCP/IP is actually a group of protocols that control many different aspects of communication. Before data is transmitted on a network, it is first broken up into segments. Each data segment is put into a packet with information about the packet put at the beginning and the end of the data. This information identifies the type of data, where it came from, and where it's going. Information at the beginning of the data is called a header, and information at the end of the data is called a trailer. If the data to be sent is large, it is first divided into several packets, each small enough to travel on the network.

A+ Tip The A+ 220-701 Essentials exam expects you to be familiar with many networking terms. This chapter is full of key terms you need to know for the exam.

You can connect a computer or LAN to the Internet using a broadband, wireless, or dial-up connection. Now let's look at some of the important details of each type of connection.

BROADBAND TECHNOLOGIES

Broadband technologies used to connect to the Internet are cable modem, DSL, fiber-optic, satellite and ISDN. ISDN (Integrated Services Digital Network) is an outdated broadband technology developed in the 1980s that uses regular phone lines, and is accessed by a dial-up connection. In most areas of the country, cable modem and DSL compete as the two most popular ways to connect to the Internet. Let's first compare these two technologies and then we'll look at satellite and fiber-optic dedicated lines.

COMPARE CABLE MODEM AND DSL

Cable modem and DSL are the two most popular ways to connect to the Internet.

- Cable modem communication uses cable lines that already exist in millions of households. Just as with cable TV, cable modems are always connected (always up). With a cable modem, the TV signal to your television and the data signals to your PC share the same coax cable. Just like a dial-up modem, a cable modem converts a PC's digital signals to analog when sending them and converts incoming analog data to digital.
- DSL (Digital Subscriber Line) is a group of broadband technologies that covers a wide range of speeds. DSL uses ordinary copper phone lines and a range of frequencies on the copper wire that are not used by voice, making it possible for you to use the same phone line for voice and DSL at the same time. When you make a regular phone call, you dial in as usual. However, the DSL part of the line is always connected (always up) for most DSL services. A few DSL services offer the option to connect on demand. For these services, a username and passcode are sent to the ISP when making a connection. Asymmetric DSL (ADSL) uses one upload speed from the consumer to an ISP and a faster download speed. Symmetric DSL (SDSL) uses equal bandwidths in both directions.

A+
220-701
4.1
4.3

Here are some important similarities and differences between cable modem and DSL:

- Both cable modem and DSL can sometimes be purchased on a sliding scale, depending on the bandwidth you want to buy. Subscriptions offer residential and the more-expensive business plans. Business plans are likely to have increased bandwidth and better support when problems arise.
- With cable modem, you share the TV cable infrastructure with your neighbors, which can result in service becoming degraded if many people in your neighborhood are using cable modem at the same time. I once used cable modem in a neighborhood where I found I needed to avoid Web surfing between 5:00 and 7:00 p.m. when folks were just coming in from work and using the Internet. With DSL, you're using a dedicated phone line, so your neighbors' surfing habits are not important.
- With DSL, static over phone lines in your house can be a problem. The DSL company provides filters to install at each phone jack (see Figure 17-2), but still the problem might not be fully solved. Also, your phone line must qualify for DSL; some lines are too dirty (too much static or noise) to support DSL.

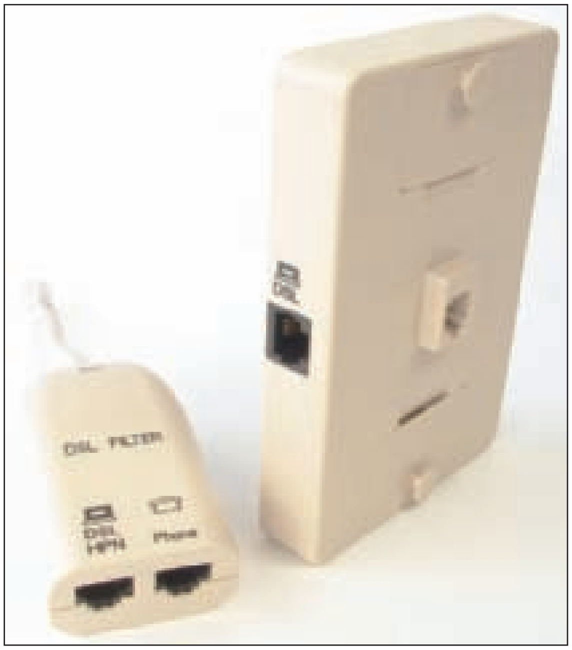


Figure 17-2 When DSL is used in your home, filters are needed on every phone jack except the one used by the DSL modem
Courtesy: Course Technology/Cengage Learning

- Setup of cable modem and DSL works about the same way, using either a cable modem box or a DSL box for the interface between the broadband jack (TV jack or phone jack) and the PC. Figure 17-3 shows the setup for a cable modem connection using a network cable between the cable modem and the PC.
- With either installation, in most cases, you can have the cable modem or DSL provider do the entire installation for you at an additional cost. A service technician comes to your home, installs all equipment, including a network card if necessary, and configures your PC to use the service.

A+
220-701
4.1
4.3

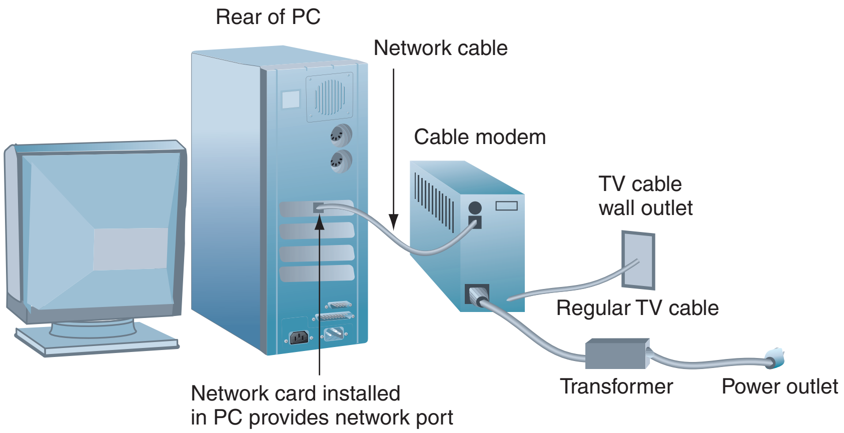


Figure 17-3 Cable modem connecting to a PC through a network card installed in the PC
Courtesy: Course Technology/Cengage Learning

- In most cases, cable modem and DSL use a network port or a USB port on the PC to connect to the cable modem or DSL box. A DSL box is shown in Figure 17-4.

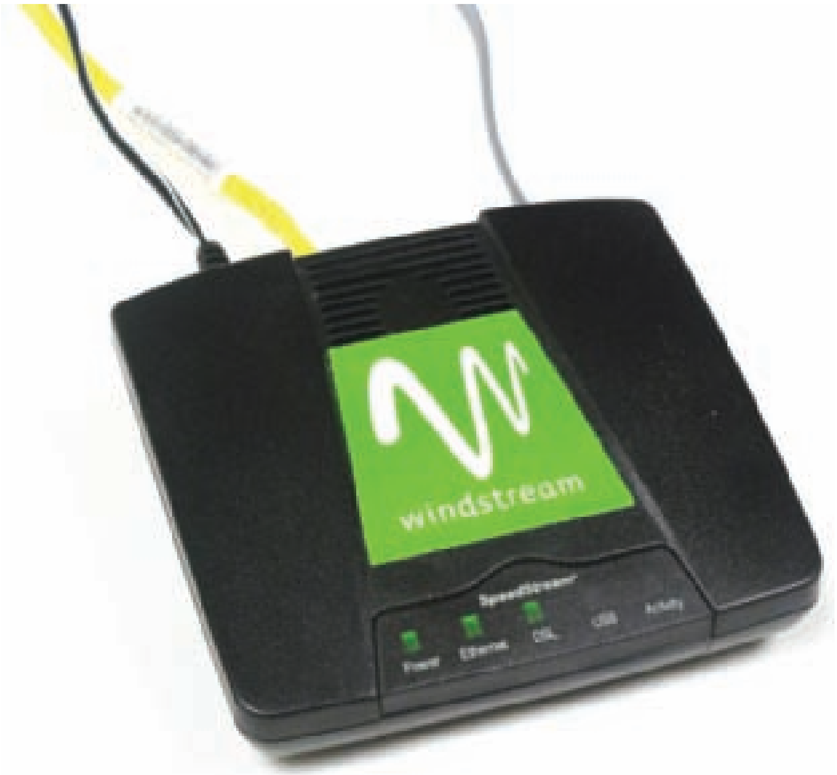


Figure 17-4 This DSL box connects to a phone jack and a PC to provide a broadband connection to an ISP
Courtesy: Course Technology/Cengage Learning

SATELLITE

People who live in remote areas and want high-speed Internet connections often are limited in their choices. DSL and cable modem options might not be available where they live, but satellite access is available from pretty much anywhere. Internet access by

A+
220-701
4.1
4.3

satellite is available even on airplanes. Passengers can connect to the Internet using a wireless hotspot and satellite dish on the plane. A satellite dish mounted on top of your house or office building communicates with a satellite used by an ISP offering the satellite service (see Figure 17-5). One disadvantage of using satellite for an Internet connection is that it experiences delays in transmission (called latency), especially when uploading, more so than DSL or cable modem.

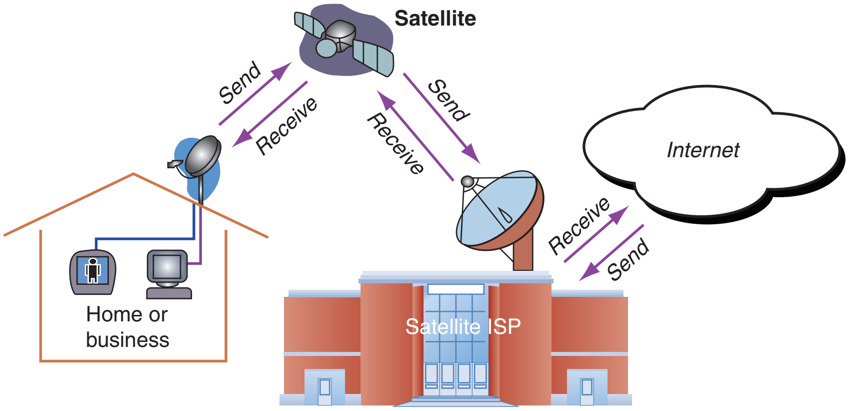


Figure 17-5 Communication by satellite can include television and Internet access
Courtesy: Course Technology/Cengage Learning

DEDICATED LINE USING FIBER OPTIC

Another broadband technology used for Internet access is **fiber optic**. The technology uses a dedicated line from your ISP to your place of business or residence. This dedicated line is called a point-to-point (PTP) connection because no other business or residence shares the line with you. Many types of cabling can be used for dedicated lines, but fiber-optic cabling is becoming popular. Television, Internet data, and voice communication all share the broadband **fiber-optic cable**. Verizon calls the technology FiOS (Fiber Optic Service), and the fiber-optic cabling is used all the way from the ISP to your home. Other providers might provide fiber-optic cabling up to your neighborhood and then use coaxial cable (similar to that used in cable modem connections) for the last leg of the connection to your business or residence. Upstream and downstream speeds and prices vary.

WIRELESS TECHNOLOGIES

Wireless networks, as the name implies, use radio waves or infrared light instead of cables or wires to connect computers or other devices. Although wireless networks have some obvious advantages in places where running cables would be difficult or overly expensive, wireless networks tend to be slower than wired networks, especially when they are busy. Another problem with wireless networks is security.

Now let’s look at some details of several wireless technologies used to connect two devices or connect to a local network or to the Internet, including Wi-Fi, WiMAX, cellular, and Bluetooth. One other wireless technology that you need to be aware of is infrared, which is discussed in Chapter 9.

A+
220-701
4.1
4.3
5.2

WI-FI OR 802.11 WIRELESS

By far, the most popular technology for wireless local networks is IEEE 802.11, first published in 1990. These standards are also called **Wi-Fi (Wireless Fidelity)**. Most wireless devices today support three IEEE standards; look for **802.11b/g/n** on the packages. Several IEEE 802.11 standards are listed below:

- *802.11g and 802.11b*. These two standards use a frequency range of 2.4 GHz in the radio band and have a distance range of about 100 meters. 802.11b/g has the disadvantage that many cordless phones use the 2.4-GHz frequency range and cause network interference. 802.11g runs at 54 Mbps and 802.11b runs at 11 Mbps. Apple Computer calls 802.11b **AirPort**, and it calls 802.11g AirPort Extreme.
- *802.11n*. This latest Wi-Fi standard uses **multiple input/multiple output (MIMO)** technology whereby two or more antennas are used at both ends of transmission. 802.11n can use the 2.4 GHz range and be compatible with 802.11b/g, or it can use the 5.0 GHz range and be compatible with the older 802.11a standard. Figure 17-6 shows an 802.11b/g/n network adapter. Speeds of up to 600 Mbps are possible with 802.11n.
- *802.11a*. This standard is no longer widely used. It works in the 5.0-GHz frequency range and is, therefore, not compatible with 802.11b/g. It has a shorter range from a wireless device to an access point (50 meters compared with 100 meters for 802.11b/g), supports 54 Mbps, and does not encounter interference from cordless phones, microwave ovens, and Bluetooth devices, as does 802.11b/g.

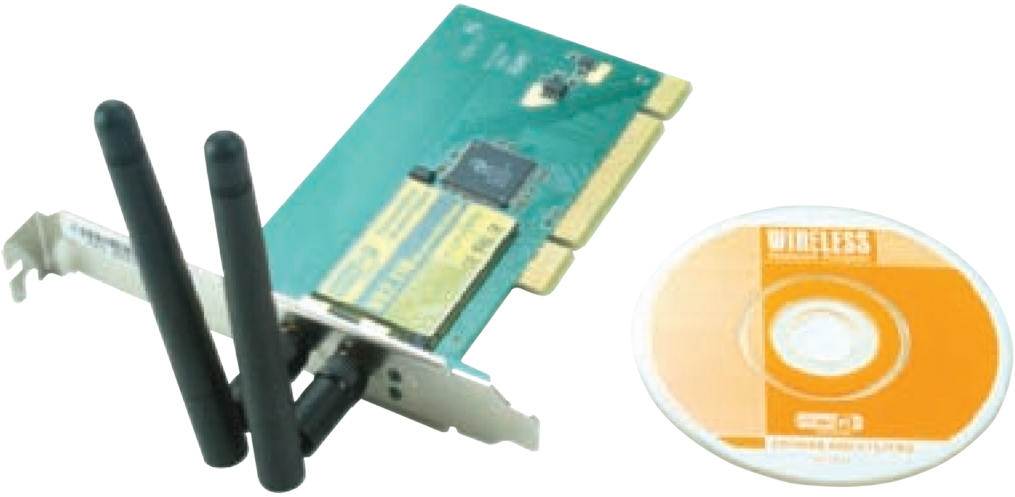


Figure 17-6 Wireless network adapter supports 802.11g/b/n
Courtesy: Course Technology/Cengage Learning

- *802.11k and 802.11r*. These two standards were designed to help manage connections between wireless devices and access points. Normally, if a wireless device senses more than one access point, by default, it connects to the access point with the strongest signal, which can cause an overload on some access points while other access points are idle. The 802.11k standard defines how wireless network traffic can better be distributed over multiple access points covering a wide area so that the access point with the strongest signal is not overloaded. The 802.11r standard defines how a mobile wireless device can easily and quickly transition as it moves out of range of one access point and into the range of another.

A+
220-701
4.1
4.3
5.2

- *802.11d.* This standard is designed to run in countries outside the United States where other 802.11 versions do not meet the legal requirements for radio band technologies.

Wireless LANs are so convenient for us at work and at home, but the downside of having a wireless network is that if we don't have the proper security in place, anyone with a wireless computer within range of our access point can use the network—and, if they know how, can intercept and read all the data sent across the network. They might even be able to hack into our computers by using our own wireless network against us. For all these reasons, it's terribly important to secure a wireless network.

A+ Exam Tip The A+ 220-701 Essentials exam expects you to be familiar with wireless encryption, including WEPx, WPAx, and client configuration (SSID).

Securing a wireless network is generally done in three ways:

- ***Method 1: Data encryption***—Data sent over a wireless connection can be encrypted. The three main protocols for encryption for 802.11 wireless networks are **WEP (Wired Equivalent Privacy)**, **WPA (Wi-Fi Protected Access)**, and **WPA2 (Wi-Fi Protected Access 2)**. With any of these protocols, data is encrypted using a firmware program on the wireless device and is only encrypted while the data is wireless; the data is decrypted before placing it on the wired network. With WEP encryption, data is encrypted using either 64-bit or 128-bit encryption keys. (Because the user can configure only 40 bits of the 64 bits, 64-bit WEP encryption is sometimes called 40-bit WEP encryption.) WEP was first defined by 802.11b. Because the key used for encryption is static (it doesn't change), a hacker can easily decrypt the code and read WEP-encrypted data. Therefore, WEP encryption is no longer considered secure. WPA encryption, also called TKIP (Temporal Key Integrity Protocol) encryption, is stronger than WEP and was designed to replace it. With WPA encryption, encryption keys are changed at set intervals. The latest and best wireless encryption standard is WPA2, also called the 802.11i standard or AES (Advanced Encryption Standard). When buying wireless devices, be sure the encryption methods used are compatible! When connecting to a wireless network that is using WEP or WPA encryption, you must enter the passphrase or key that is used to encrypt the data.
- ***Method 2: Disable SSID broadcasting***—The name of the wireless access point is called the **Service Set Identifier (SSID)**. Normally, the SSID is broadcast so that anyone with a wireless computer can see the name and use the network. If you hide the SSID, a computer can see the wireless network, but can't use it unless the SSID is known. Best practice when hiding the SSID is to also change the default name so that it cannot easily be guessed. Disabling SSID broadcasting is normally not used when data encryption is used. When you attempt to connect to a network that declares itself an "Unnamed Network," you are given the opportunity to enter the SSID to complete the connection.
- ***Method 3: Filter MAC addresses***—A wireless access point can filter the MAC addresses of wireless NICs that are allowed to use the access point. A MAC (Media Access Control) address is a 6-byte number that uniquely identifies a network adapter on a computer. This type of security prevents uninvited guests from using the wireless LAN, but does not prevent others from receiving data in the air. Also, knowledgeable users can hack through MAC address filtering, and it is, therefore, considered a weak security measure. To connect to a wireless network that is set to filter MAC addresses, the administrator of the network must enter the MAC address of your wireless network adapter in the table of MAC addresses that are allowed to use the network.

A+
220-701
4.1
4.3

WIMAX OR 802.16 WIRELESS

A newer IEEE wireless standard is WiMAX, which is defined under IEEE 802.16d and 802.16e. WiMAX supports up to 75 Mbps with a range up to several miles and uses 2- to 11-GHz frequency. The WiMAX range in miles depends on many factors. For a wide-area network, WiMAX cellular towers are generally placed 1.5 miles apart to assure complete coverage. WiMAX is used in wide-area public hot spots and as a wireless broadband solution for business and residential use. It is often used as a last-mile solution for DSL and cable modem technologies, which means that the DSL or cable connection goes into a central point in an area, and WiMAX is used for the final leg to the consumer.

Notes For more information on Wi-Fi, see *www.wi-fi.org*, and for more information on AirPort, see *www.apple.com*. For information on Bluetooth, see *www.bluetooth.com*. For information on WiMAX, see *www.wimaxforum.org*.

CELLULAR WAN

A **cellular network** or **cellular WAN** can be used when a wireless network must cover a wide area. The network consists of cells and each cell is controlled by a base station (see Figure 17-7). The **base station** is a fixed transceiver and antenna. WiMAX is sometimes used to build a cellular network, but the most common type of cellular networks are cell phone networks. Cell phones are called that because they use a cellular network.

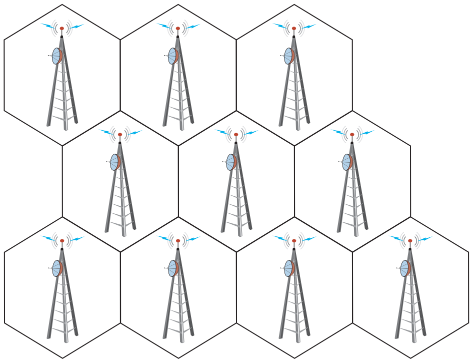


Figure 17-7 A cellular WAN is made up of many cells that provide coverage over a wide area
Courtesy: Course Technology/Cengage Learning

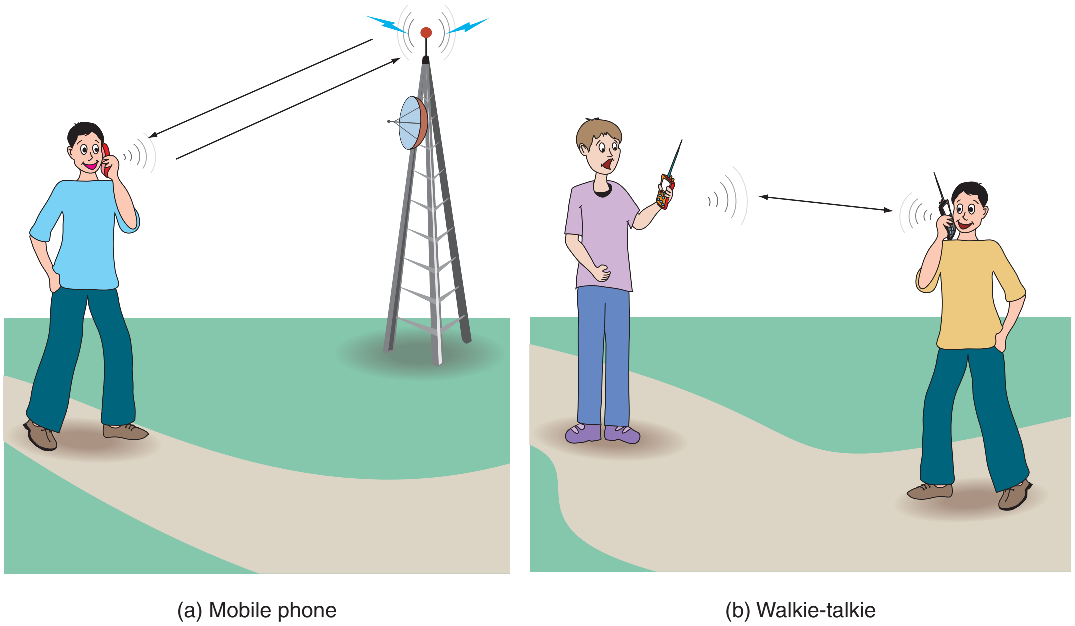
Cell phone networks use one of the following competing technologies:

- **GSM (Global System for Mobile Communications)** is an open standard that uses digital communication of data, and is accepted and used worldwide.
- **CDMA (Code Division Multiple Access)** is used by most cell phone service providers in the United States for domestic calls. If your cell phone supports the technology, you might be able to purchase a GSM plan for international calling at a higher rate.
- **TDMA (Time Division Multiple Access)** is an older, outdated technology used in the United States.

The ability to use your cell phone to browse the Web, stream music and video, play online games, use instant messaging and video conferencing is called **3G (Third Generation)** technology.

A+
220-701
4.1
4.3

All wireless phone systems, including cellular, use **full-duplex** transmission, which means both people in a conversation can talk or transmit at the same time. This is possible because the cell phones are using one frequency to transmit data and another to receive data. In contrast, walkie-talkies use **half-duplex** transmission, which means transmission works in only one direction at a time because the walkie-talkies are using the same frequency to both send and receive data. Full-duplex and half-duplex transmissions are illustrated in Figure 17-8.


(a) Mobile phone

(b) Walkie-talkie

Figure 17-8 Full-duplex and half-duplex transmission
Courtesy: Course Technology/Cengage Learning

BLUETOOTH

Bluetooth is a standard for short-range wireless communication and data synchronization between devices. Bluetooth, which has a range of only 10 meters, works in the 2.4-GHz frequency range, transfers data at up to 3 Mbps, is easy to configure, and is used for short-range personal network connections. For example, wireless headsets, mice, keyboards, and printers might use Bluetooth to communicate with a laptop that serves as the Bluetooth base station. For security, Bluetooth transmissions are encrypted. Cellular phones sometimes use Bluetooth wireless technology to make the short wireless hop between the phone and a wireless headset (see Figure 17-9). In this case, the phone serves as the base station for the headset.

Also, a cellular phone might use Bluetooth to communicate with a notebook computer, as shown in Figure 17-10. The notebook communicates with the nearby cellular phone, which communicates with the cellular WAN to provide Internet access for the notebook.

DIAL-UP TECHNOLOGY

Of all the types of networking connections, dial-up or POTS (Plain Old Telephone Service) is the least expensive and slowest connection to the Internet. Dial-up connections are painfully slow, but many times we still need them when traveling, and they're good at home when our broadband connection is down or when we just plain want to save money. Connecting to a network, such as the Internet, using a modem and regular phone line is

A+
220-701
4.1
4.3

Figure 17-9 This wireless headset accessory for a mobile phone uses Bluetooth wireless between the headset and the phone
Courtesy of Tekkeon, Inc.

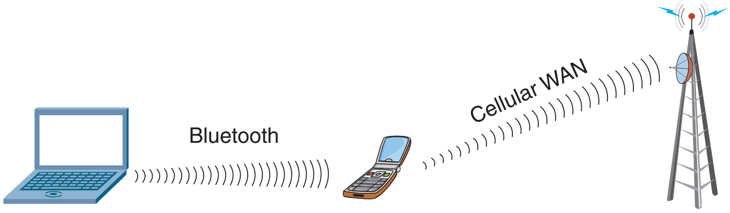


Figure 17-10 Bluetooth can be used for short transmissions between personal devices such as a cell phone and notebook computer
Courtesy: Course Technology/Cengage Learning

called **dial-up networking**. Dial-up networking works by using **PPP (Point-to-Point Protocol)** to send data packets over phone lines. PPP is, therefore, called a line protocol.

Modem cards in desktop computers provide two phone jacks (called **RJ-11 jacks**) so that one can be used for dial-up networking and the other jack can be used to plug in an extension telephone (see Figure 17-11). Laptop computers that have embedded modem capability generally have only a single phone jack. The most recent standard used by modems is the V.92 standard. Modem standards haven't changed in several years, because dial-up networking has reached its maximum bandwidth and is being outdated by other technologies to connect to the Internet.

Notes Because of the sampling rate (8,000 samples every second) used by phone companies when converting an analog signal to digital, and taking into account the overhead of data transmission (bits and bytes sent with the data that are used to control and define transmissions), the maximum transmission rate that a modem can attain over a regular phone line is about 56,000 bps, or 56 Kbps. Although theoretically possible, most modem connections don't actually attain this speed. When connecting to an ISP using a dial-up connection, to achieve 56 Kbps, the ISP must use a digital connection to the phone company.

17 A+ 220-701

A+
220-701
4.1
4.3

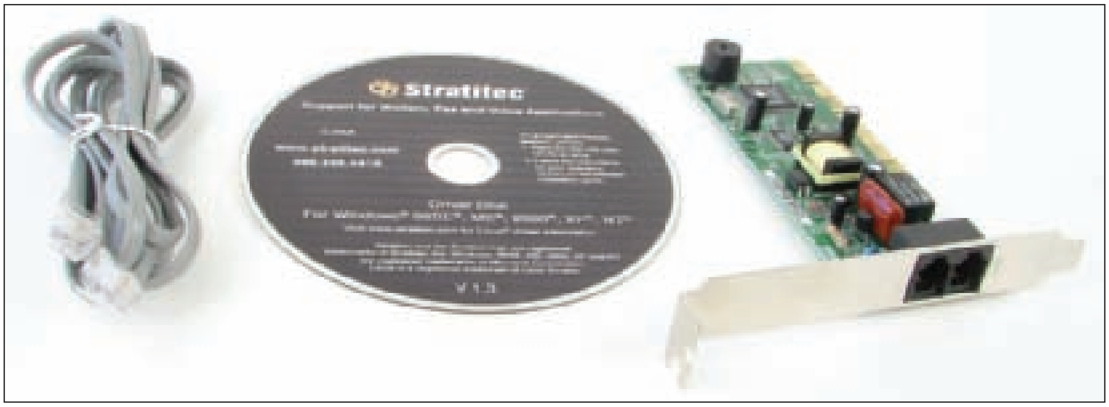


Figure 17-11 This 56K V.92 PCI modem card comes bundled with a phone cord and setup CD
Courtesy: Course Technology/Cengage Learning

INTERNET ACCESS WHEN YOU TRAVEL

When traveling in the past, the only way to connect to the Internet was to find a telephone line and use your laptop computer to dial in to your ISP. Today, we have many options:

- A cellular **Internet card**, also called an air card, works like a cell phone to connect to a cellular WAN to give your computer Internet access. The device can be a USB device or can be a card that inserts into a PC Card slot or ExpressCard slot on a laptop. The AirCard 402 shown in Figure 17-12 is a combo device that includes an adapter so that it can fit either a PC Card slot or an ExpressCard slot. Use an Internet card wherever you have a cell phone signal to connect your PC to the Internet. You pay for the service through your cell phone provider.

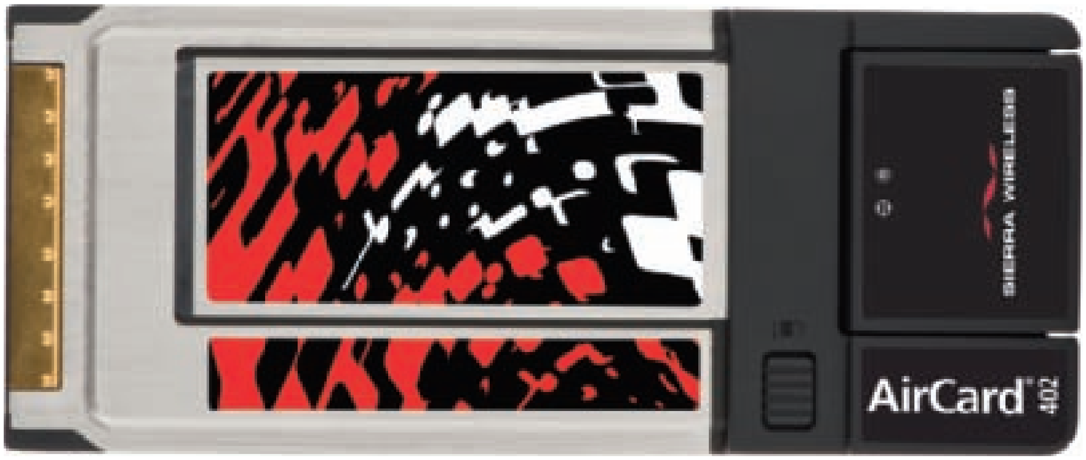


Figure 17-12 AirCard 402 Modem by Sierra Wireless fits a PC Card or ExpressCard slot on a laptop to provide GPS and Internet through a cellular network
Courtesy of Sierra Wireless

- Find a public Wi-Fi hot spot and connect your laptop wirelessly. You'll sometimes pay a fee to use the hotspot.
- Mobile satellite broadband can be used by travelers who want to tote about a portable satellite dish. Figure 17-13 shows a dish by Ground Control (*www.groundcontrol.com*) mounted on top of a truck. Dishes can also be purchased to mount on top of an RV or that are small enough to pack with a laptop. Some satellite dish systems can automatically point the dish to the southern sky to make a high-speed connection.

A+
220-701
4.1
4.3

Figure 17-13 This satellite Internet system by Ground Control gives high-speed Internet access anywhere
Courtesy of Ground Control

HARDWARE USED BY LOCAL NETWORKS

A+
220-701
1.2
1.9
4.1

In this part of the chapter, you will learn about the hardware devices that create and connect to networks. Hardware discussed includes desktop and laptop devices, cables and their connectors, hubs, switches, wireless access devices, and routers.

NETWORKING ADAPTERS AND PORTS

A desktop to laptop computer connects to a local network using an Ethernet wired network or wireless networking.

A+
220-701
1.2
1.9
4.1
2.2

ETHERNET NETWORK ADAPTERS AND PORTS

A PC makes a direct connection to a network by way of a **network adapter**, which might be a network port embedded on the motherboard or a **network interface card (NIC)**, using an expansion slot, such as the one shown in Figure 17-14. In addition, the adapter might also be an external device connecting to the PC using a USB port. The adapter provides an **RJ-45** port (RJ stands for registered jack) that looks like a large phone jack. Laptops can make connections to a network through a PC Card NIC, a built-in network port, or an external device that connects to the laptop by way of a USB port. (You will learn about PC Cards in Chapter 21.)

A+
220-701
1.2
1.9
4.1
2.2

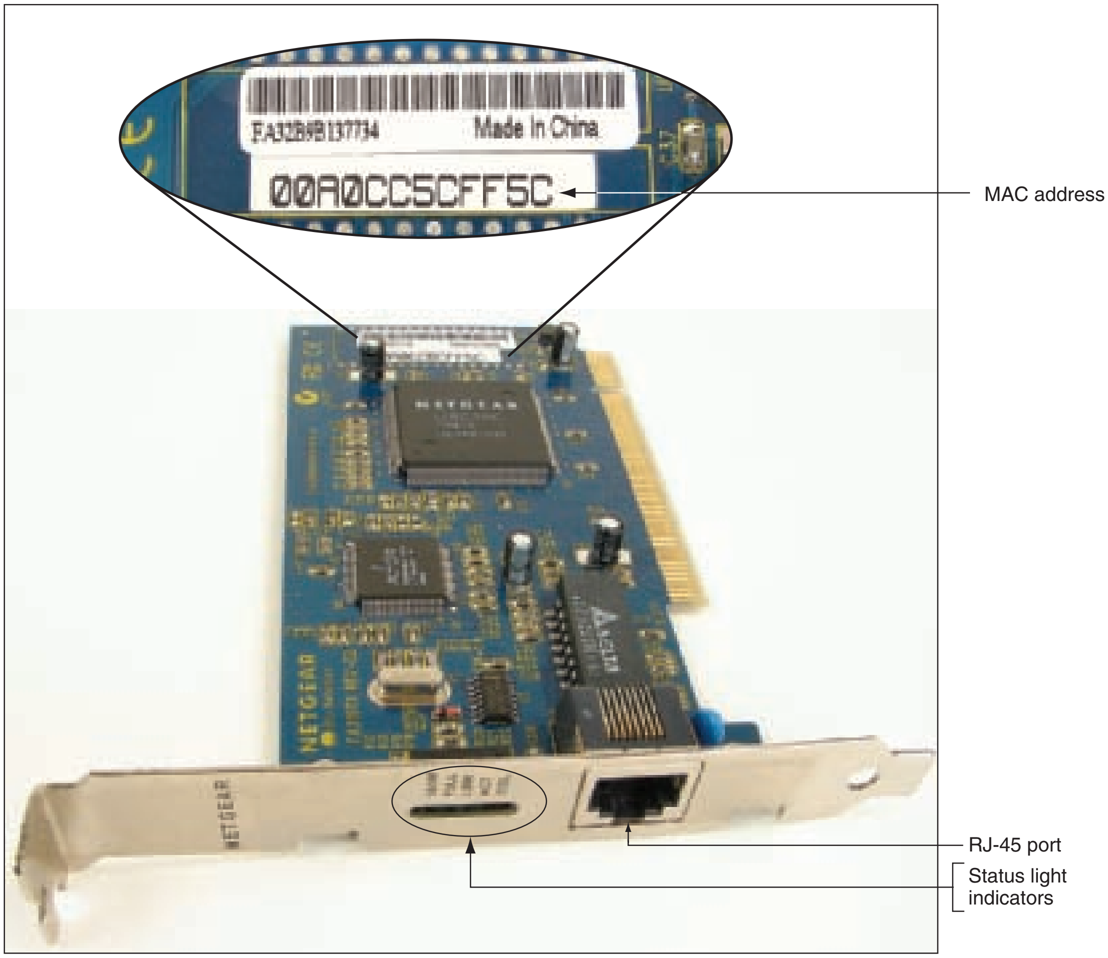


Figure 17-14 Ethernet network card showing its MAC address
Courtesy: Course Technology/Cengage Learning

A+ Exam Tip The A+ 220-701 Essentials exam expects you to know the purpose of an RJ-45 port and an RJ-11 port.

Most network cards also provide **status light indicators** near the RJ-45 port. You can see a bank of these indicators on the card in Figure 17-14. Depending on the card, the lights might indicate the speed of transmission being used among those the card supports, connectivity, and activity. For a network port on the motherboard, a solid light indicates connectivity and a blinking light indicates activity. For example, in Figure 17-15, the yellow light blinks to indicate activity and the green light is steady or solid to indicate connectivity. When you first discover you have a problem with a PC not connecting to a network, be sure to check the status light indicators to verify you have connectivity and activity. If not, then the problem is related to hardware. Check the cable connections at both ends. If the connections are solid, then the problem is with the NIC, the cable, or other networking hardware.

Every network adapter (including a network card, onboard wireless, or wireless NIC) has a 48-bit (6-byte) number hard-coded on the card by its manufacturer that is unique for that

A+
220-701
1.2
1.9
4.1
2.2

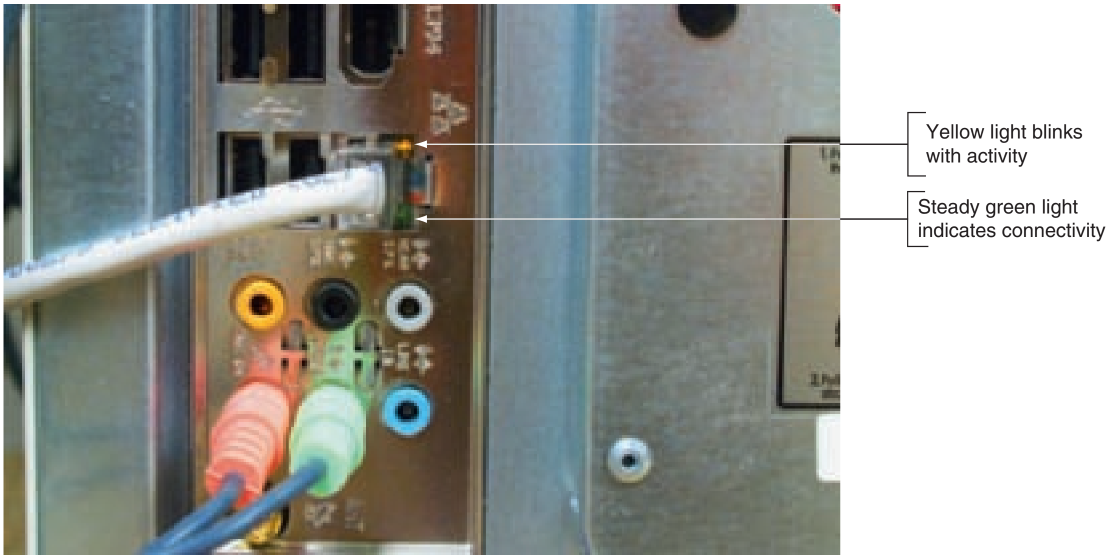

Yellow light blinks with activity
Steady green light indicates connectivity

Figure 17-15 Status indicator lights for the embedded network port
Courtesy: Course Technology/Cengage Learning

adapter, and this number is used to identify the adapter on the network. The number is written in hex and is called the **MAC (Media Access Control) address**, **hardware address**, **physical address**, **adapter address**, or Ethernet address. An example of a MAC address is 00-0C-6E-4E-AB-A5. Part of the MAC address refers to the manufacturer, and the second part of the address is a serial number assigned by the manufacturer. Therefore, no two adapters should have the same MAC address. Most likely the MAC address is printed on the card, as shown in Figure 17-14. Every NIC used today for a wired network follows the Ethernet standards. Recall that the four speeds for Ethernet are 10 Mbps, 100 Mbps (Fast Ethernet), 1 Gbps (Gigabit Ethernet), and 10 Gbps (10-gigabit Ethernet). Most network cards sold today use Gigabit Ethernet and also support the two slower speeds.

A+
220-701
1.2
1.9

WI-FI WIRELESS ADAPTERS

Video
Wireless Network Cards

Wi-Fi wireless connections using 802.11b/g/n standards can be made with a variety of devices, four of which are shown in Figure 17-16. In addition, most laptops sold today have a wireless antenna embedded inside the laptop.

A+
220-701
4.2

CABLES AND CONNECTORS

Several variations of Ethernet cables and connectors have evolved over the years, and are primarily identified by their speeds and the types of connectors used to wire these networks. Table 17-2 compares cable types and Ethernet versions.

A+ Exam Tip The A+ 220-701 Essentials exam expects you to know the details shown in Table 17-2.

A+
220-701
4.2

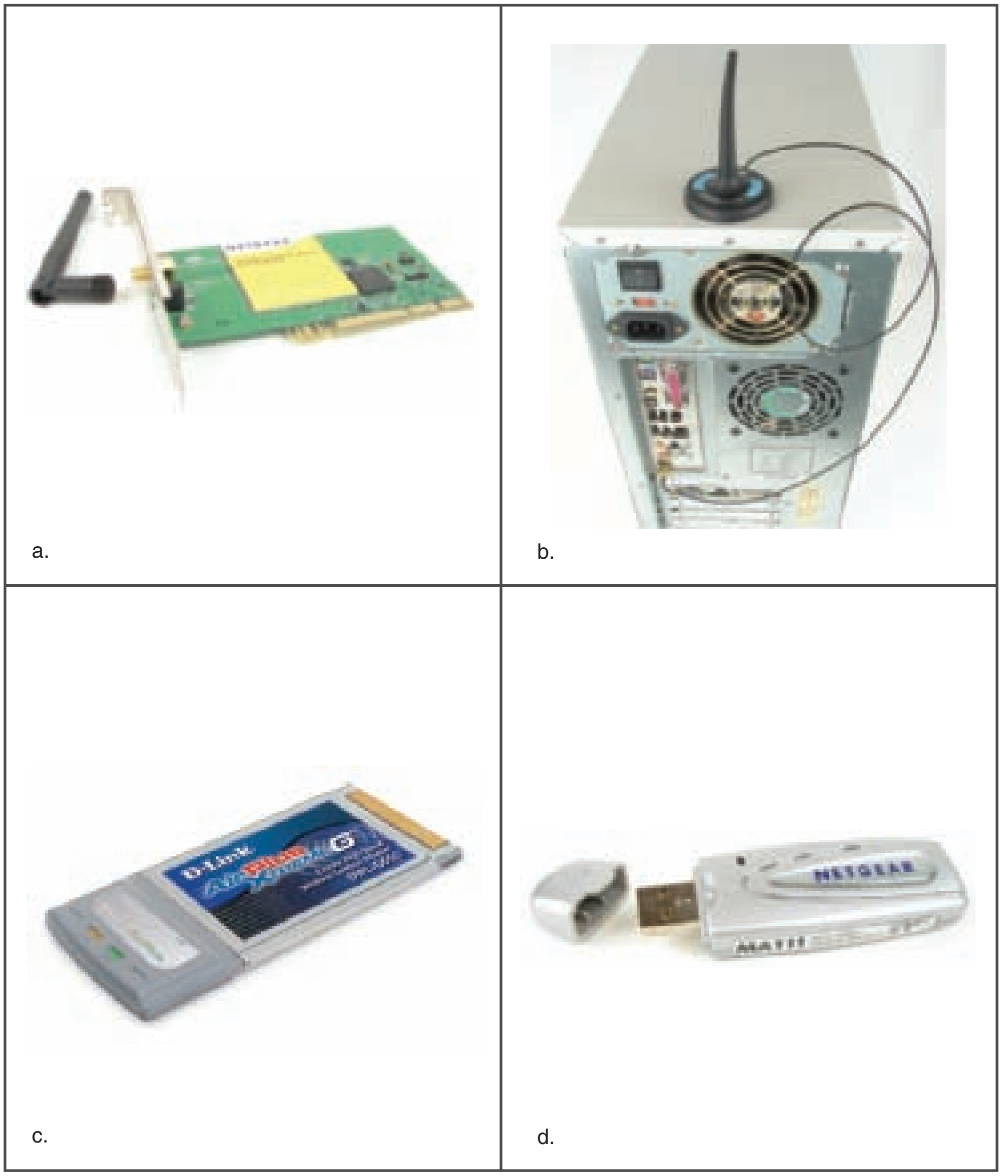


Figure 17-16 Four different types of wireless network adapters: (a) wireless NIC that fits in a PCI slot; (b) onboard wireless with an antenna that can be moved; (c) PC Card wireless NIC with embedded antenna; and (d) wireless NIC that uses a USB port on a desktop or notebook computer
Courtesy: Course Technology/Cengage Learning

As you can see from Table 17-2, the three main types of cabling used by Ethernet are twisted-pair, coaxial, and fiber optic. Coaxial cable is older and almost never used today. Within each category, there are several variations:

- *Twisted-pair cable*. Twisted-pair cable is the most popular cabling method for local networks. It comes in two varieties: **unshielded twisted pair (UTP) cable** and **shielded twisted pair (STP) cable**. UTP cable is the most common and least expensive. UTP is rated by category: **CAT-3 (Category 3)** is less expensive than the more popular **CAT-5** cable or **enhanced CAT-5 (CAT-5e)**. **CAT-6** has less crosstalk than CAT-5 or CAT-5e. STP uses a covering around the pairs of wires inside the cable that protects it from electromagnetic interference caused by electrical motors, transmitters, or high-tension lines. It costs more than unshielded cable, so it's used only when the situation

A+
220-701
4.2

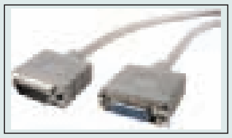
Cable System	Speed	Cables and Connectors	Example of Connectors	Maximum Cable Length
10Base2 (ThinNet)	10 Mbps	Coaxial uses a BNC connector.	Courtesy of Cables4Computer.com	185 meters or 607 feet
10Base5 (ThickNet)	10 Mbps	Coaxial uses an AUI 15-pin D-shaped connector.	 Courtesy of Black Box Corporation	500 meters or 1,640 feet
10BaseT, 100BaseT (Twisted-pair), Gigabit Ethernet, and 10-Gigabit Ethernet	10 Mbps, 100 Mbps, 1 Gbps, or 10 Gbps	Twisted pair (UTP or STP) uses an RJ-45 connector.	Courtesy of Tyco Electronics	100 meters or 328 feet
10BaseF, 10BaseFL, 100BaseFL, 100BaseFX, 1000BaseFX, or 1000BaseX (fiber optic)	10 Mbps, 100 Mbps, 1 Gbps,or 10 Gbps	Fiber-optic cable uses ST or SC connectors (shown to the right) or LC and MT-RJ connectors (not shown).	Courtesy of Black Box Corporation	Up to 2 kilometers (6,562 feet)

Table 17-2 Variations of Ethernet and Ethernet cabling

demands it. Twisted-pair cable has four pairs of twisted wires for a total of eight wires and uses a connector called an RJ-45 connector. Figure 17-17 shows unshielded twisted-pair cables and the RJ-45 connector.

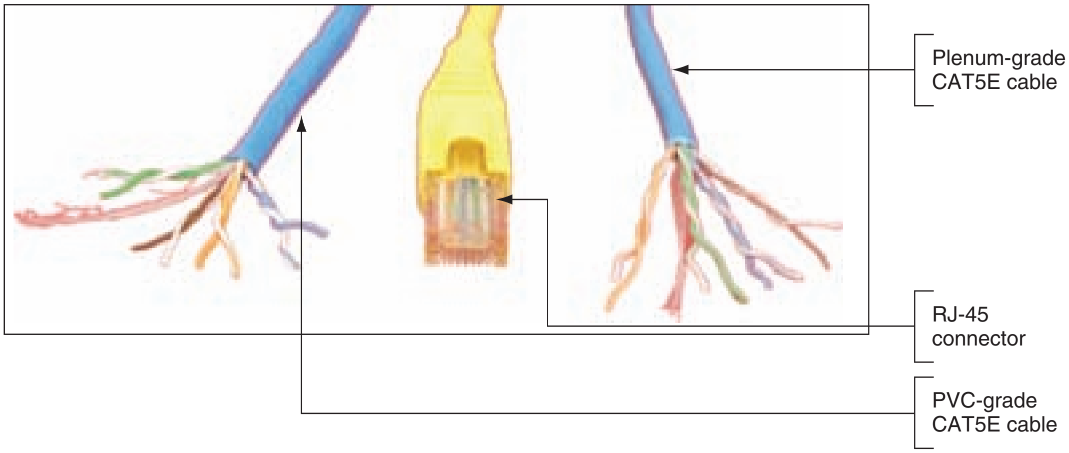


Figure 17-17 The most common networking cable for a local network is UTP cable using an RJ-45 connector
Courtesy: Course Technology/Cengage Learning

A+
220-701
4.2

Notes Normally, the plastic covering of a cable is made of PVC (polyvinyl chloride), which is not safe when used inside plenums (areas between the floors of buildings). In these situations, plenum cable covered with Teflon is used because it does not give off toxic fumes when burned. Plenum cable is two or three times more expensive than PVC cable. Figure 17-17 shows plenum cable and PVC cable, both of which are unshielded twisted pair CAT5e cables.

- *Coaxial cable.* **Coaxial cable** has a single copper wire down the middle and a braided shield around it (see Figure 17-18). The cable is stiff and difficult to manage, and is no longer used for networking. RG6 coaxial cable is used for cable TV, having replaced the older and thinner RJ59 coaxial cable once used for cable TV.

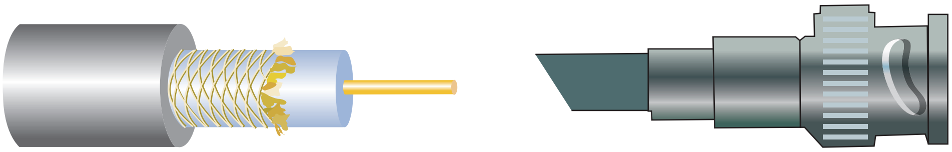


Figure 17-18 Coaxial cable and a BNC connector are used with ThinNet Ethernet
Courtesy: Course Technology/Cengage Learning

- *Fiber optic.* **Fiber-optic cables** transmit signals as pulses of light over glass strands inside protected tubing, as illustrated in Figure 17-19. Fiber-optic cable comes in two types: single-mode (thin, difficult to connect, expensive, and best performing) and multimode (most popular). A single-mode cable uses a single path for light to travel in the cable and multimode cable uses multiple paths for light. Both single-mode and multimode fiber-optic cables can be constructed as loose-tube cables for outdoor use or tight-buffered cable for indoor or outdoor use. Loose-tube cables are filled with gel to prevent water from soaking into the cable, and tight-buffered cables are filled with yarn to protect the fiber-optic strands, as shown in Figure 17-19.

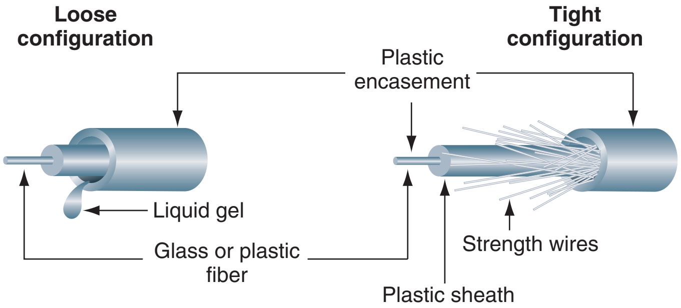
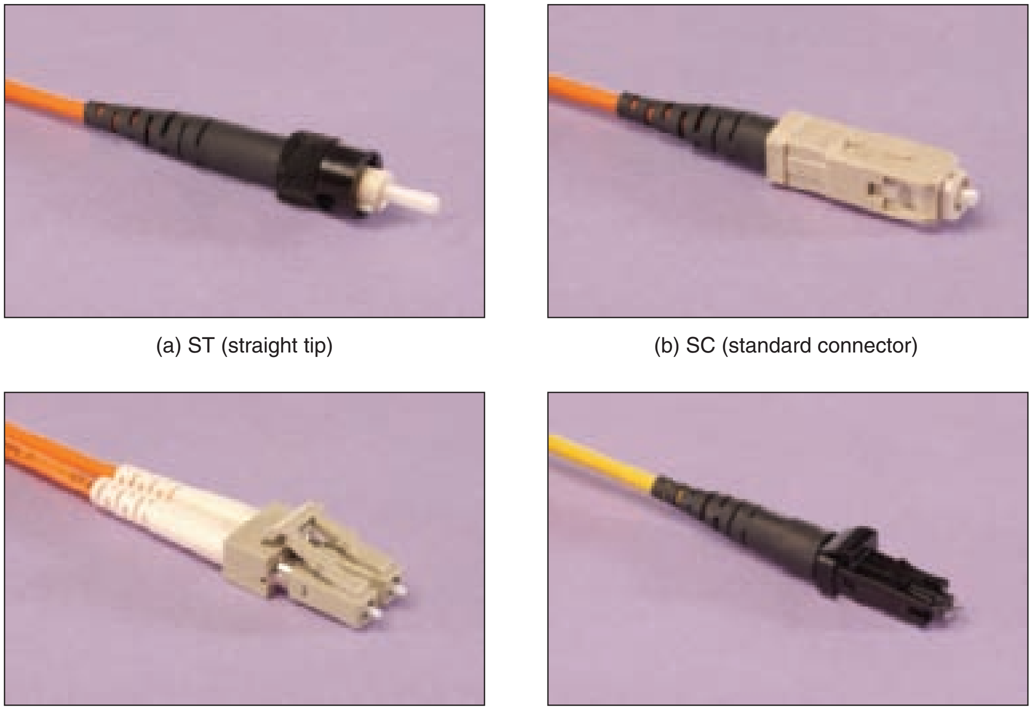


Figure 17-19 Fiber-optic cables contain a glass core for transmitting light
Courtesy: Course Technology/Cengage Learning

A+
220-701
4.2

Fiber-optic cables can use one of four connectors, all shown in Figure 17-20. The two older types are ST (straight tip) and SC (subscriber connector or standard connector). Two newer types are LC (local connector) and MT-RJ (mechanical transfer registered jack) connectors. Any one of the four connectors can be used with either single-mode or multimode fiber-optic cable.



(a) ST (straight tip)

(b) SC (standard connector)

(c) LC (local connector)

(d) MT-RJ (mechanical transfer RJ)

Figure 17-20 Four types of fiber-optic connectors: (a) ST, (b) SC, (c) LC, and (d) MT-RJ
Courtesy of Fiber Communications, Inc. (*www.fiberc.com*)

A+ Exam Tip The A+ 220-701 Essentials exam expects you to know about these cable types: Plenum, PVC, UTP, CAT3, CAT5, CAT5e, CAT6, STP, fiber, and coaxial cable.

Each version of Ethernet can use more than one cabling method. Here is a brief description of the types of Ethernet identified by the cabling methods they use:

- *10-Mbps Ethernet*. This first Ethernet specification was invented by Xerox Corporation in the 1970s, and later became known as Ethernet.
- *100-Mbps Ethernet or Fast Ethernet*. This improved version of Ethernet (sometimes called **100BaseT** or **Fast Ethernet**) operates at 100 Mbps and uses STP or UTP cabling rated CAT-5 or higher. 100BaseT networks can support slower

A+
220-701
4.2

speeds of 10 Mbps so that devices that run at either 10 Mbps or 100 Mbps can coexist on the same LAN. Two variations of 100BaseT are 100BaseTX and 100BaseFX. The most popular variation is 100BaseTX. 100BaseFX uses fiber-optic cable.

- *1000-Mbps Ethernet or Gigabit Ethernet*. This version of Ethernet operates at 1000 Mbps and uses twisted-pair cable and fiber-optic cable. **Gigabit Ethernet** is currently replacing 100BaseT Ethernet as the choice for LAN technology. Because it can use the same cabling and connectors as 100BaseT, a company can upgrade from 100BaseT to Gigabit without great expense.
- *10-Gigabit Ethernet*. This version of Ethernet operates at 10 billion bits per second (10Gbps) and uses fiber cable. It can be used on LANs, MANs, and WANs, and is also a good choice for backbone networks. (A backbone network is a channel whereby local networks can connect to wide area networks or to each other.)

HUBS AND SWITCHES

A+
220-701
4.1

Older Ethernet networks that used coaxial cable connected all the devices (called nodes) on the network in a logical bus formation, which means that nodes were all strung together in a daisy chain with terminators at each end, similar to how SCSI devices are chained together. Today's Ethernet networks use a star formation (called a star topology) whereby nodes are connected to a centralized hub or switch (see Figure 17-21). PCs on the LAN are like points of a star around the hub or switch in the middle, which connects the nodes on the LAN. An Ethernet hub transmits the data packet to every device, except the device that sent the transmission, as shown in Figure 17-21.

You can think of a **hub** (see Figure 17-22) as just a pass-through and distribution point for every device connected to it, without regard for what kind of data is passing through

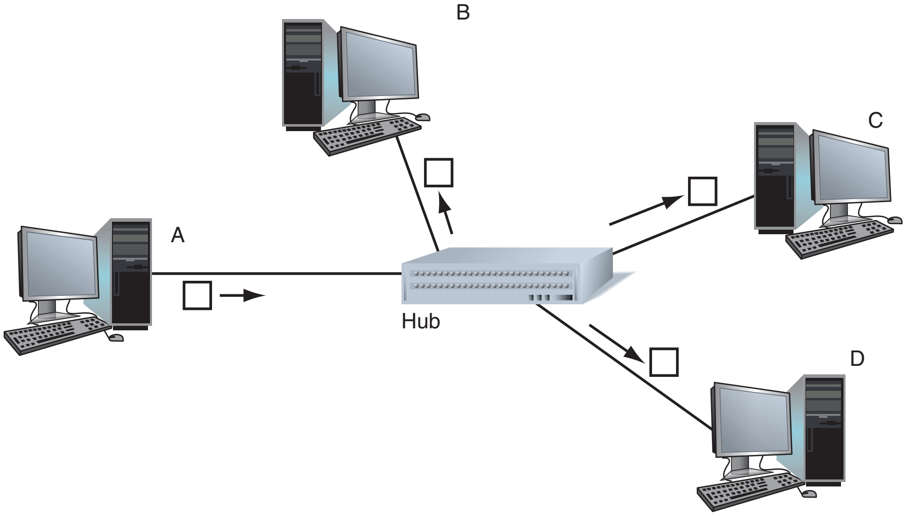


Figure 17-21 Any data received by a hub is replicated and passed on to all other devices connected to it
Courtesy: Course Technology/Cengage Learning

A+
220-701
4.1

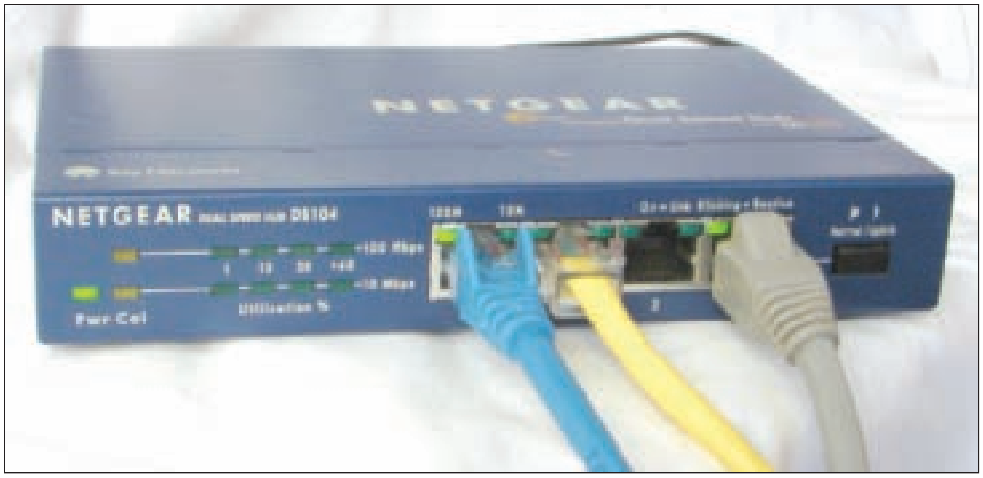


Figure 17-22 A hub is a pass-through device to connect nodes on a network
Courtesy: Course Technology/Cengage Learning

and where the data might be going. Hubs are outdated technology, having been replaced by switches.

A switch (see Figure 17-23) is smarter and more efficient than a hub, as it keeps a table of all the devices connected to it. It uses this table to determine which path to use when sending packets. The switch only passes data to the device to which the data is addressed.

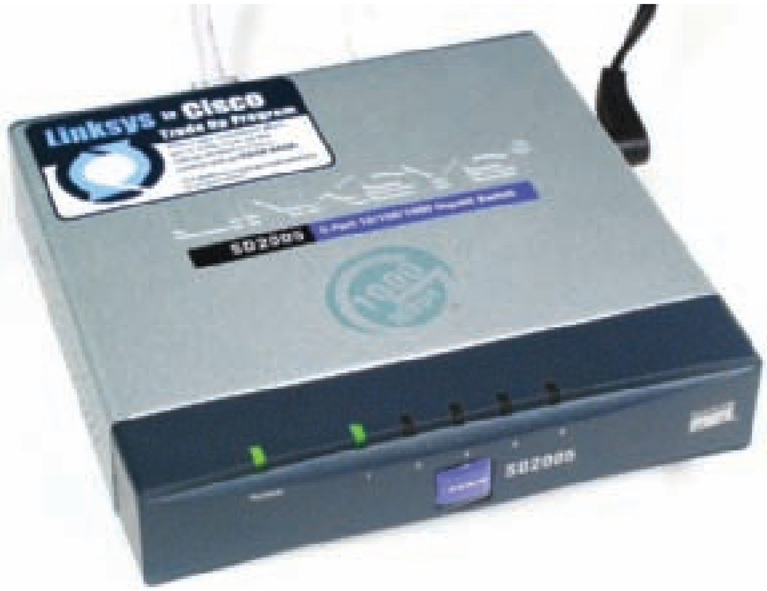


Figure 17-23 A five-port Gigabit Ethernet switch by Linksys
Courtesy: Course Technology/Cengage Learning

As network needs grow, you can add a switch so that you can connect more devices to the network. Figure 17-24 shows an example of a network that uses three switches in

A+
220-701
4.1

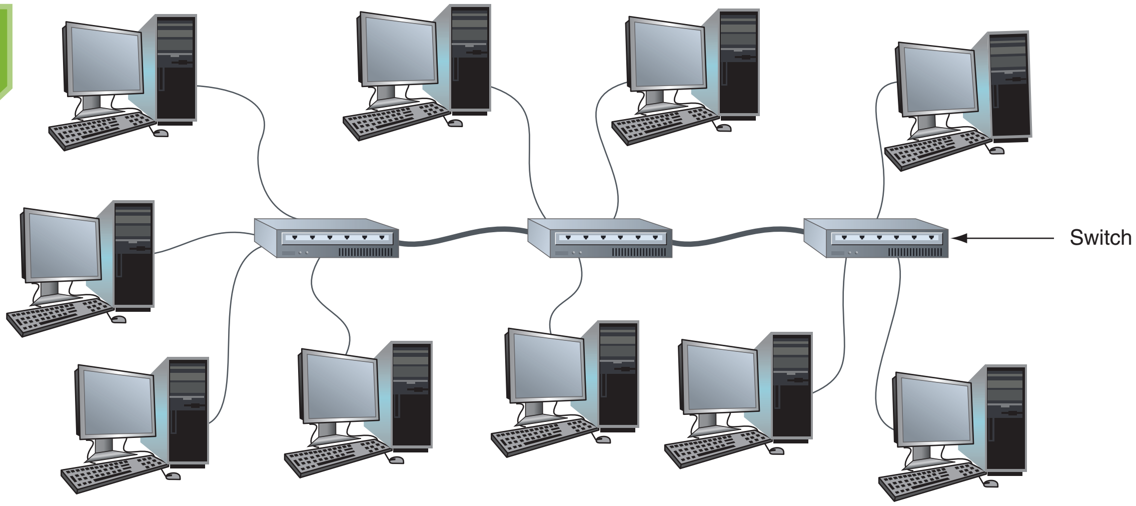


Figure 17-24 An Ethernet network with three switches
Courtesy: Course Technology/Cengage Learning

sequence. Physically, the network cables that run between two switches or a switch and a computer might be inside a building's walls with a network jack on the wall providing an RJ-45 connector. You plug a network cable into the jack to make the connection. In practice, a small network might begin as one switch and three or four computers. As the need for more computers grows, new switches are added to provide these extra connections.

Another reason to add a switch to a network is to regenerate the network signal. STP and UTP Ethernet cables should not exceed 100 meters (about 328 feet) in length. If you need to reach distances greater than that, you can add a switch in the line, which regenerates the signal.

Two types of network cables can be used when building a network: a patch cable and a crossover cable. A **patch cable** (also called a straight-through cable) is used to connect a computer to a hub or switch. A **crossover cable** is used to connect two like devices such as a switch to a switch or a PC to a PC (to make the simplest network of all).

The difference in a patch cable and a crossover cable is the way the transmit and receive lines are wired in the connectors at each end of the cables. A crossover cable has the transmit and receive lines reversed so that one device receives off the line to which the other device transmits. You can use a crossover cable to connect a switch to a switch. However, some switches have an uplink port so that you can use a patch cable to connect it to another switch. Other switches use auto-uplinking, which means you can connect a switch to a switch using a patch cable on any port.

A patch cable and a crossover cable look identical and have identical connectors. One way to tell them apart is to look for the labeling imprinted on the cables, as shown in Figure 17-25. If you don't see labeling, know that you can use a cable tester to find out what type of cable you have.

Video
Ethernet Cables

WIRELESS ACCESS POINTS

Wireless devices can communicate directly (such as a PC to a PC, which is called Ad Hoc mode), or they can connect to a LAN by way of a wireless **access point (AP)**, as shown in

A+
220-701
4.1

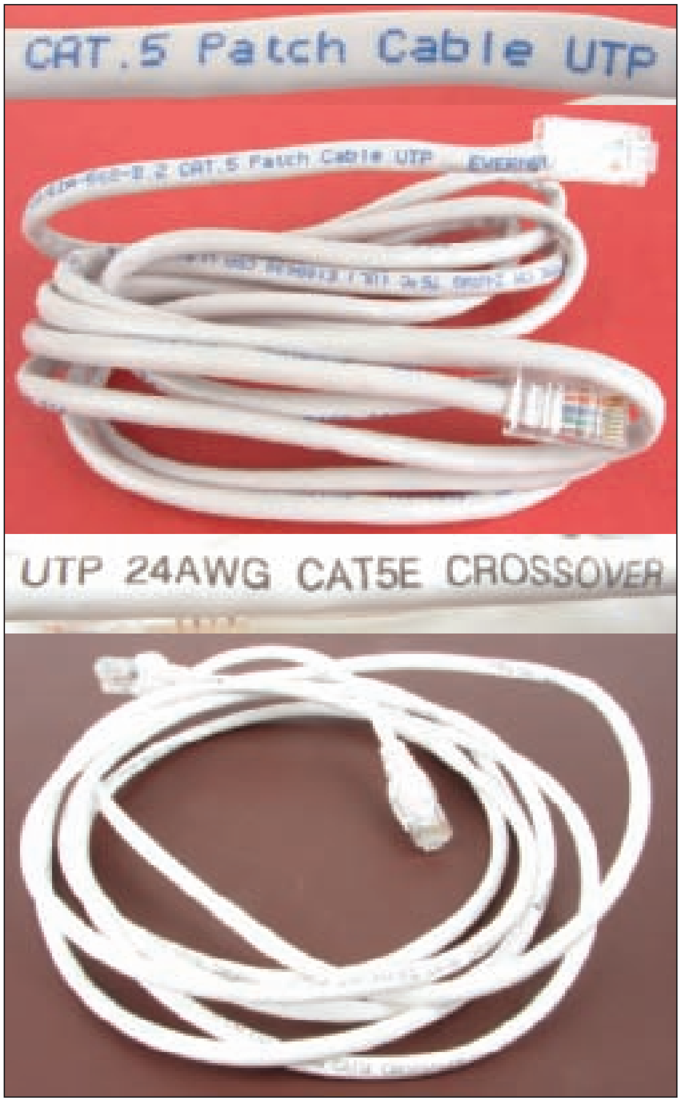


Figure 17-25 Patch cables and crossover cables look the same but are labeled differently
Courtesy: Course Technology/Cengage Learning

Figure 17-26. Multiple access points can be positioned so that nodes can access at least one access point from anywhere in the covered area. When devices use an access point, they communicate through the access point instead of communicating directly. Often a wireless access point is doing double duty as a router, a device that connects one network to another.

Video
Using a Multifunction Router

A+ Exam Tip The A+ 220-701 Essentials exam expects you to know the differences among a hub, switch, and router.

A+
220-701
4.1

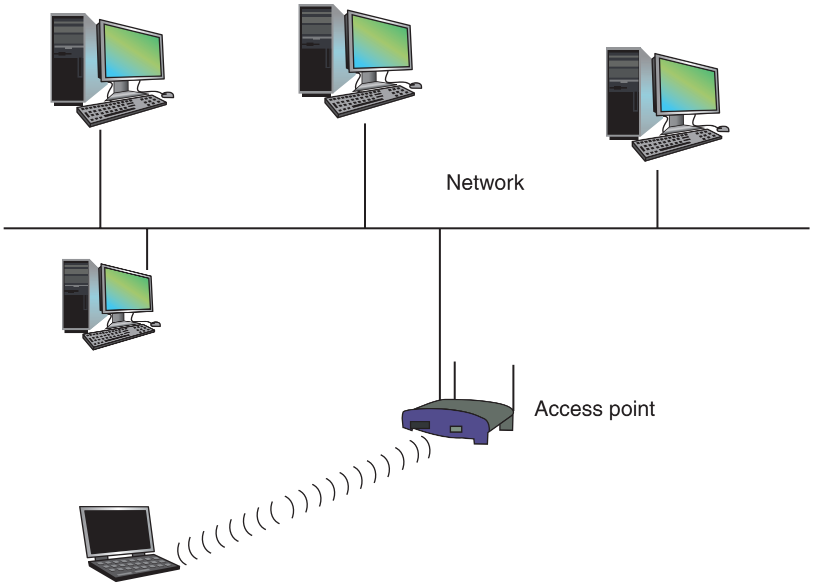


Figure 17-26 Nodes on a wireless LAN connect to a wired network by way of an access point
Courtesy: Course Technology/Cengage Learning

Notes The wired network in Figure 17-26 shows connectivity but does not indicate the details of that connectivity. Know that, in practice, this network might involve switches and hubs.

ROUTERS

A **router** is a device that manages traffic between two networks. In Figure 17-27, you can see that a router stands between the ISP network and the local network. The router is the gateway to the Internet. Note in the figure that computers can connect to the router directly or by way of one or more switches. Routers can range from small ones designed to manage a small network connecting to an ISP (costing less than $100) to those that manage multiple networks and extensive traffic (costing several thousand dollars).

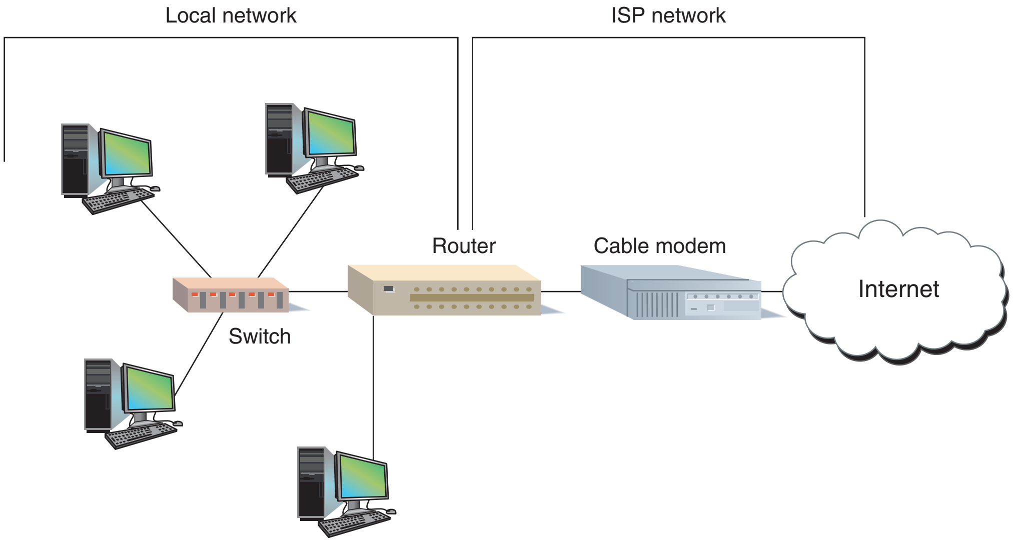


Figure 17-27 A router stands between a local network and the Internet and manages traffic between them
Courtesy: Course Technology/Cengage Learning

A+
220-701
4.1

Four companies that make routers suitable for small networks are D-Link (*www.dlink.com*), Linksys (*www.linksys.com*), NetGear (*www.netgear.com*), and Belkin (*www.belkin.com*). An example of a multifunction router is the Wireless-N Gigabit Router by Linksys shown in Figures 17-28 and 17-29. It has one port for the broadband modem and four ports for computers on the network. The router is also an 802.11b/g/n wireless access point having multiple antennas to increase speed and range using Multiple In, Multiple Out (MIMO) technology. The antennas are built in.

Figure 17-28 The Wireless-N Gigabit router by Linksys has built-in wireless antennas and can be used with a DSL or cable modem Internet connection
Courtesy: Course Technology/Cengage Learning

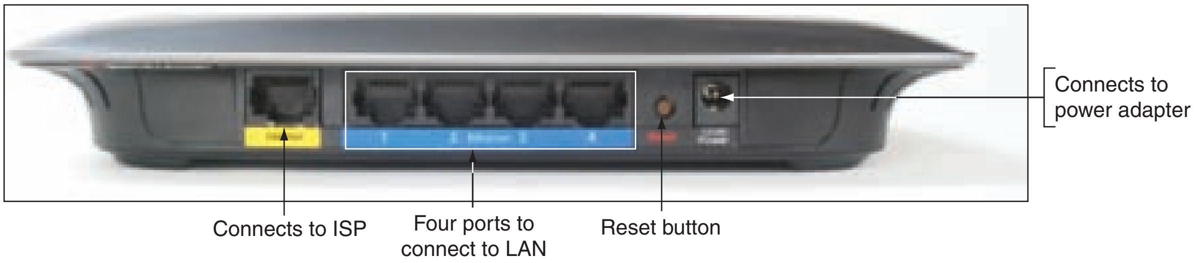


Figure 17-29 Connectors and ports on the back of the Linksys router
Courtesy: Course Technology/Cengage Learning

A **DHCP (dynamic host configuration protocol)** server gives IP addresses to computers on the network when they attempt to initiate a connection to the network and request an IP address. With a DHCP server on the network, computers can use dynamic IP addressing, so that you don't have to assign and keep up with unique IP addresses for each computer.

The router shown in Figure 17-28 is typical of many brands and models of routers used in a small office or small home network to manage the Internet connection. This router is several devices in one:

- *Function 1:* As a router, it stands between the ISP network and the local network, routing traffic between the two networks.

A+
220-701
4.1

- *Function 2:* As a switch, it manages four network ports that can be connected to four computers or to a switch or hub that connects to more than one computer.
- *Function 3:* As a DHCP server, all computers can receive their IP address from this server. With a DHCP server on the network, computers can use dynamic IP addressing so that you don't have to assign and keep up with unique IP addresses for each computer.
- *Function 4:* As a wireless access point, a computer can connect to the network using a wireless device. This wireless connection can be secured using four different wireless security features.
- *Function 5:* As a **firewall**, unwanted traffic initiated from the Internet can be blocked. These firewall functions include a security feature called NAT redirection. **NAT (Network Address Translation)** is a protocol that substitutes the IP address of the router for the IP address of other computers inside the network when these computers need to communicate on the Internet. You will learn more about NAT in Chapter 18. Another firewall feature is to restrict Internet access for computers behind the firewall. Restrictions can apply to days of the week, time of day, keywords used, or certain Web sites.

In the small office setting pictured in Figure 17-30, a router connects four network jacks that are wired in the walls to four other jacks in the building. Two of these remote jacks have switches connected that accommodate two or more computers.

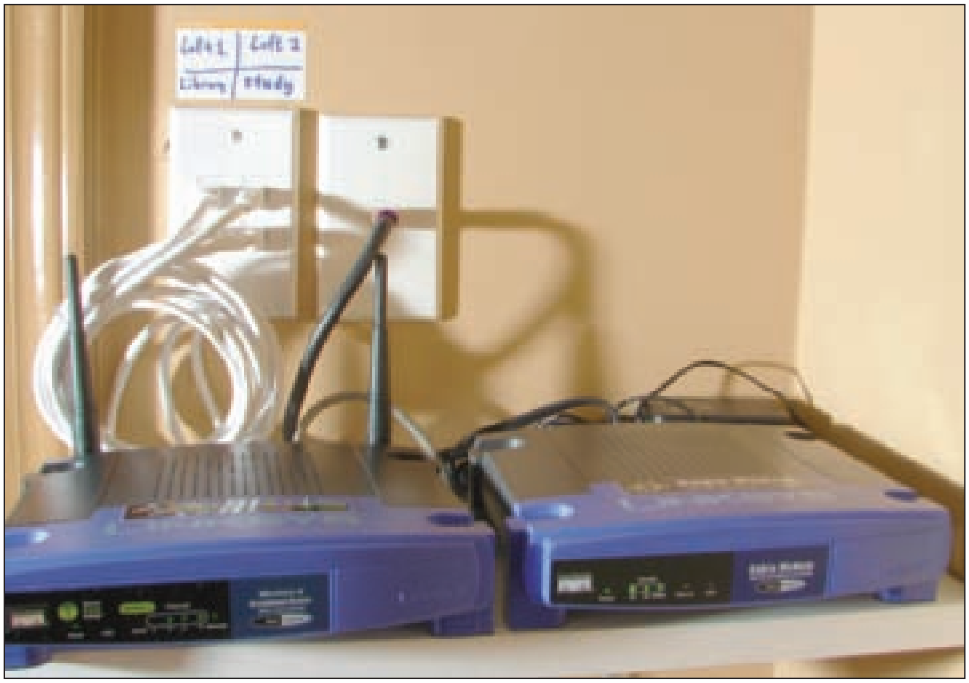


Figure 17-30 A router and cable modem are used to provide Internet access for a small network
Courtesy: Course Technology/Cengage Learning

Notes The speed of a network depends on the speed of each device on the network. Routers, switches, and network adapters currently run at three speeds: Gigabit Ethernet (1,000 Mbps or 1 Gbps), Fast Ethernet (100 Mbps), or Ethernet (10 Mbps). If you want your entire network to run at the fastest speed, make sure all your devices are rated for Gigabit Ethernet. Very few networks today use 10 Mbps Ethernet, and Gigabit Ethernet is slowly replacing Fast Ethernet as the most popular standard.

A+
220-701
4.1

So far in this chapter, we've looked at all the different hardware devices and hardware technologies to build networks. Each hardware device on a network, such as a NIC, switch, router, or wireless access point, uses a hardware protocol to communicate on the network. For most wired LANs, that protocol is Ethernet. However, in addition to the hardware protocol, there is a layer of network communication at the operating system level. The next section looks at the different OS networking protocols and how they work.

WINDOWS ON A NETWORK

Most applications that use the Internet are **client/server applications**, which means that two computers and two applications are involved. The client application (for example, a Web browser) on one computer makes a request for data from the server application (for example, a Web server) on another computer (see Figure 17-31). In this client/server environment, the application serving up data is called the server and the computer on which this server application is installed can also be referred to as the server. In other words, a server is any computer or application serving up data when that data is requested.

Communication between a client application and a server application happens at three levels (hardware, operating system, and application) and is dependent on one computer addressing the other computer is such a way that they find one another. Now let's see how these three levels for communication on a network work and how computers find each other on a network.

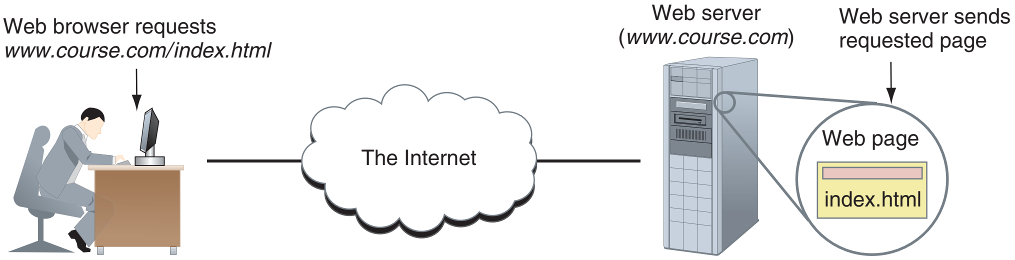


Figure 17-31 A Web browser (client software) requests a Web page from a Web server (server software); the Web server returns the requested data to the client
Courtesy: Course Technology/Cengage Learning

LAYERS OF NETWORK COMMUNICATION

When your computer at home is connected to your ISP off somewhere in the distance, your computer and a computer on the Internet are communicating at the application, operating system, and hardware levels. The computers need a way to address each other at each level. These three levels and the addresses used at each level are diagrammed in Figure 17-32. Listed next is a description of each level of communication:

- *Level 1: Hardware level.* At the root level of communication is hardware. The hardware or physical connection might be wireless or might use network cables, phone lines (for DSL or dial-up), or TV cable lines (for cable modem). For local wired or wireless networks, a network adapter inside your computer is part of this physical network. The rules for communication are predetermined and these rules are called protocols. Recall that each network adapter is assigned a MAC address, and this address is used to uniquely identify a computer on a local network.

17
A+ 220-701

A+
220-701
4.1

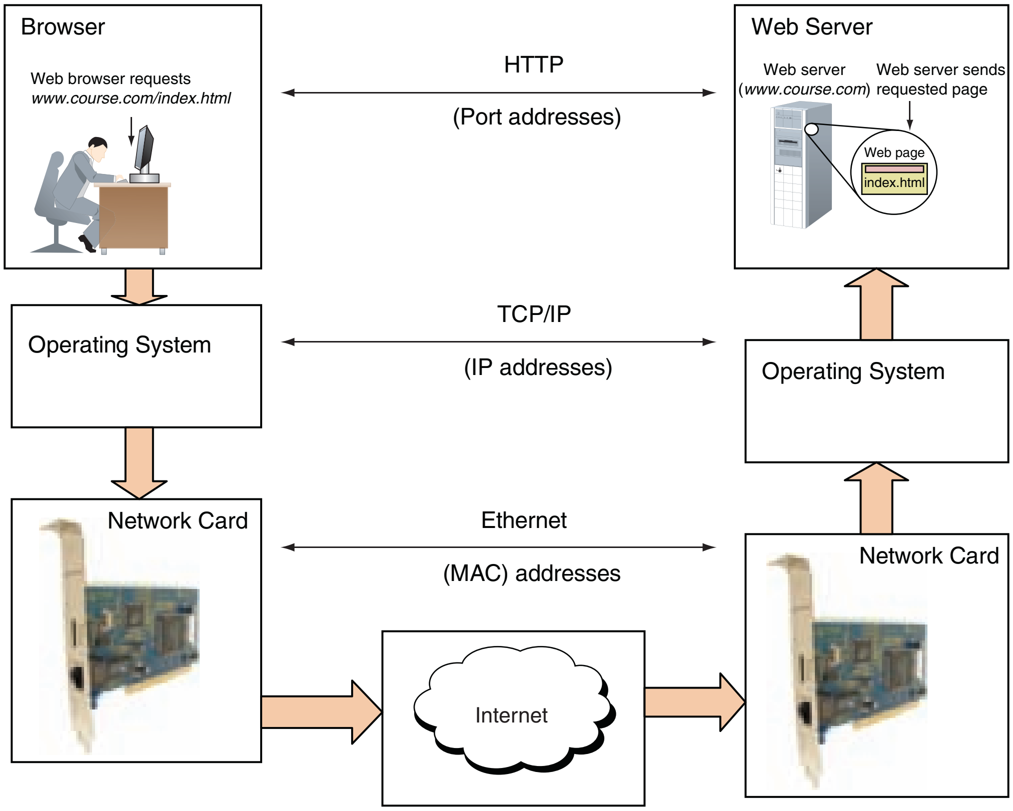


Figure 17-32 Network communication happens in layers
Courtesy: Course Technology/Cengage Learning

- *Level 2: Operating system level*. An OS is responsible for managing communication between itself and another computer, using rules for communication that both operating systems understand. This group, or suite, of communication protocols is collectively called TCP/IP. One OS addresses the other OS using addresses called IP addresses. An **IP address** is a 32-bit string used to identify a computer on a network. These 32 bits are organized into four groups of eight bits each, which are presented as four decimal numbers separated by periods, such as 72.56.105.12. Because the largest possible 8-bit number is 255, each of the four numbers can be no larger than 255. A network can use static IP addressing, in which each computer is assigned an IP address that never changes, or dynamic IP addressing, in which each time the computer connects to the network, it gets a new IP address from the DHCP server (called leasing the IP address). IP addresses are used to identify a computer both inside and outside its local network. Consider a MAC address a local address and an IP address a long-distance address, as shown in Figure 17-33.
- *Level 3: Application level*. When you use the Internet to surf the Web or download your e-mail, you are using an application on your computer called an Internet client. For Web surfing, that client, such as Internet Explorer or Firefox, is called a browser. The client communicates with another application somewhere on the Internet, called a server. Examples of server applications are your e-mail server at your ISP or a Web server anywhere on the Web. The client and server applications are each assigned a number that uniquely identifies the application on the computer. This number is called a **port number**, **port**, or **port address**. Table 17-3 lists common port assignments for some well-known applications. For example, you can address a Web server by entering

A+
220-701
4.1

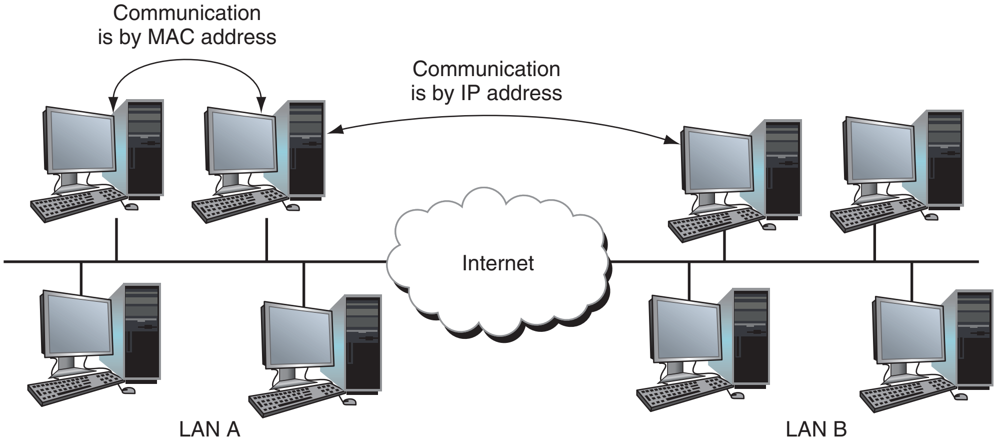


Figure 17-33 Computers on the same LAN use MAC addresses to communicate, but computers on different LANs use IP addresses to communicate over the Internet
Courtesy: Course Technology/Cengage Learning

Port	Protocol	Service	Description
20	FTP	FTP	File transfer data.
21	FTP	FTP	File transfer control information.
22	SSH	Secure Shell	Remote control to a networked computer that includes encrypting transmitted login information and data.
23	Telnet	Telnet	Remote control to a networked computer from a command prompt that does not use encryption.
25	SMTP	Email	Simple Mail Transfer Protocol; used by a client to send e-mail.
53	DNS	DNS server	Domain Name Service; used to find an IP address when a computer's character-based name is known.
80	HTTP	Web server	World Wide Web protocol.
110	POP3	Email	Post Office Protocol, version 3; used by a client to receive e-mail.
143	IMAP	Email	Internet Message Access Protocol, a newer protocol used by clients to receive e-mail.
443	HTTPS	Web server	HTTP with added security that includes authentication and encryption.
3389	RDP	Remote Desktop	Remote Desktop Protocol used to connect to a computer. Transmissions are encrypted. Remote Desktop and Remote Assistance both use RDP.

Table 17-3 Common TCP/IP port assignments for client/server applications

into a browser address box an IP address followed by a colon and then the port number. These values are known as a socket. For example, suppose a computer with an IP address of 136.60.30.5 is running an e-mail server application as well as a Web server application. If a client computer sends a request to 136.60.30.5:25, the e-mail server that is listening at that port responds. On the other hand, if a request is sent to 136.60.30.5:80, the Web server listening at port 80 responds (see Figure 17-34).

A+
220-701
4.1

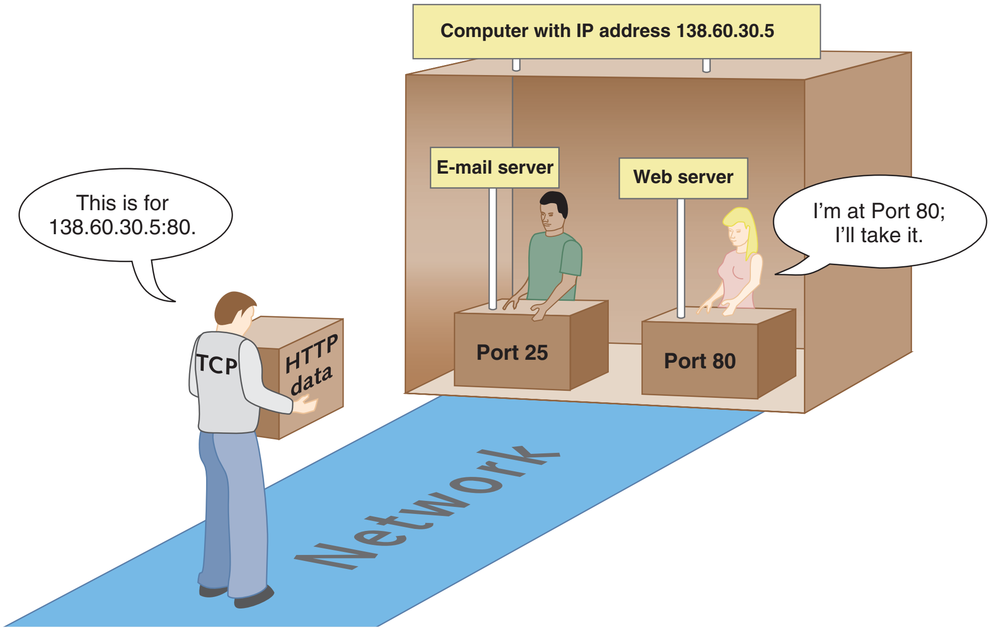

Computer with IP address 138.60.30.5
E-mail server
Web server
This is for 138.60.30.5:80.
I'm at Port 80; I'll take it.
TCP
HTTP data
Port 25
Port 80
Network

Figure 17-34 Each server running on a computer is addressed by a unique port number
Courtesy: Course Technology/Cengage Learning

A+ Exam Tip The A+ 220-701 Essentials exam expects you to know the common port assignments of the HTTP, FTP, POP, SMTP, Telnet, and HTTPS protocols.

Figure 17-35 shows how communication moves from a browser to the OS to the hardware on one computer and on to the hardware, OS, and Web server on a remote computer. As you connect a computer to a network, keep in mind that the connection must work at all three levels. And when things don't work right, it helps to understand that you must solve the problem at one or more levels. In other words, the problem might be with the physical equipment, with the OS, or with the application.

Now let's turn our attention to the details of understanding how IP addresses are used on a network.

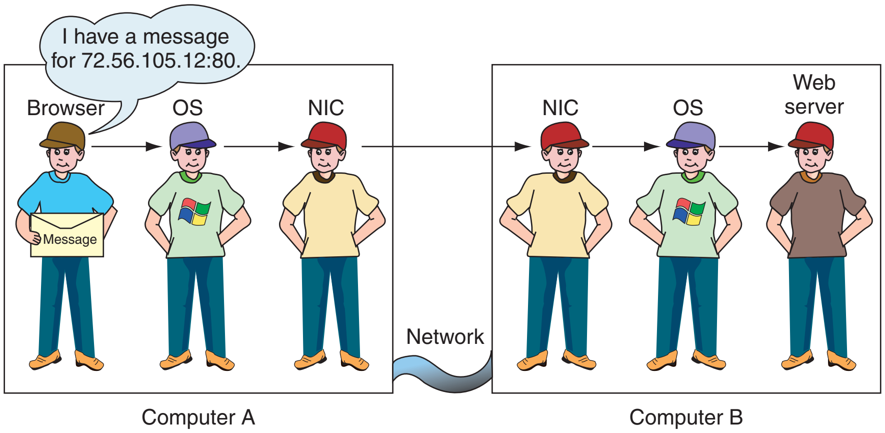


Figure 17-35 How a message gets from a browser to a Web server using three levels of communication
Courtesy: Course Technology/Cengage Learning

A+
220-701
4.1

UNDERSTANDING IP ADDRESSES AND HOW THEY ARE USED

All protocols of the TCP/IP suite identify a device on the Internet or an intranet by its IP address. (An **intranet** is a private network that uses the TCP/IP protocols.) An IP address is 32 bits long, made up of 4 bytes, each 8 bits long. When displayed, an IP address is expressed as four decimal numbers separated by periods, as in this address: 190.180.40.120. The largest possible 8-bit number is 11111111, which is equal to 255 in decimal, so the largest possible IP address in decimal is 255.255.255.255, which in binary is 11111111.11111111.11111111.11111111. Each of the four numbers separated by periods is called an **octet** (for 8 bits) and can be any number from 0 to 255, making a total of 4.3 billion potential IP addresses (256x256x256x256). Because of the allocation scheme used to assign these addresses, not all of them are available for use.

Notes The standard that determines an IP address has 32 bits is called the IPv4 (IP version 4) standard. Partly because of a potential shortage of IP addresses, the IPv6 (IP version 6) standard has been developed, which uses 128 bits for an IP address. Windows Vista and Windows XP with Service Pack 2 support IPv6, although 128-bit IP addresses are seldom used.

The first part of an IP address identifies the network, and the last part identifies the host. It's important to understand how the bits of an IP address are used, in order to understand how routing happens over interconnected networks such as the Internet, and how TCP/IP can locate an IP address anywhere on the globe. When data is routed over interconnected networks, the network portion of the IP address is used to locate the right network. After the data arrives at the local network, the host portion of the IP address is used to identify the one computer on the network that is to receive the data. Finally, the IP address of the host must be used to identify its MAC address so the data can travel on the host's LAN to that host. The next section explains this in detail.

CLASSES OF IP ADDRESSES

The Internet Corporation for Assigned Names and Numbers (ICANN) is responsible for keeping track of assigned IP addresses and domain names. IP addresses that are leased by companies and individuals through ICANN are divided into three classes: Class A, Class B, and Class C, based on the number of possible IP addresses in each network within each class. IP addresses are assigned to these classes according to the scheme outlined in Table 17-4.

Class	Network Octets*	Total Number of Possible Networks or Licenses	Total Number of Possible IP Addresses in Each Network
A	1.x.y.z to 126.x.y.z	127	16 million
B	128.0.x.y to 191.255.x.y	16,000	65,000
C	192.0.0.x to 223.255.255.x	2 million	254

*An x, y, or z in the IP address stands for an octet used to identify hosts.

Table 17-4 Classes of IP addresses

A+
220-701
4.1

You can determine the class of an IP address and the size or type of company to which an address is licensed by looking at the address. More important, you also can determine what portion of an IP address is dedicated to identifying the network and what portion is used to identify the host on that network.

A+ Exam Tip The A+ 220-701 Essentials exam expects you to know how to identify the class of any given IP address.

Figure 17-36 shows how each class of IP address is divided into the network and host portions. A Class A address uses the first (leftmost) octet for the network address and the remaining octets for host addresses. A Class A license assigns a single number that is used in the first octet of the address, which is the network address. The remaining three octets of the IP address can be used for host addresses that uniquely identify each host on this network. The first octet of a Class A license is a number between 0 and 126. For example, if a company is assigned 87 as its Class A network address, then 87 is used as the first octet for every host on this one network. Examples of IP addresses for hosts on this network are 87.0.0.1, 87.0.0.2, and 87.0.0.3. (The last octet does not use 0 or 255 as a value, so 87.0.0.0 is not valid.) In the example address 87.0.0.1, the 87 is the network portion of the IP address, and 0.0.1 is the host portion. Because three octets can be used for Class A host addresses, one Class A license can have approximately 256x256x254 host addresses, or about 16 million IP addresses. Only very large corporations with heavy communication needs have been able to obtain a Class A license.

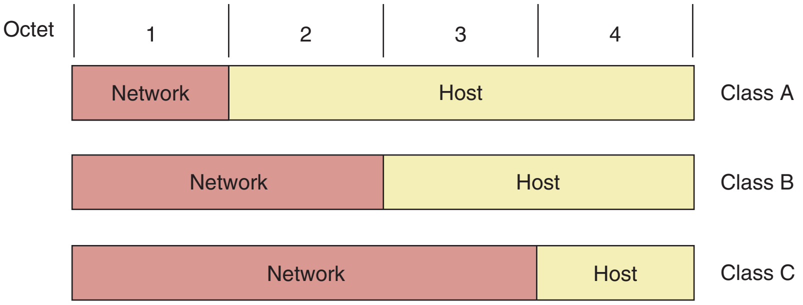


Figure 17-36 The network portion and host portion for each class of IP addresses
Courtesy: Course Technology/Cengage Learning

A Class B address uses the first two octets for the network portion and the last two for the host portion. A Class B license assigns a number for each of the two leftmost octets, leaving the third and fourth octets for host addresses. How many host addresses are there in one Class B license? The number of possible values for two octets is about 256x254, or about 65,000 host addresses in a single Class B license. (Some IP addresses are reserved, so these numbers are approximations.) The first octet of a Class B license is a number between 128 and 191, which gives about 63 different values for a Class B first octet. The second number can be between 0 and 255, so there are approximately 63x256, or about 16,000, Class B networks. For example, suppose a company is assigned 135.18 as the network address for its Class B license. The first two octets for all hosts on this network are 135.18, and the company uses the last two octets for host addresses. Examples of IP addresses on this company's Class B network are 135.18.0.1, 135.18.0.2, and 135.18.0.3. In the first example listed, 135.18 is the network portion of the IP address, and 0.1 is the host portion.

A+
220-701
4.1

A Class C license assigns three octets as the network address. With only one octet used for the host addresses, there can be only 254 host addresses on a Class C network. The first number of a Class C license is between 192 and 223. For example, if a company is assigned a Class C license for its network with a network address of 200.80.15, some IP addresses on the network would be 200.80.15.1, 200.80.15.2, and 200.80.15.3.

Class D and Class E IP addresses are not available for general use. Class D addresses begin with octets 224 through 239 and are used for **multicasting**, in which one host sends messages to multiple hosts, such as when the host transmits a video conference over the Internet. Class E addresses begin with 240 through 254 and are reserved for research.

SUBNET MASKS

The subnet mask used in the TCP/IP configuration for a network tells the OS which part of an IP address is the network portion and which part identifies the host. Using a subnet mask, a computer or other device can know if an IP address of another computer is on its network or another network (see Figure 17-37).

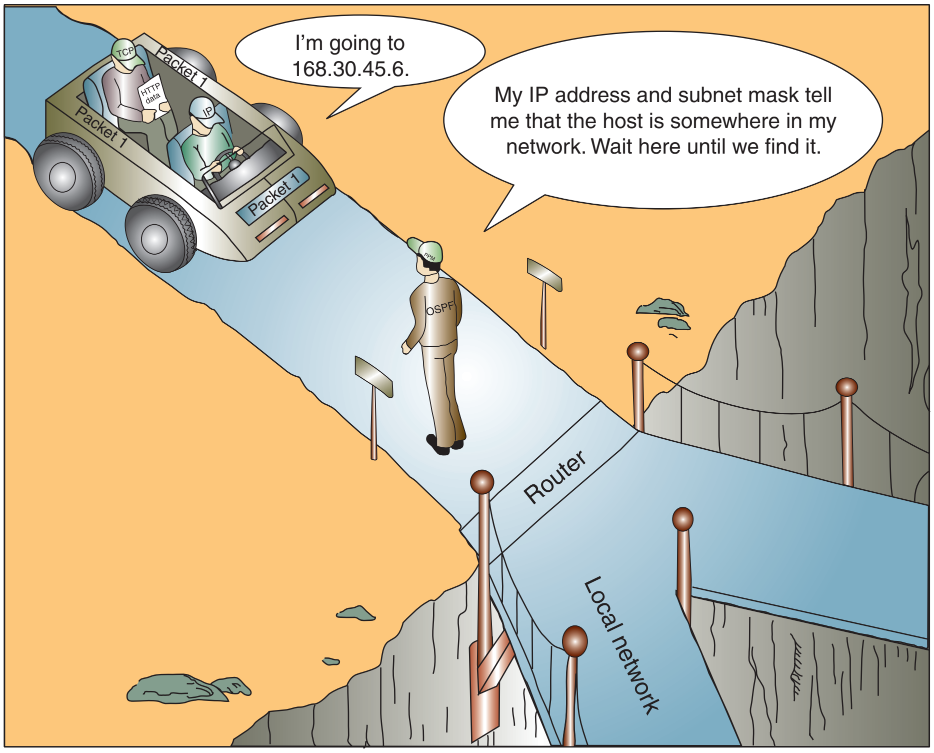

I'm going to 168.30.45.6.
My IP address and subnet mask tell me that the host is somewhere in my network. Wait here until we find it.
Packet 1
Packet 1
Packet 1
TCP
HTTP data
IP
OSPF
Router
Local network

Figure 17-37 A host (router, in this case) can always determine if an IP address is on its network
Courtesy: Course Technology/Cengage Learning

A subnet mask is a group of ones followed by a group of zeros. The ones in a subnet mask say, "On our network, this part of an IP address is the network part," and the group of zeros says, "On our network, this part of an IP address is the host part." For example, Table 17-5 shows the subnet masks that might be used for three IP addresses.

Class	Subnet Mask	Address	Network ID	Host ID
Class A	11111111.00000000.00000000.00000000	89.100.13.78	89	100.13.78
Class B	11111111.11111111.00000000.00000000	190.78.13.250	190.78	13.250
Class C	11111111.11111111.11111111.00000000	201.18.20.208	201.18.20	208

Table 17-5 Default subnet masks for classes of IP addresses

These three subnet masks would be displayed in a TCP/IP configuration window like this:

- Subnet mask of 11111111.00000000.00000000.00000000 is displayed as 255.0.0.0
- Subnet mask of 11111111.11111111.00000000.00000000 is displayed as 255.255.0.0
- Subnet mask of 11111111.11111111.11111111.00000000 is displayed as 255.255.255.0

Subnet masks that contain all ones or all zeros in an octet are called **classful subnet masks**, and the three subnet masks shown above are classful subnet masks. A **classless subnet mask** can have a mix of zeros and ones in one octet such as 11111111.11111111.11110000.00000000, which can be written as 255.255.240.0. These types of classless subnet masks are used to segment large corporate networks into subnetworks, or subnets, using a system called Classless Interdomain Routing (CIDR).

APPLYING CONCEPTS

Larry is setting up a new computer on a network. He creates TCP/IP settings to use static IP addressing. He assigns a subnet mask of 255.255.240.0 and an IP address of 15.50.212.59 to this computer. Suppose this computer wants to communicate with a computer assigned an IP address of 15.50.235.80. When the communication reaches the router controlling the network, the router must decide if these two computers are in the same subnet so that it will know how to route the request. The router compares the binary values of the first two octets and determines they match. It then compares the binary values of the third octet, like this:

```
212 = 11010100

235 = 11101011
```

To be in the same subnet, the first four bits must match, which they don't. Therefore, these two computers are not in the same subnet. The router then knows to route the data to another subnet. However, an IP address that is in the same subnet as 15.50.212.59 is 15.50.220.100, because the first two octets match and the first four bits of the third octet match (comparing 11010100 to 11011100).

Notes Sometimes using CIDR notation, an IP address and subnet mask are written using a shorthand notation like this: 15.50.212.59/20, where the /20 means that the subnet mask is written as 20 ones followed by enough zeros to complete the full 32 bits.

A+
220-701
4.1

DIFFERENT WAYS OF ASSIGNING IP ADDRESSES

When a small company is assigned a Class C license, it obtains 254 IP addresses for its use. If it has only a few hosts (for example, fewer than 25 on a network), many IP addresses go unused, which is one reason there is a shortage of IP addresses. But suppose that the company grew and now has 300 workstations on the network and is running out of IP addresses. There are two approaches to solving this problem: Use private IP addresses or use dynamic IP addressing. Many companies combine both methods. An explanation of each of these solutions follows.

Public, Private, and Reserved IP Addresses

When a company applies for a Class A, B, or C license, it is assigned a group of IP addresses that are different from all other IP addresses and are available for use on the Internet. The IP addresses available to the Internet are called **public IP addresses**.

One thing to consider, however, is that not all of a company's workstations need to have Internet access, even though they might be on the network. So, although each workstation might need an IP address to be part of the TCP/IP network, those not connected to the Internet don't need addresses that are unique and available to the Internet; these workstations can use private IP addresses. **Private IP addresses** are IP addresses used on private intranets that are not allowed on the Internet. A computer using a private IP address on a private network can still access the Internet if a router or other device that stands between the network and the Internet is using NAT redirection. Recall that when using NAT redirection, the device substitutes its own public IP address for the private IP address of a computer behind the firewall.

Because of NAT redirection, a small company can rely solely on private IP addresses for its internal network and use only the s one public IP address assigned to it by its ISP for Internet communication. IEEE recommends that the following IP addresses be used for private networks :

- 10.0.0.0 through 10.255.255.255
- 172.16.0.0 through 172.31.255.255
- 192.168.0.0 through 192.168.255.255

Notes IEEE, a nonprofit organization, is responsible for many Internet standards. Standards are proposed to the networking community in the form of an RFC (Request for Comment). RFC 1918 outlines recommendations for private IP addresses. To view an RFC, visit the Web site *www.rfc-editor.org*.

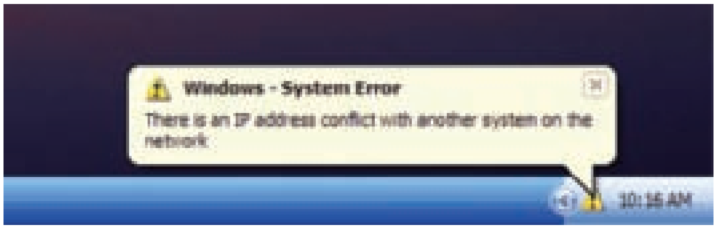
When assigning isolated IP addresses, also keep in mind that a few IP addresses are reserved for special use by TCP/IP and should not be assigned to a device on a network. Table 17-6 lists these reserved IP addresses.

IP Address	How It Is Used
255.255.255.255	Broadcast messages
0.0.0.0	Currently unassigned IP address
127.0.0.1	Indicates your own workstation and is called the loopback address

Table 17-6 Reserved IP addresses

A+
220-701
4.1

All IP addresses on a network must be unique for that network. (Figure 17-38 shows the Windows XP error that appears when two computers on the network have been assigned the same IP address.) A network administrator might assign an IP address to a stand-alone computer (for example, if someone is testing networking software on a PC that is not connected to the network). As long as the network is a private network, the administrator can assign any IP address, although a good administrator avoids using the reserved addresses.



Windows - System Error

There is an IP address conflict with another system on the network

Figure 17-38 An error occurs when two networked computers use the same IP address
Courtesy: Course Technology/Cengage Learning

Dynamically Assigned IP Addresses

If an administrator must configure each host on a network manually, assigning it a unique IP address, the task of going from PC to PC to make these assignments and keeping up with which address is assigned to which PC can be an administrative nightmare. The solution is to have a server automatically assign an IP address to a workstation each time it comes onto the network. Instead of permanently assigning a **static IP address** to a workstation, a **dynamic IP address** is assigned for the current connection only. When the connection terminates, the IP address is returned to the list of available addresses.

When a workstation has an IP address assigned to it, it is said that the workstation is leasing the IP address. An ISP customarily uses dynamic IP addressing for its individual subscribers and static IP addresses for its business subscribers.

Recall that a DHCP server manages dynamically assigned IP addresses on a network. Workstations that work with DHCP servers are called DHCP clients. DHCP software resides on both the client and the server to manage the dynamic assignments of IP addresses. DHCP client software is built into Windows.

A+ Exam Tip The A+ 220-701 Essentials exam expects you to know what a DHCP server is and understand how to use static and dynamic IP addressing.

When you configure a DHCP server, you specify the range of IP addresses that can be assigned to clients on the network. Figure 17-39 shows the configuration window for a DHCP server embedded as firmware on a router. In the figure, you can see that the router's IP address is 192.168.1.1, and the starting IP address to be assigned to clients is 192.168.1.100. Because the administrator specified that the server can have up to 50 clients, the range of IP addresses is, therefore, 192.168.1.100 to 192.168.1.149. Also shown in the figure is a list of currently assigned IP addresses and the MAC address of the computer that currently leases that IP address.

When a PC first connects to the network, it attempts to lease an address from the DHCP server. If the attempt fails, it uses an **Automatic Private IP Address (APIPA)** in the address range 169.254.*x*.*y*. How to configure a Windows workstation to use dynamic or static IP addressing is covered later in the chapter.

A+
220-701
4.1

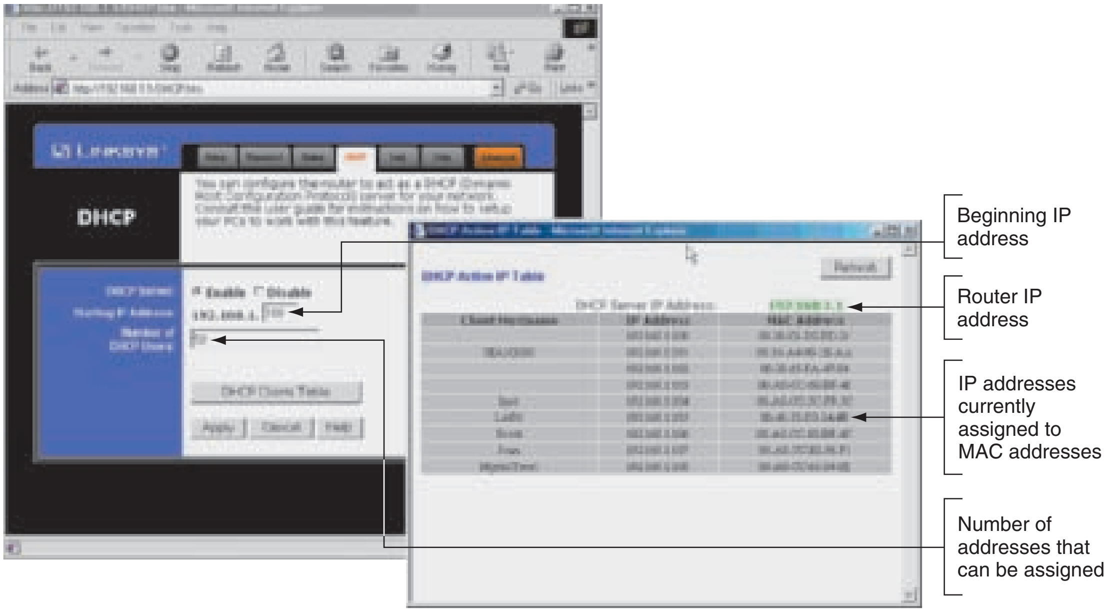


Figure 17-39 A DHCP server has a range of IP addresses it can assign to clients on the network
Courtesy: Course Technology/Cengage Learning

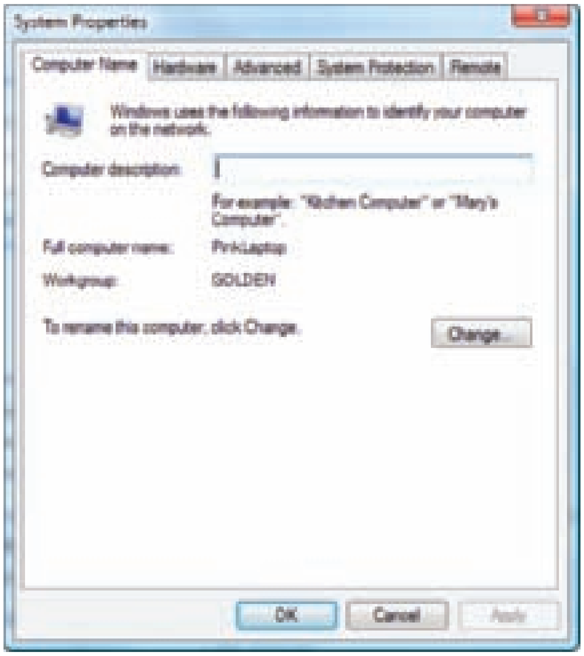
Now let's see how character-based names can be used in place of IP addresses to identify computers and networks.

CHARACTER-BASED NAMES IDENTIFY COMPUTERS AND NETWORKS

Remembering an IP address is not always easy, so character-based names are used to substitute for IP addresses. Here are the possibilities:

- A host name, also called a computer name, is the name of a computer and can be used in place of its IP address. Examples of host names are www, ftp, Jean's Computer, TestBox3, and PinkLaptop. You assign a host name to a computer when you first configure it for a network connection. The name can have up to 63 characters, including letters, numbers, and special characters. On a local network, you can use the computer name in the place of an IP address to identify a computer. To find out and change the computer name in Vista, click **Start**, right-click **Computer** and select **Properties** from the shortcut menu. In the System window, click **Advanced system settings** and respond to the UAC box. In the System Properties box, click the **Computer Name** tab (see Figure 17-40). For XP, click **Start**, right-click **My Computer**, and select **Properties** from the shortcut menu. Then click the **Computer Name** tab.
- A NetBIOS name can be up to 15 characters. NetBIOS (Network Basic Input/Output System) is a protocol that applications use to communicate with each other. NetBIOS was used by a Windows networking protocol called NetBEUI (NetBIOS Extended User Interface, pronounced *net-BOO-ee*). NetBEUI has been replaced by TCP/IP, and NetBIOS names are only used when the network is supporting a legacy application that requires a computer name no longer than 15 characters.
- A workgroup name identifies a workgroup. The workgroup name is only recognized within the local network.

A+
220-701
4.1



Windows uses the following information to identify your computer on the network.

Computer description:

For example: "Kitchen Computer" or "Mary's Computer".

Full computer name: PinkLaptop

Workgroup: GOLDEN

To rename this computer, click Change.

Figure 17-40 View and change the computer name
Courtesy: Course Technology/Cengage Learning

- A **domain name** identifies a network. Examples of domain names are the names that appear before the period in microsoft.com, course.com, and mycompany.com. The letters after the period are called the top-level domain and tell you something about the domain. Examples are .com (commercial), .org (nonprofit), .gov (government), and .info (general use).
- A **fully qualified domain name (FQDN)** identifies a computer and the network to which it belongs. An example of an FQDN is www.course.com. The host name is *www* (a Web server), *course* is the domain name, and *com* is the top-level domain name of the Course Technology network. Another FQDN is *joesmith.mycompany.com*.

On the Internet, a fully qualified domain name must be associated with an IP address before this computer can be found. This process of associating a character-based name with an IP address is called **name resolution**. The protocol and service used to track these names are called **DNS (Domain Name System**, also called **Domain Name Service)**. A **DNS server** can find an IP address for a computer when the fully qualified domain name is known. (An older proprietary Microsoft service used to track NetBIOS names is WINS (Windows Internet Naming Service). Your ISP is responsible for providing you access to one or more DNS servers as part of the service it provides for Internet access. When a Web hosting site first sets up your Web site, IP address, and domain name, it is responsible for entering the name resolution information into its primary DNS server. This server can present the information to other DNS servers on the Web and is called the authoritative name server for your site.

Notes When you enter a fully qualified domain name such as www.microsoft.com in a browser address bar, that name is translated into an IP address followed by a port number. It's interesting to know that you can skip the translation step and enter the IP address and port number in the address box. See Figure 17-41.

A+
220-701
4.1

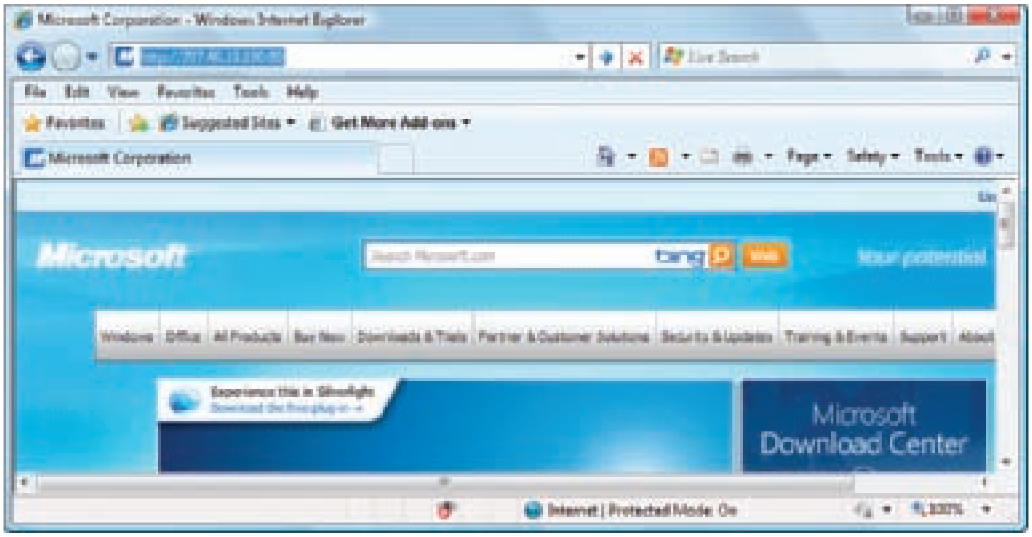

Microsoft Corporation - Windows Internet Explorer
File Edit View Favorites Tools Help
Favorites
Suggested Sites
Get More Add-ons
Microsoft Corporation
Page
Safety
Tools
Live Search
Microsoft
Search Microsoft.com
bing
Windows Office All Products Buy Now Downloads & Trials Partner & Customer Solutions Security & Updates Training & Events Support About
Experience this in Silverlight
Microsoft Download Center
Internet | Protected Mode: On
100%

Figure 17-41 A Web site can be accessed by its IP address and port number
Courtesy: Course Technology/Cengage Learning

A+ Exam Tip The A+ 220-701 Essentials exam expects you to be familiar with a DNS service.

When Windows is trying to resolve a computer name to an IP address, it first looks in the **Hosts file** in the C:\Windows\System32\drivers\etc folder. This file, which has no file extension, contains computer names and their associated IP addresses on the local network. An administrator is responsible for manually editing the hosts file when the association is needed on the local network. If the computer name is not found in the hosts file, Windows then turns to a DNS server if it has the IP address of the server. For NetBIOS names, Windows first looks for entries in the LMHosts file in the C:\Windows\System32\drivers\etc folder before it turns to a WINS server to resolve the NetBIOS name.

Notes For an entry in the Hosts file to work, the remote computer must always use the same IP address. One way to accomplish this is to assign a static IP address to the computer. Alternately, if your DHCP server supports this feature, you can configure it to assign the same IP address to this computer each time if you tell the DHCP server the computer's MAC address. This method of computer name resolution is often used for intranet Web servers, Telnet servers, and other servers.

TCP/IP PROTOCOL LAYERS

Recall that a protocol is an agreed-to set of rules for communication between two parties. Operating systems and client/server applications on the Internet all use protocols that are supported by TCP/IP. The left side of Figure 17-42 shows these different layers of protocols and how they relate to one another. As you read this section, this figure can serve as your road map to the different protocols.

A+
220-701
4.1

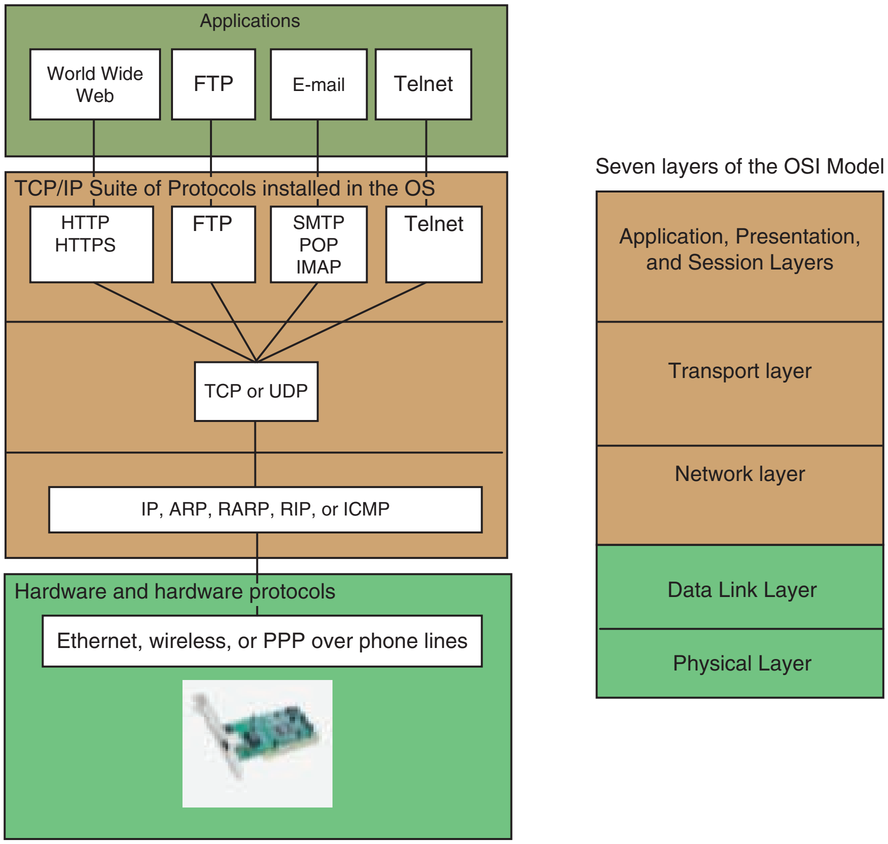

Applications
World Wide Web
FTP
E-mail
Telnet
TCP/IP Suite of Protocols installed in the OS
HTTP
HTTPS
FTP
SMTP
POP
IMAP
Telnet
TCP or UDP
IP, ARP, RARP, RIP, or ICMP
Hardware and hardware protocols
Ethernet, wireless, or PPP over phone lines
Seven layers of the OSI Model
Application, Presentation, and Session Layers
Transport layer
Network layer
Data Link Layer
Physical Layer

Figure 17-42 How software, protocols, and technology on a TCP/IP network relate to each other
Courtesy: Course Technology/Cengage Learning

Notes When studying networking theory, the OSI Model is used, which divides network communication into seven layers. In the OSI Model, protocols used by hardware are divided into two layers (data link and physical), and TCP/IP protocols used by the OS are divided into five layers (network, transport, session, presentation, and application). These seven layers are shown on the right side of Figure 17-42.

In the following sections, the more significant applications and operating system protocols are introduced. However, you should know that the TCP/IP protocol suite includes more protocols than just those mentioned in this chapter; some of them are shown in Figure 17-42.

TCP/IP PROTOCOLS USED BY APPLICATIONS

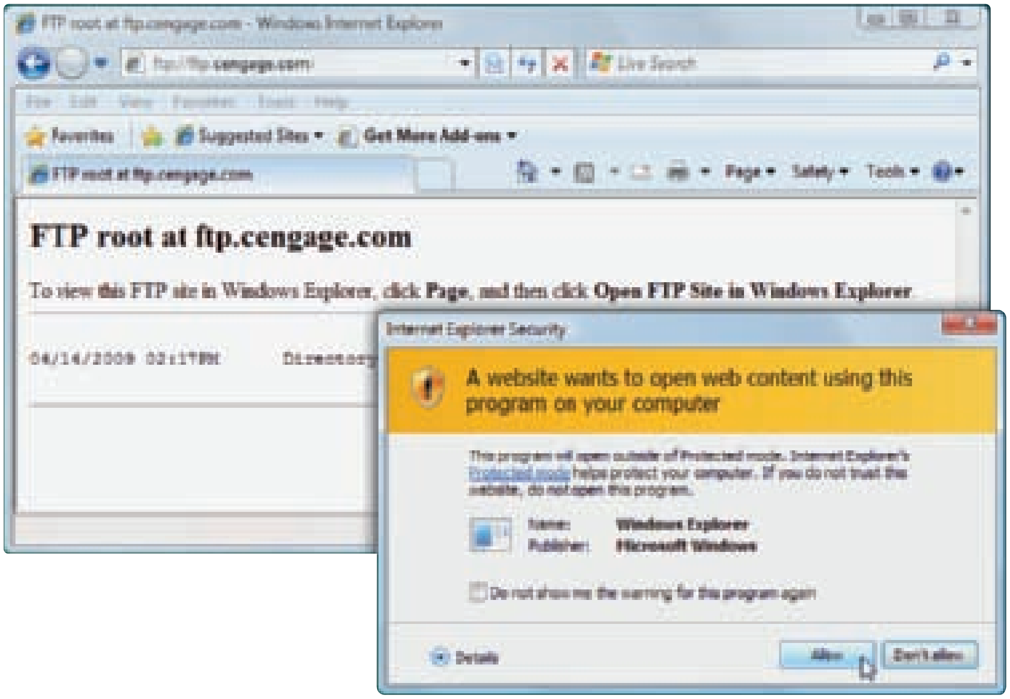
Some common applications that use the Internet are Web browsers, e-mail, chat, FTP, Telnet, Remote Desktop, and Remote Assistance. When one of these applications wants to send data to a counterpart application on another host, it makes an API (application programming interface) call to the operating system, which handles the request. (An API call is a common way for an application to ask an operating system to do something.) The API call causes the OS to generate a request. Here is a bit of information about several of these application protocols:

- *HTTP*. **HTTP (Hypertext Transfer Protocol)** is the protocol used for the World Wide Web and used by Web browsers and Web servers to communicate. You can see when a

A+
220-701
4.1

browser is using this protocol by looking for http at the beginning of a URL in the address bar of a browser, such as *http://www.microsoft.com*.

- *HTTPS*. The HTTPS (HTTP secure) protocol is used by Web browsers and servers to encrypt the data before it is sent and then decrypt it before the data is processed. To know this secure protocol is being used, look for https in the URL, as in *https://www.wachovia.com*.
- *FTP*. FTP (File Transfer Protocol) is used to transfer files between two computers. Web browsers can use the protocol. Also, special FTP client software such as CuteFTP by GlobalSCAPE (*www.cuteftp.com*) can be used, as the software offers more features for file transfer than does a browser. To use FTP from your browser, enter the address of an FTP site in the address box. When the browser recognizes the site is using the FTP protocol, you will see ftp in the URL, as in *ftp://ftp.cengage.com*. Sometimes it's easier to use Windows Explorer to transfer files rather than Internet Explorer. To use Windows Explorer for file transfers in Windows Vista, on the menu bar of Internet Explorer, click **Page**, **Open FTP site in Windows Explorer**. Then click **Allow** in the Internet Explorer Security box (see Figure 17-43). Windows Explorer opens, showing files and folders on the FTP site. Using Windows XP, Internet Explorer works similar to Windows Explorer when you navigate to an FTP site.



FTP root at ftp.cengage.com - Windows Internet Explorer
ftp://ftp.cengage.com
Live Search
File Edit View Favorites Tools Help
Favorites
Suggested Sites
Get More Add-ons
FTP root at ftp.cengage.com
Page
Safety
Tools
Internet Explorer Security
Details
Allow
Don't allow

FTP root at ftp.cengage.com

To view this FTP site in Windows Explorer, click **Page**, and then click **Open FTP Site in Windows Explorer**

```
04/14/2009 02:17PM      Directory
```

A website wants to open web content using this program on your computer

This program will open outside of Protected mode. Internet Explorer's Protected mode helps protect your computer. If you do not trust the website, do not open this program.

Name: Windows Explorer
Publisher: Microsoft Windows

□ Do not show me the warning for this program again

Figure 17-43 Open Windows Explorer to transfer files using FTP
Courtesy: Course Technology/Cengage Learning

- *SMTP*. SMTP (Simple Mail Transfer Protocol) is used to send an e-mail message to its destination (see Figure 17-44). An improved version of SMTP is SMTP AUTH (SMTP Authentication). This protocol is used to authenticate a user to an e-mail server when the e-mail client first tries to connect to the e-mail server to send e-mail. Using SMTP AUTH, an extra dialogue between the client and server happens before the client can fully connect that proves the client is authorized to use the service. After authentication, the client can then send e-mail to the e-mail server. The e-mail server that takes care of sending e-mail messages (using the SMTP protocol) is often referred to as the SMTP server.

A+
220-701
4.1

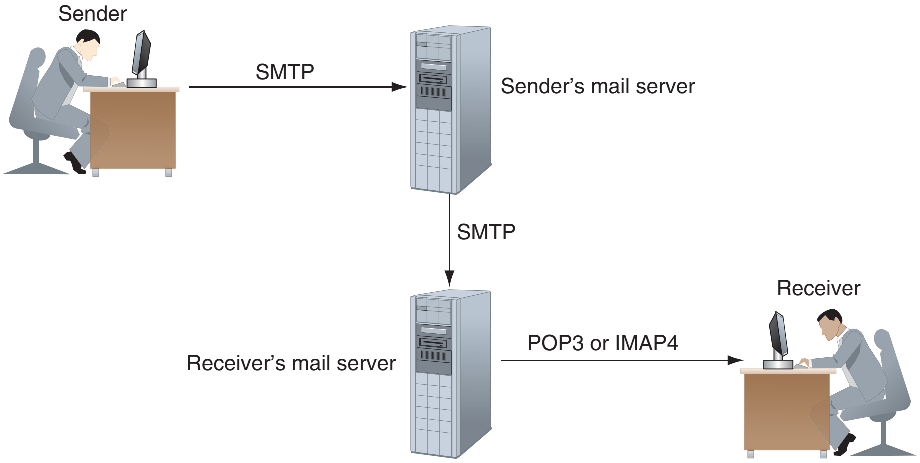


Figure 17-44 The SMTP protocol is used to send e-mail to a recipient's mail server, and the POP3 or IMAP4 protocol is used to download e-mail to the client
Courtesy: Course Technology/Cengage Learning

- *POP and IMAP.* After an e-mail message arrives at the destination e-mail server, it remains there until the recipient requests delivery. The recipient's e-mail server uses one of two protocols to deliver the message: POP3 (Post Office Protocol, version 3) or IMAP4 (Internet Message Access Protocol, version 4), which is a newer e-mail protocol. IMAP is slowly replacing POP for receiving e-mail. IMAP gives more control over how e-mail is stored on the server and client machines.
- *Telnet.* The Telnet protocol is used by the Telnet client/server applications to allow an administrator or other user to control a computer remotely.

TCP/IP PROTOCOLS USED BY THE OS

Looking back at Figure 17-42, you can see three layers of protocols between the applications and the hardware protocols. These three layers make up the heart of TCP/IP communication. In the figure, TCP or UDP manages communication with the applications protocols above them as well as the protocols shown underneath TCP and UDP, which control communication on the network.

Remember that all communication on a network happens by way of packets delivered from one location on the network to another. When a Web browser makes a request for data from a Web server, a packet is created and an attempt is made to deliver that packet to the server. In TCP/IP, the protocol that guarantees packet delivery is TCP (Transmission Control Protocol). TCP makes a connection, 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 e-mail. Guaranteed delivery takes longer and is used when it is important to know that the data reached its destination.

On the other hand, 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 a best-effort protocol. UDP is primarily used for broadcasting and other types of transmissions, such as streaming video or sound over the Web, where guaranteed delivery is not as important as fast transmission.

For TCP to guarantee delivery, it uses IP to establish a session between client and server to verify that communication has taken place. When a TCP packet reaches its destination, an acknowledgment is sent back to the source (see Figure 17-45). If the source TCP does not receive the acknowledgment, it resends the data or passes an error message back to the higher-level application protocol.

A+
220-701
4.1

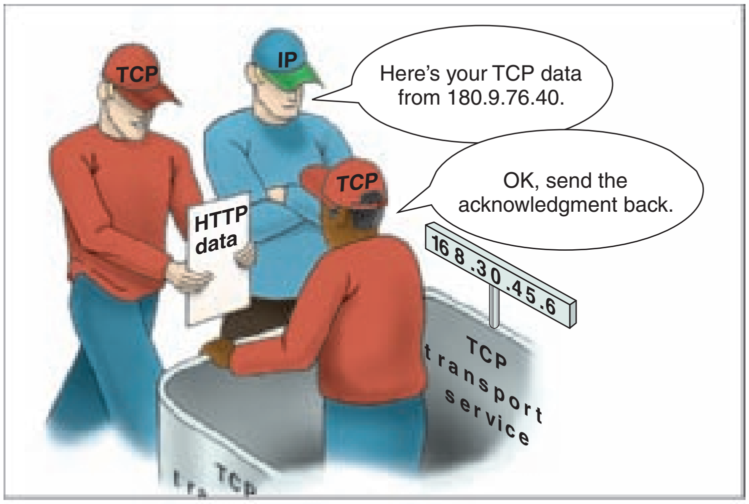

TCP
IP
Here's your TCP data from 180.9.76.40.
TCP
OK, send the acknowledgment back.
HTTP data
168.30.45.6
TCP transport service
TCP

Figure 17-45 TCP guarantees delivery by requesting an acknowledgment
Courtesy: Course Technology/Cengage Learning

A+
220-701
4.1
3.2

PING, IPCONFIG, AND TELNET

Three TCP/IP utilities used to solve problems with TCP/IP and communicate on a TCP/IP network are Ping, Ipconfig, and Telnet. In this part of the chapter, you will learn to use all three. In the next chapter, you will learn about other TCP/IP utilities and how to use them when troubleshooting a network or Internet connection.

USE PING TO TEST FOR CONNECTIVITY

The **Ping (Packet InterNet Groper)** command tests connectivity by sending an echo request to a remote computer. If the remote computer is online and detects the signal, it responds to the ping. When testing for connectivity or problems with name resolution, Ping should be the first tool you use. A few examples are shown in Table 17-7. The first two examples are shown in Figure 17-46.

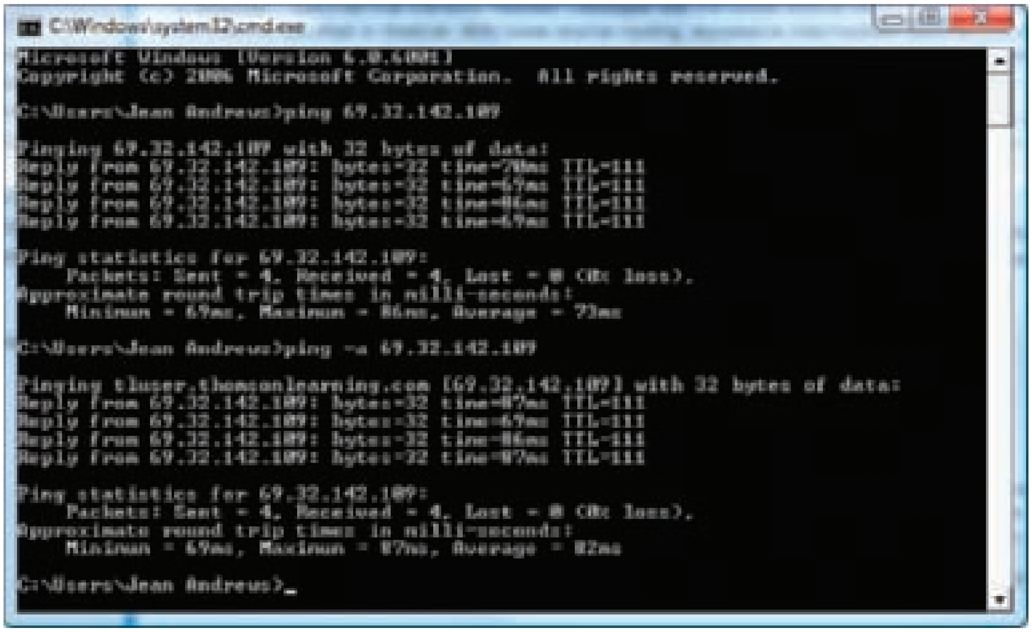
Ping Command	Description
Ping 69.32.142.109	To test for connectivity using an IP address. If the remote computer responds, the round-trip times are displayed.
Ping –a 69.32.142.109	The –a parameter tests for name resolution. Use it to display the host name and verify DNS is working.
Ping –t 69.32.142.109	The –t parameter causes pinging to continue until interrupted. To display statistics, press Ctrl-Break. To stop pinging, press Ctrl-C.
Ping –l 6500 69.32.142.109	The –l parameter changes the size of the data packet sent with the ping. Default size is 32 bytes, and the size can be up to 65,527 bytes.
Ping 127.0.0.1	A loopback address test. The IP address 127.0.0.1 always refers to the local computer. If the local computer does not respond, you can assume there is a problem with the TCP/IP configuration.
Ping www.course.com	Use a host name to find out the IP address of a remote computer. If the computer does not respond, assume there is a problem with DNS. On the other hand, some computers are not configured to respond to pings.

Table 17-7 Examples of the Ping command

17

A+ 220-701

A+
220-701
4.1
3.2



```
Microsoft Windows [Version 6.0.6001]
Copyright (c) 2006 Microsoft Corporation.  All rights reserved.

C:\Users\Jean Andrews>ping 69.32.142.109

Pinging 69.32.142.109 with 32 bytes of data:
Reply from 69.32.142.109: bytes=32 time=70ms TTL=111
Reply from 69.32.142.109: bytes=32 time=69ms TTL=111
Reply from 69.32.142.109: bytes=32 time=86ms TTL=111
Reply from 69.32.142.109: bytes=32 time=69ms TTL=111

Ping statistics for 69.32.142.109:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 69ms, Maximum = 86ms, Average = 73ms

C:\Users\Jean Andrews>ping -a 69.32.142.109

Pinging tluser.thomsonlearning.com [69.32.142.109] with 32 bytes of data:
Reply from 69.32.142.109: bytes=32 time=87ms TTL=111
Reply from 69.32.142.109: bytes=32 time=69ms TTL=111
Reply from 69.32.142.109: bytes=32 time=86ms TTL=111
Reply from 69.32.142.109: bytes=32 time=87ms TTL=111

Ping statistics for 69.32.142.109:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 69ms, Maximum = 87ms, Average = 82ms

C:\Users\Jean Andrews>_
```

Figure 17-46 Use the Ping command to test for connectivity and name resolution
Courtesy: Course Technology/Cengage Learning

USE IPCONFIG TO TROUBLESHOOT TCP/IP CONFIGURATION

The Ipconfig command can display TCP/IP configuration information and refresh the IP address. When using the Ipconfig command in Vista, use an elevated command prompt window. Some examples of the command are listed in Table 17-8.

Ipconfig Command	Description
Ipconfig /all	Displays TCP/IP information (see Figure 17-47).
Ipconfig /release	Release the IP address when dynamic IP addressing is being used.
Ipconfig /renew	Lease a new IP address from a DHCP server.
Ipconfig /displaydns	Displays information about name resolutions that Windows currently holds in the DNS resolver cache.
Ipconfig /flushdns	Flushes the name resolver cache, which might solve a problem when the browser cannot find a host on the Internet.

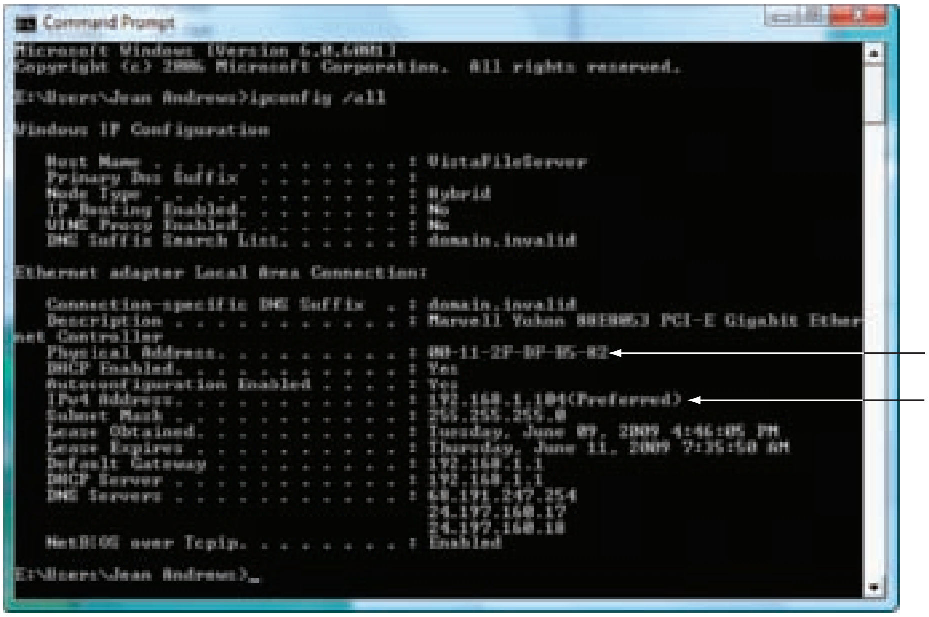
Table 17-8 Examples of the Ipconfig command

USE TELNET TO COMMUNICATE WITH A REMOTE COMPUTER

Using Telnet, a user connects to a remote computer and controls it through the command prompt window provided by Telnet. Telnet was once a popular method for an administrator to connect to a server to troubleshoot a problem on the server. However, because Telnet only provides a command-line interface and is not secure, other methods such as Remote Assistance and Remote Desktop are becoming more popular than Telnet. You will learn to use these tools in the next chapter.

A+ Exam Tip The A+ 220-701 Essentials exam expects you to be able to use a Telnet interface as well as the Ping and Ipconfig utilities.

A+
220-701
4.1
3.2



```
Microsoft Windows [Version 6.0.6001]
Copyright (c) 2006 Microsoft Corporation.  All rights reserved.

E:\Users\Jean Andrews>ipconfig /all

Windows IP Configuration

   Host Name . . . . . . . . . . . . : VistaFileServer
   Primary Dns Suffix  . . . . . . . :
   Node Type . . . . . . . . . . . . : Hybrid
   IP Routing Enabled. . . . . . . . : No
   WINS Proxy Enabled. . . . . . . . : No
   DNS Suffix Search List. . . . . . : domain.invalid

Ethernet adapter Local Area Connection:

   Connection-specific DNS Suffix  . : domain.invalid
   Description . . . . . . . . . . . : Marvell Yukon 88E8053 PCI-E Gigabit Ether
net Controller
   Physical Address. . . . . . . . . : 00-11-2F-DF-B5-82
   DHCP Enabled. . . . . . . . . . . : Yes
   Autoconfiguration Enabled . . . . : Yes
   IPv4 Address. . . . . . . . . . . : 192.168.1.104(Preferred)
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Lease Obtained. . . . . . . . . . : Tuesday, June 09, 2009 4:46:05 PM
   Lease Expires . . . . . . . . . . : Thursday, June 11, 2009 7:35:58 AM
   Default Gateway . . . . . . . . . : 192.168.1.1
   DHCP Server . . . . . . . . . . . : 192.168.1.1
   DNS Servers . . . . . . . . . . . : 68.191.247.254
                                       24.197.160.17
                                       24.197.160.18
   NetBIOS over Tcpip. . . . . . . . : Enabled

E:\Users\Jean Andrews>_
```

Figure 17-47 Results of the ipconfig /all command
Courtesy: Course Technology/Cengage Learning

Here are some tips about using Telnet:

- Telnet is a client/server application. That means one computer (the remote computer) is running the Telnet server and another computer (the local computer) runs the Telnet client. The Telnet server must be configured on Windows Vista Business or Ultimate editions or Windows XP Professional. Any Windows computer can run the Telnet client.
- For a user to log into a remote computer using Telnet, the user account must belong to the TelnetClients group. This user account and password must match the account and password used on the local computer.
- The Telnet server application must be running on the remote computer before you use Telnet. The service can be started from the Services console and set to start automatically or manually.
- By default, the Telnet client and server applications are installed on Windows XP, but not on Vista. For Vista, you must manually install the server and/or client.

Some Telnet commands are listed in Table 17-9.

Telnet Command	Explanation
Set localecho	Displays command responses that are given by the remote computer.
Set ntlm	Uses NTLM to authenticate login account and password. NTLM is a Windows authentication protocol for user IDs and passwords.
Open <*host name*> [*port*]	Connect to the remote computer. Use either the IP address or computer name to identify the computer. If you don't specify a port, port 23 will be used.
Close	Closes the current connection to a remote computer.
Quit	Closes the Telnet window.

Table 17-9 Telnet commands (continued)

A+
220-701
4.1
3.2

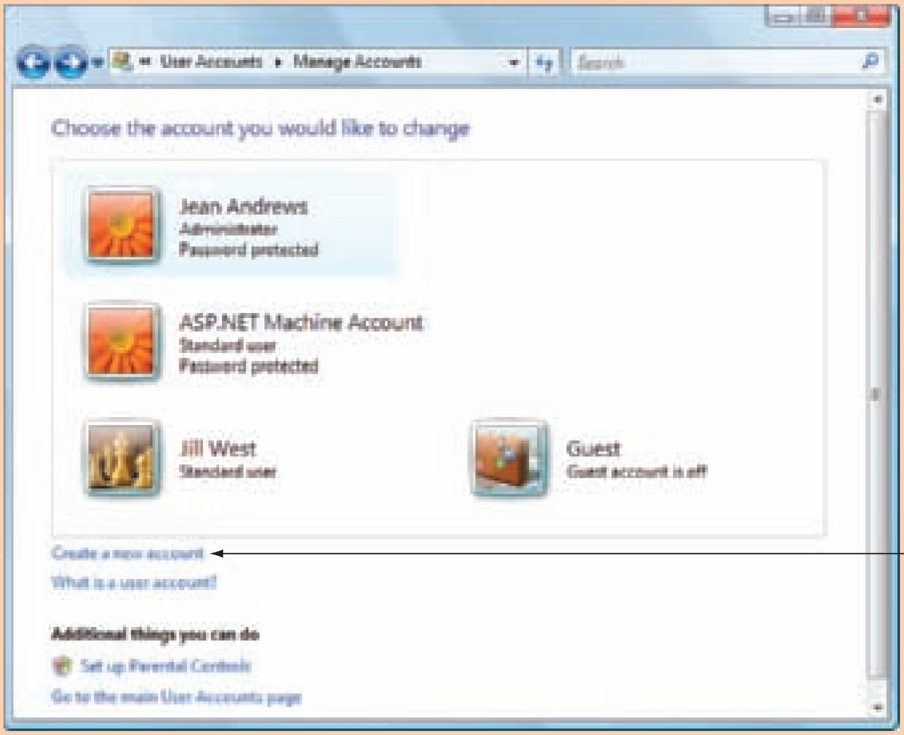
Telnet Command	Explanation
Ctrl+]	Switch from the remote computer session mode window to the Telnet command mode window.
Press the Enter key	Switch from the Telnet command mode window to the remote computer session mode window.

Table 17-9 Telnet commands

APPLYING CONCEPTS

To use Telnet, you need a user account and password that match on both computers. User accounts can be created using the Control Panel for all versions of Windows or using Computer Management for Vista Ultimate and Business editions or for XP Professional. If you need to create a new user account on either computer, follow these steps using Control Panel:

1. For Vista, click **Add or remove user accounts** in Control Panel and respond to the UAC box. In the Manage Accounts window, click **Create a new account** (see Figure 17-48).

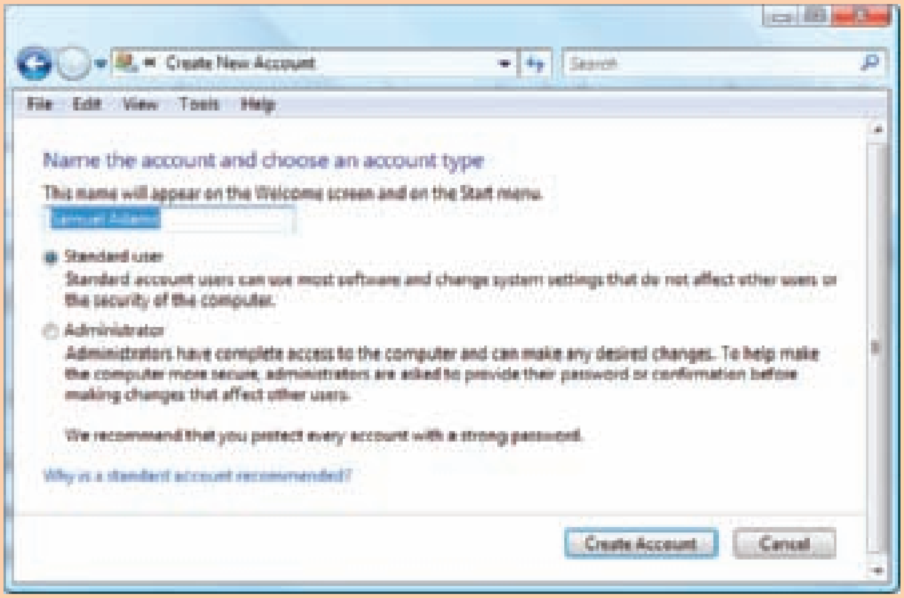

Choose the account you would like to change

To create a new account

Figure 17-48 Create a new user account
Courtesy: Course Technology/Cengage Learning

2. In the next window, enter the user name (see Figure 17-49). Select if the account will be a Standard or Administrator account. A standard account has fewer privileges than an administrator account, but either account type can use Telnet. Click **Create Account**.
3. To create a password for the account, in the Manage Account box, click the account icon and click **Create a password** on the next box. Enter the new password and click **Create password**.

A+
220-701
4.1
3.2



Create New Account

Search

Name the account and choose an account type

This name will appear on the Welcome screen and on the Start menu.

[illegible]

● Standard user

Standard account users can use most software and change system settings that do not affect other users or the security of the computer.

○ Administrator

Administrators have complete access to the computer and can make any desired changes. To help make the computer more secure, administrators are asked to provide their password or confirmation before making changes that affect other users.

We recommend that you protect every account with a strong password.

Why is a standard account recommended?

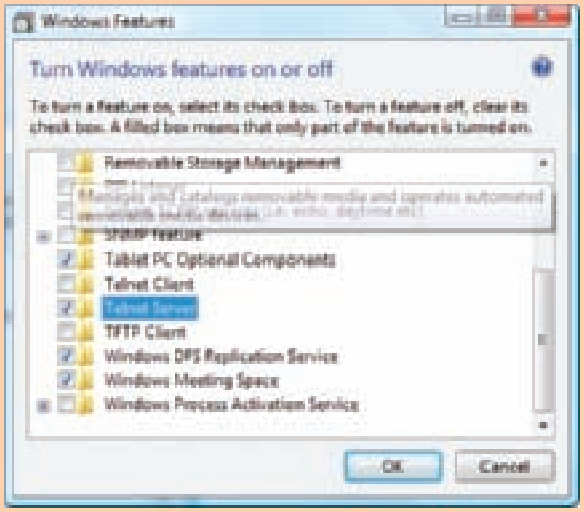
Figure 17-49 Decide the privilege level for the new account
Courtesy: Course Technology/Cengage Learning

To create a new account in Windows XP, open the **User Accounts** applet in Control Panel and click **Create a new account**. Enter an account name and click **Next**. For the privilege level of the account, select either Computer administrator or Limited. Click **Create Account**.

Using two computers that are networked together, you can use the following steps to practice using Telnet. The remote computer must use Windows XP Professional or Windows Vista Ultimate or Business. On the remote computer, follow these steps to configure and start the Telnet server application:

1. If you are using Vista, you need to install the Telnet server application. To do that, open the Control Panel and click **Programs**. Then click **Turn Windows features on or off** and respond to the UAC box.

2. In the Windows Features box, check **Telnet Server** (see Figure 17-50). Click **OK**. (For XP, the Telnet server and client are installed by default.)



Windows Features

Turn Windows features on or off

To turn a feature on, select its check box. To turn a feature off, clear its check box. A filled box means that only part of the feature is turned on.

□ Removable Storage Management

Manages and catalogs removable media and operates automated removable media devices.

□ SNMP feature

☑ Tablet PC Optional Components

□ Telnet Client

☑ Telnet Server

□ TFTP Client

☑ Windows DFS Replication Service

☑ Windows Meeting Space

□ Windows Process Activation Service

Figure 17-50 Turn on the Telnet client and server applications
Courtesy: Course Technology/Cengage Learning

A+
220-701
4.1
3.2

3. To add the user account to the TelnetClients group, enter **Compmgmt.msc** in the Vista Start Search box or the XP Run box and press **Enter**. For Vista, respond to the UAC box. The Computer Management console opens (see the left side of Figure 17-51).

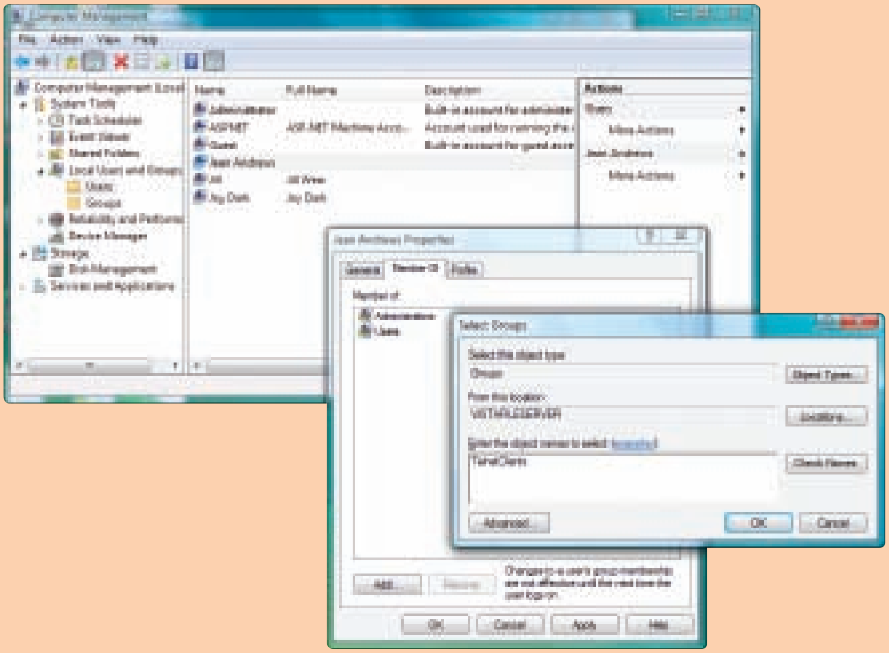


Figure 17-51 Add the user to the TelnetClients group
Courtesy: Course Technology/Cengage Learning

4. Drill down to the user account under **System Tools**, **Local Users and Groups**, and **Users**. Right-click the user and select **Properties** from the shortcut menu. The user Properties box opens. Click the **Member Of** tab.

5. Click **Add**. In the Select Groups box (the right side of Figure 17-51), type **TelnetClients** in the objects area (be sure to type it exactly as shown). Click **OK**. In the user Properties box, click **Apply** and click **OK** to close the box. Close the **Computer Management** console.

6. The next step is to start the Telnet server: To open the Services console, type **Services.msc** in the Vista Start Search box or XP Run box and press **Enter**. For Vista, respond to the UAC box. Scroll down to the Telnet service. Right-click it and select **Properties** from the shortcut menu. In the properties box, change the Startup type of Telnet to **Manual**. Click **Apply**. Click **Start** to start the Telnet service. Close the Telnet Properties box and the Services console.

7. To find out the IP address of this computer, open a command prompt window and enter the command **ipconfig /all**. Look for the IP address in the output, as shown in Figure 17-47 earlier in the chapter. In our example, the IP address is 109.168.1.104.

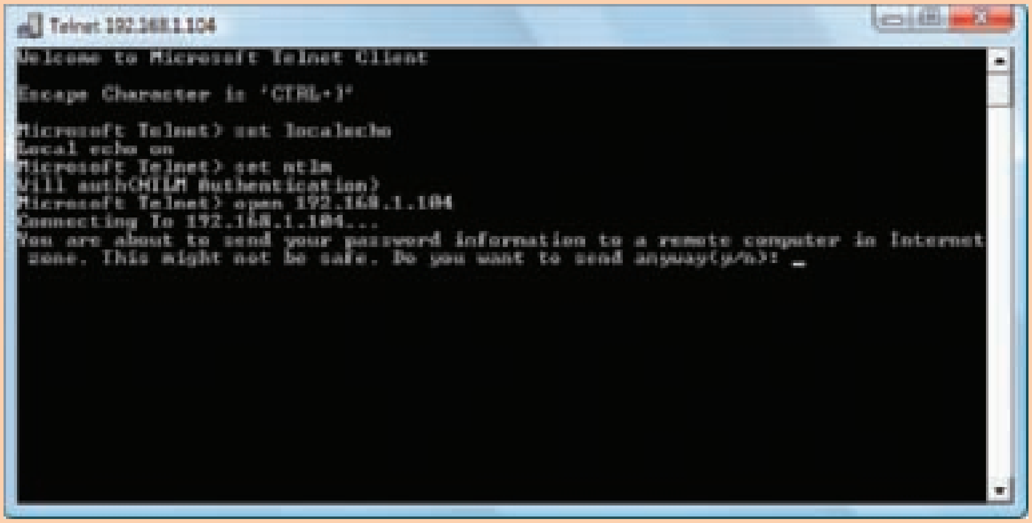
On the second or local computer, do the following to "telnet in" to the remote computer:

1. Log onto Windows with a user account and password that is the same as that on the remote computer.

2. Recall that Vista does not automatically install Telnet. For Vista, open **Control Panel** and turn on the **Telnet Client** application, following the steps given earlier (refer back to Figure 17-50).

A+
220-701
4.1
3.2

3. You are now ready to open the Telnet client application. In the Vista Start Search box or the XP Run box, enter **Telnet** and press **Enter**. The Telnet command prompt window opens (see Figure 17-52). To see the results of commands executed by the remote computer, enter the command **set localecho** and press **Enter**.



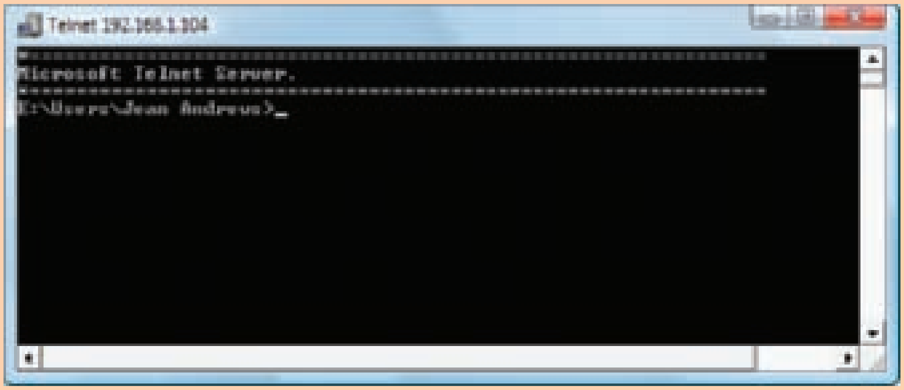
```
Welcome to Microsoft Telnet Client

Escape Character is 'CTRL+]'

Microsoft Telnet> set localecho
Local echo on
Microsoft Telnet> set ntlm
Will auth(NTLM Authentication)
Microsoft Telnet> open 192.168.1.104
Connecting To 192.168.1.104...
You are about to send your password information to a remote computer in Internet
 zone. This might not be safe. Do you want to send anyway(y/n)): _
```

Figure 17-52 Telnet command prompt window
Courtesy: Course Technology/Cengage Learning

4. To use the NTLM authentication protocol for user accounts and passwords, enter the command **set ntlm** and press **Enter**.

5. To open the connection to the remote computer, enter the command **open 192.168.1.104**, substituting the IP address of your Telnet server in the command line. Press **Enter** after the command. You should now see the message that appears near the bottom of Figure 17-52.

6. Enter **y** to complete the connection. The window changes from the Telnet command mode to the remote computer session mode (see Figure 17-53). The prompt in this window is that provided by the remote computer. Commands you enter in this window are Windows commands (not Telnet commands) that are executed by the remote computer. At this point, you would enter whatever Windows commands you needed to do your work on the remote computer.



```
*===============================================================================
Microsoft Telnet Server.
*===============================================================================
C:\Users\Jean Andrews>_
```

Figure 17-53 Telnet window in session mode with the remote computer
Courtesy: Course Technology/Cengage Learning

A+
220-701
4.1
3.2

Because localecho is on, each letter you enter appears twice in the command line, and you will be able to see the results of the command as displayed by the remote computer. To see how a command works in this window, enter the **dir** command and press **Enter**.

7. To return to the Telnet command mode window, enter **Ctrl+]**. To switch from the Telnet window to the session mode window, press **Enter**. Press **Ctrl+]** to return one more time to the Telnet command mode window.
8. Enter **close** and press **Enter** to close the connection. Enter **quit** and press **Enter** to close the Telnet window.

Notes You can use the computer name rather than the IP address to connect to a remote computer. If the computer name is not recognized, add it to the bottom of the C:\Windows\System32\drivers\etc\hosts file on the local computer. For example, if the computer name of the remote computer is FileServer, add this line to the bottom of the file: 192.168.1.104 FileServer. To edit the hosts file, first remove the read-only attribute from the \etc folder.

If you plan to use this same computer name to initiate Telnet sessions in the future, the Telnet server needs to use static IP addressing. This way, the Hosts file will always be accurate.

The major disadvantage of using Telnet to connect to a remote computer is the lack of security. The Telnet protocol does not encrypt transmitted data, which can therefore be read by others on the network. A better protocol to use is Secure Shell (SSH). The protocol is supported by Windows, but Windows does not provide SSH applications. Therefore, you must use third-party SSH applications such as SecureCRT by Van Dyke (*www.vandyke.com*). Two versions of SSH exist; be sure to select an application that uses SSH Version 2 to get the best security.

A+
220-701
4.1

VIRTUAL PRIVATE NETWORKS

Many people travel on their jobs or work from home, and the need is constantly growing for people to access private corporate data from somewhere on the Internet. Also growing are the dangers of private data being exposed in this way. The solution for securing private data traveling over a public network is a **virtual private network (VPN)**. A VPN works by using encrypted data packets between a private network and a computer somewhere on the Internet, as shown in Figure 17-54. The VPN is managed by client/server software such as Citrix Access Gateway by Citrix Systems (*www.citrix.com*).

With a VPN, security is attained using both of these methods:

- User accounts and passwords are required for connection to the corporate network. When the remote user sends this information to the authentication server, the data is encrypted. The encryption protocols supported by Windows for the user account and password data are EAP (Extensible Authentication Protocol), SPAP (Shiva Password Authentication Protocol), CHAP (Challenge Handshake Authentication Protocol), and MS-CHAP (Microsoft CHAP).
- After the user is authenticated, a tunnel is created so that all data sent between the user and the company is strongly encrypted. One of these four tunneling protocols is used: Point-to-Point Tunneling Protocol (PPTP), Layer Two Tunneling Protocol

A+
220-701
4.1

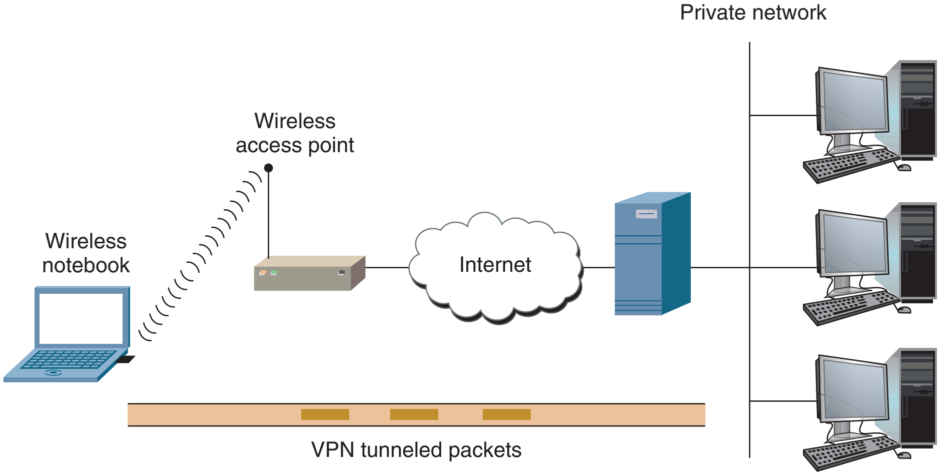


Figure 17-54 With a VPN, tunneling is used to send encrypted data over wired and wireless networks and the Internet
Courtesy: Course Technology/Cengage Learning

(L2TP), SSL (Secure Sockets Layer), or IPsec (IP security). Of the four, PPTP is the weakest protocol. The strongest protocol is a combination of L2TP and IPSec, which is called L2TP over IPSec. The two most popular protocols are SSL and IPsec.

When you first configure a computer to connect to a corporate network by way of the Internet, follow links on the corporate Web site to download the VPN client software. Then install the software on the computer and configure it to use the VPN. The user authorized to use the VPN will need to enter the user account and password authorized on the VPN to test the connection and make sure he or she can access resources on the corporate network. The resources the user can access depend on the permissions assigned the account.

Now that you know about networking hardware and the operating system methods and protocols used on a network, let's turn our attention to how to connect a computer to a network.

HOW TO CONNECT A COMPUTER TO A NETWORK

A+
220-701
4.1
1.10
3.2

Connecting a computer to a network is quick and easy in most situations. In this part of the chapter, you'll learn to connect a computer to a network using both wired and wireless connections. Then we'll look at what can go wrong and how to fix problems when the connection doesn't work.

CONNECT TO A NETWORK USING AN ETHERNET CONNECTION

To connect a computer to a network using a wired connection, follow these steps:

1. If the network adapter is not yet installed, install it now following the steps given in Chapter 9 to install an expansion card. These steps include physically installing the card, installing drivers, and using Device Manager to verify that Windows recognizes the adapter without errors.
2. Connect a network cable to the Ethernet RJ-45 port and to the network wall jack or directly to a switch or router. (Connecting a PC directly to a switch or router might require a crossover cable.) Indicator lights near the network port should light up to

A+
220-701
4.1
1.10
3.2

indicate connectivity and activity. If you connected the cable directly to a switch or router, verify the light at that port is also lit.

3. By default, Windows assumes dynamic IP addressing and automatically configures the network connection. To find out if the connection is working, click **Start, Network** to open the Network window (see Figure 17-55). For Windows XP, click **Start, My Network Places** to open the My Network Places window. You should see icons that represent other computers on the network. Double-click a computer and drill down to shared folders and files to verify you can access these resources.

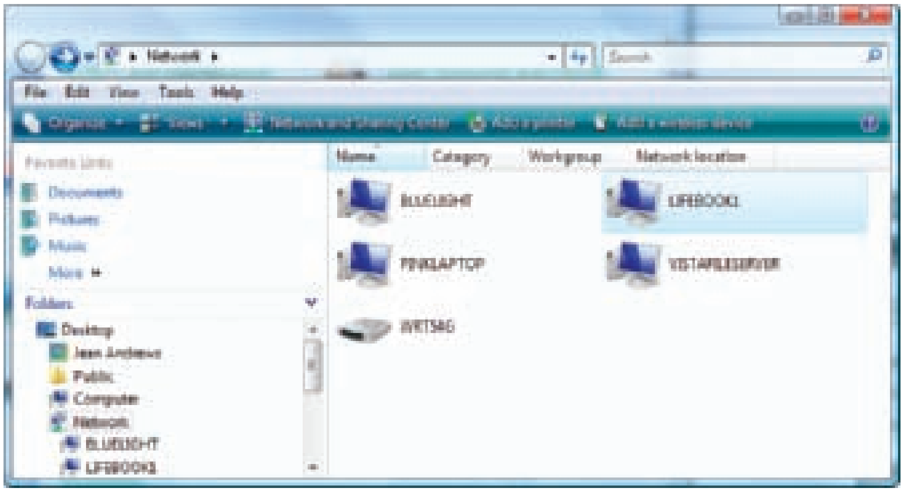


Figure 17-55 The Vista Network window shows resources on the network
Courtesy: Course Technology/Cengage Learning

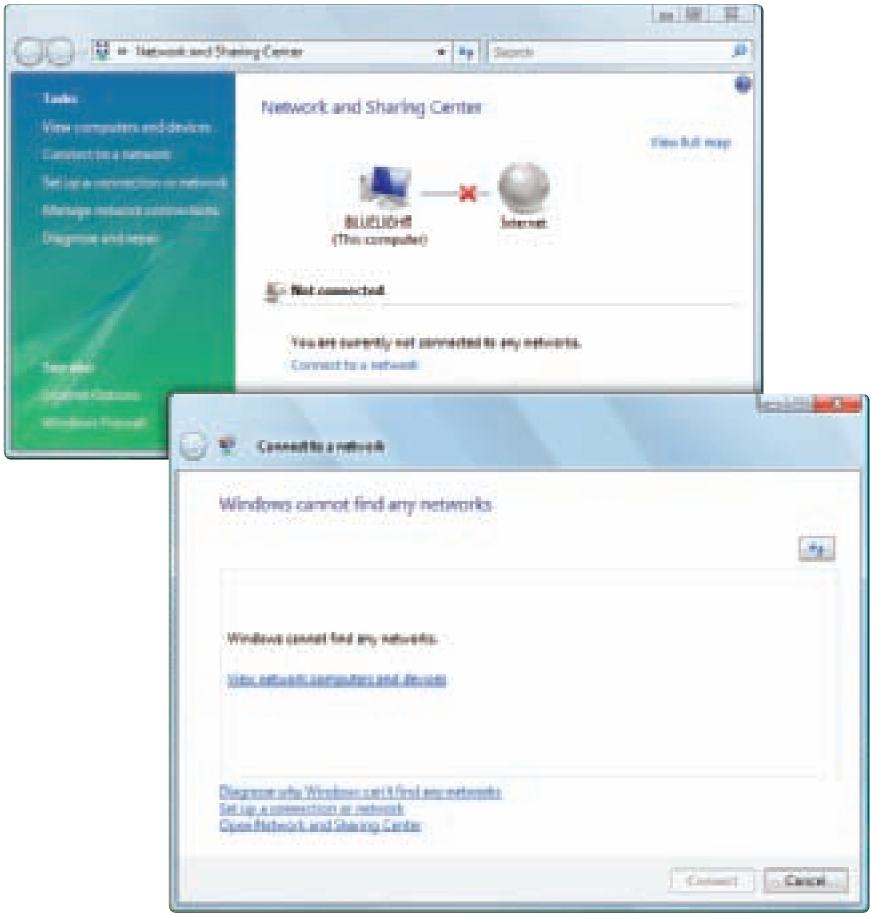
4. To verify you have Internet connectivity, open Internet Explorer and browse to a few Web sites.

If the connection does not work, it's time to verify that network settings are configured correctly. Follow these steps using Windows Vista:

1. Verify that Device Manager recognizes the network adapter without errors. If you find an error, try updating the network adapter drivers. If that doesn't work, then try uninstalling and reinstalling the drivers. Make sure Device Manager recognizes the network adapter without errors before you move on to the next step.
2. If Network is not listed in the Start menu, open **Control Panel**. Click **Network and Internet** and then click **Network and Sharing Center**. In the Network and Sharing Center window (see the top part of Figure 17-56), click **Connect to a network**.
3. When Vista recognizes available networks, they are listed in the Connect to a network box shown in the lower part of Figure 17-56. If none are shown, click **Diagnose why Windows can't find any networks**. Then follow the recommendations that appear.

For Windows XP, to connect to a network or repair a connection, click **Start**, right-click **My Network Places**, and select **Properties** from the shortcut menu. The **Network Connections** window opens. Right-click the **Local Area Connection** icon, and then select **Repair** from the shortcut menu. See Figure 17-57. To connect to a network, in the Network Connections window, click **Create a new connection**.

A+
220-701
4.1
1.10
3.2


Network and Sharing Center
Search
Tasks
View computers and devices
Connect to a network
Set up a connection or network
Manage network connections
Diagnose and repair
See also
Internet Options
Windows Firewall
Network and Sharing Center
View full map
BLUELIGHT
(This computer)
Internet
Not connected
Connect to a network
Connect to a network
Windows cannot find any networks
View network computers and devices
Diagnose why Windows can't find any networks
Set up a connection or network
Open Network and Sharing Center
Connect
Cancel

You are currently not connected to any networks.

Windows cannot find any networks.

Figure 17-56 Vista Network and Sharing Center manages network connections
Courtesy: Course Technology/Cengage Learning

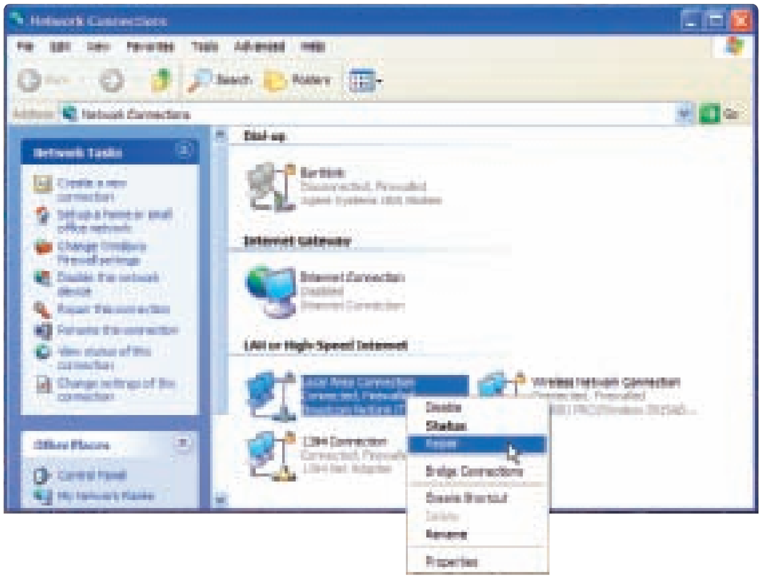


Figure 17-57 Windows XP Network Connections window
Courtesy: Course Technology/Cengage Learning

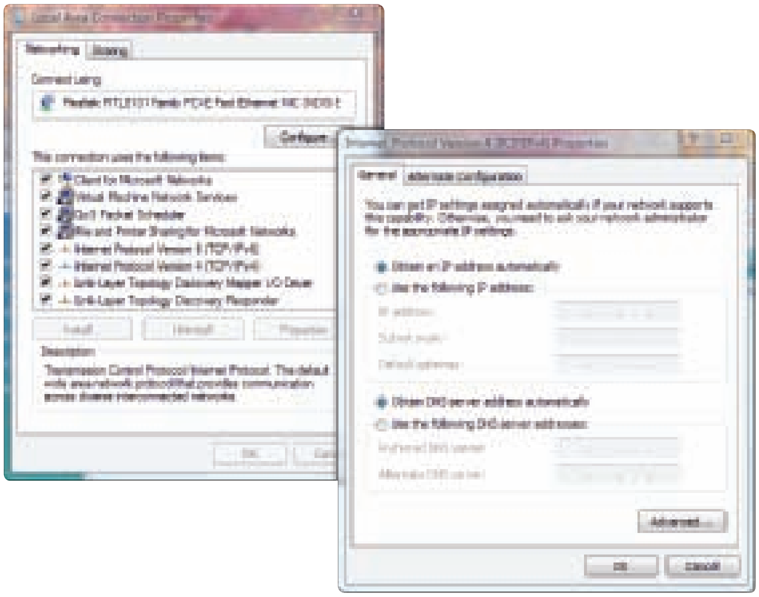
A+
220-701
4.1
1.10
3.2

Most networks use DHCP servers and dynamic IP addressing. If your network uses static IP addressing, you will need to know this information:

- The IP address for this computer.
- The subnet mask. A **subnet mask** is a group of four dotted decimal numbers such as 255.255.0.0 that tells TCP/IP if a computer's IP address is on the same or a different network.
- The default gateway. A **gateway** is a computer or other device, such as a router, that allows a computer on one network to communicate with a computer on another network. A **default gateway** is the gateway a computer uses to access another network if it does not have a better option.
- The IP addresses of one or more DNS servers that the network uses.

Follow these steps to verify and change TCP/IP settings:

1. Click **Start**, right-click **Network**, and select **Properties** from the shortcut menu. The Network and Sharing Center opens. In the left pane, click **Manage network connections**. In the Network Connections window, right-click **Local Area Connection** and select **Properties** from the shortcut menu. Respond to the UAC box. The properties box appears (see the left side of Figure 17-58).



☑ Client for Microsoft Networks
☑ Virtual Machine Network Services
☑ QoS Packet Scheduler
☑ File and Printer Sharing for Microsoft Networks
☑ Internet Protocol Version 6 (TCP/IPv6)
☑ Internet Protocol Version 4 (TCP/IPv4)
☑ Link-Layer Topology Discovery Mapper I/O Driver
☑ Link-Layer Topology Discovery Responder

Transmission Control Protocol/Internet Protocol. The default wide area network protocol that provides communication across diverse interconnected networks.

You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.

● Obtain an IP address automatically
○ Use the following IP address:

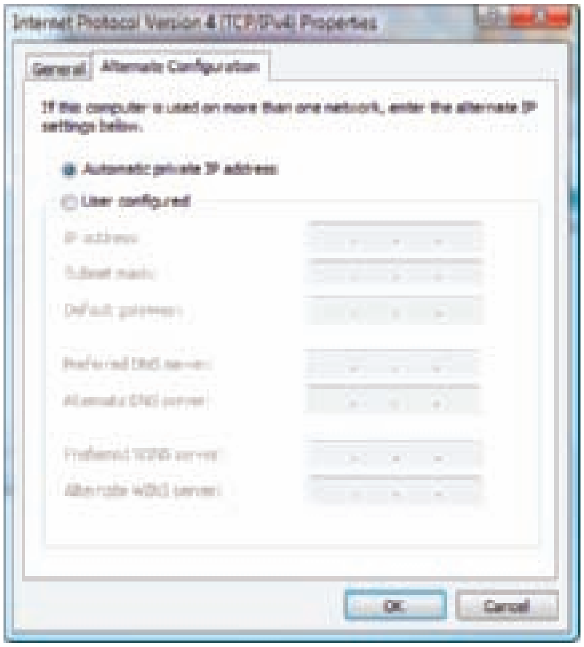
● Obtain DNS server address automatically
○ Use the following DNS server addresses:

Figure 17-58 Verify and change TCP/IP settings
Courtesy: Course Technology/Cengage Learning

2. Select **Internet Protocol Version 4** (**TCP/IPv4**) and click **Properties**. The properties box on the right side of Figure 17-58 appears. Settings are correct for dynamic IP addressing.
3. To change the settings to static IP addressing, select **Use the following IP address**. Then enter the IP address, subnet mask, and default gateway.
4. If you have been given the IP addresses of DNS servers, check **Use the following DNS server addresses** and enter up to two IP addresses. If you have other DNS IP addresses, click **Advanced** and enter them on the **DNS** tab of the Advanced TCP/IP Settings box.

A+
220-701
4.1
1.10
3.2

5. By the way, if the computer you are using is a laptop that moves from one network to another, you can click the **Alternate Configuration** tab and configure static IP address settings for a second network (see Figure 17-59). One way to use this configuration is to configure the General tab to use dynamic IP addressing and configure the Alternate Configuration tab to use static IP addressing. Using this method, the computer will first try to use dynamic IP addressing. If that is not available on the network, it then applies the static IP address settings. If static IP address settings are not available on this tab, the computer uses an automatic private IP address (APIPA).



If this computer is used on more than one network, enter the alternate IP settings below.

● Automatic private IP address
○ User configured

IP address: . . .
Subnet mask: . . .
Default gateway: . . .
Preferred DNS server: . . .
Alternate DNS server: . . .
Preferred WINS server: . . .
Alternate WINS server: . . .

Figure 17-59 Alternate configuration that applies if the first TCP/IP settings do not work
Courtesy: Course Technology/Cengage Learning

A+ Exam Tip The A+ 220-701 Essentials exam expects you to know the basics of configuring static and dynamic IP addressing and DNS server IP addresses.

To verify and change the TCP/IP setting for Windows XP, click **Start**, right-click **My Network Places**, and select **Properties** from the shortcut menu. The **Network Connections** window opens. Right-click the **Local Area Connection** icon, and then select **Properties** from the shortcut menu. Refer back to Figure 17-57. The properties box opens. Select **Internet Protocol** (**TCP/IP**) and click **Properties**. Configure the TCP/IP properties the same as with Windows Vista.

Video
Setting up a Network with Hub and Patch Cables

A+
220-701
1.10
3.2

CONNECT TO A NETWORK USING A WIRELESS CONNECTION

Wireless networks are either public, unsecured hotspots or private, secured hotspots. In this part of the chapter, you learn how to connect to each.

A+
220-701
1.10
3.2

HOW TO CONNECT TO A PUBLIC WIRELESS HOTSPOT

When using a public wireless hotspot, know that whatever you send over the network might be read by others. Also, unless you protect your computer by using strong firewall settings, your computer might get hacked. Here are the steps to connect to a public hotspot for a laptop using Windows Vista and how to protect your computer on that network:

1. Install the wireless adapter. For external adapters such as the one shown in Figure 17-60, be sure to follow the manufacturer's instructions for the installation. Most likely you'll be asked to first install the software before installing the device. During the installation process, you will be given the opportunity to use the manufacturer's configuration utility to manage the wireless adapter or to use Windows to do the job. For best results, use the utility provided by the manufacturer. In the following steps, we're using the Windows utility.

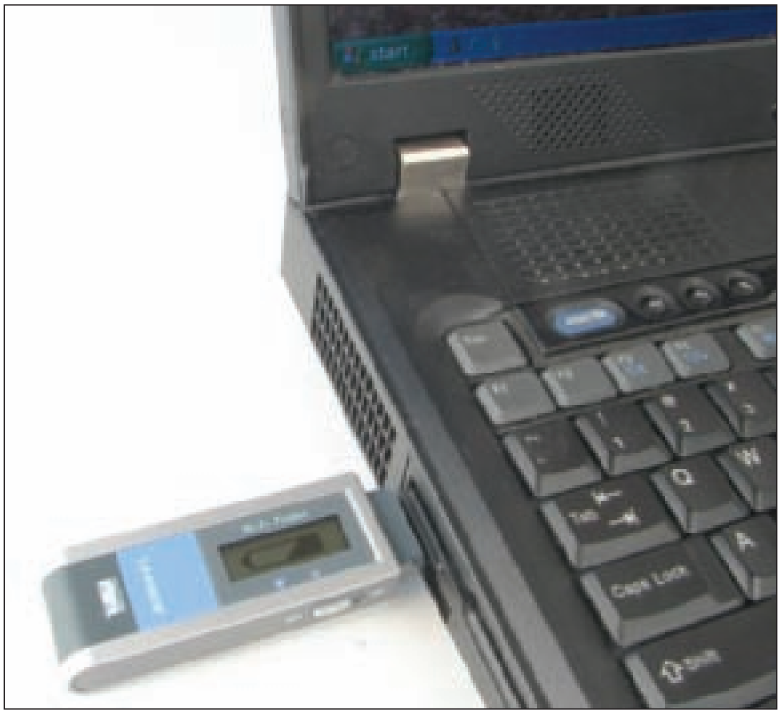


Figure 17-60 Plug the wireless USB adapter into the USB port
Courtesy: Course Technology/Cengage Learning

2. For embedded wireless, turn on your wireless device. For some laptops, that's done by a switch on the keyboard (see Figure 17-61) or on the side of the laptop. The wireless antenna is usually in the lid of a notebook and gives best performance when the lid is fully raised. For a desktop computer, make sure the antenna is in an upright position (see Figure 17-62).
3. Using your mouse, hover over or double-click the network icon in your notification area. Vista reports that wireless networks are available (see Figure 17-63).
4. Click **Connect to a network**. A list of available networks appears (see Figure 17-64).
5. If you select an unsecured network, Vista warns you about sending information over it. Click **Connect Anyway**.

A+
220-701
1.10
3.2

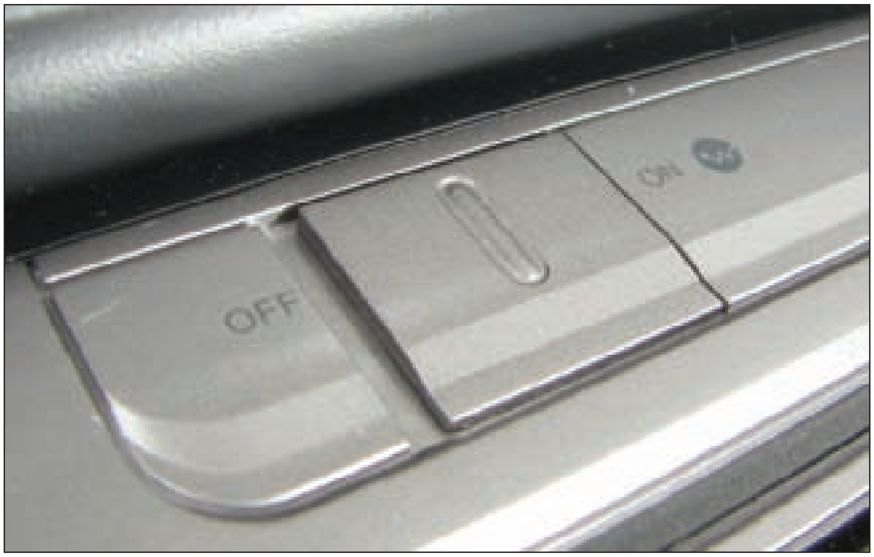


Figure 17-61 Turn on the wireless switch on your laptop
Courtesy: Course Technology/Cengage Learning

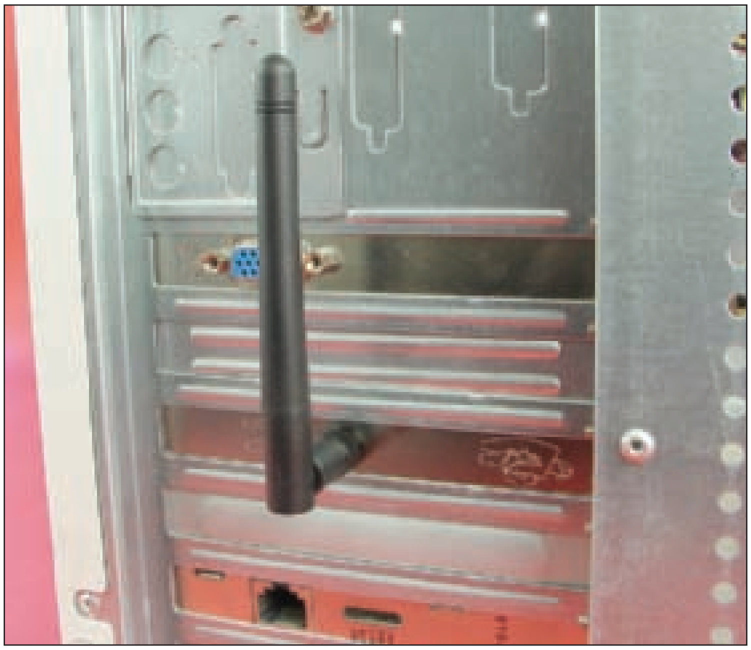
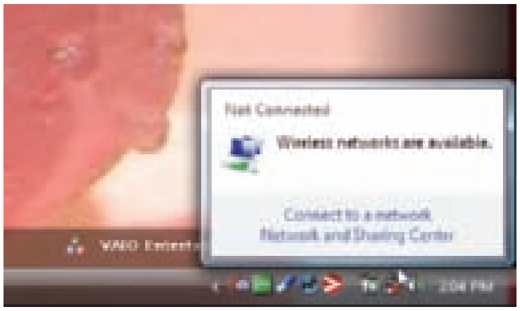


Figure 17-62 Raise the antenna on a NIC to an upright position
Courtesy: Course Technology/Cengage Learning



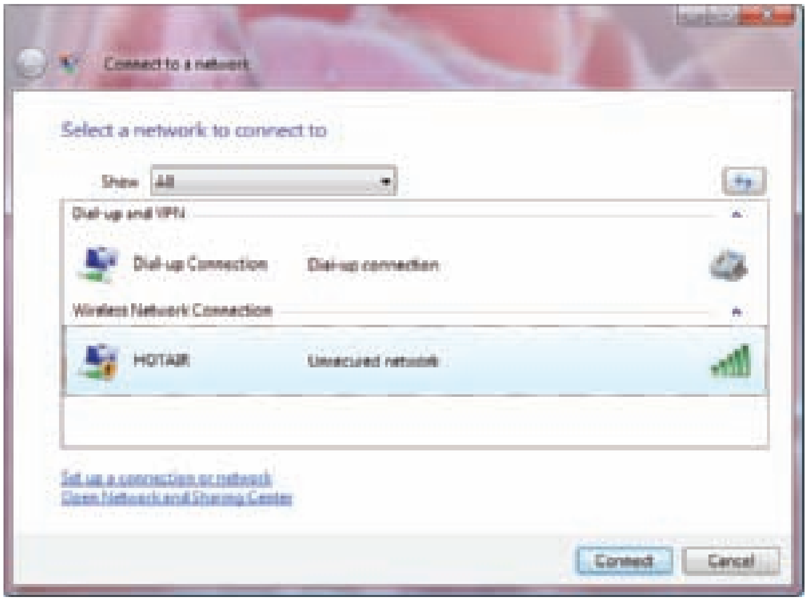
Not Connected

Wireless networks are available.

Connect to a network
Network and Sharing Center

Figure 17-63 Windows reports that wireless networks are available
Courtesy: Course Technology/Cengage Learning

A+
220-701
1.10
3.2


Connect to a network

Select a network to connect to

Show: All

Dial-up and VPN

Dial-up Connection Dial-up connection

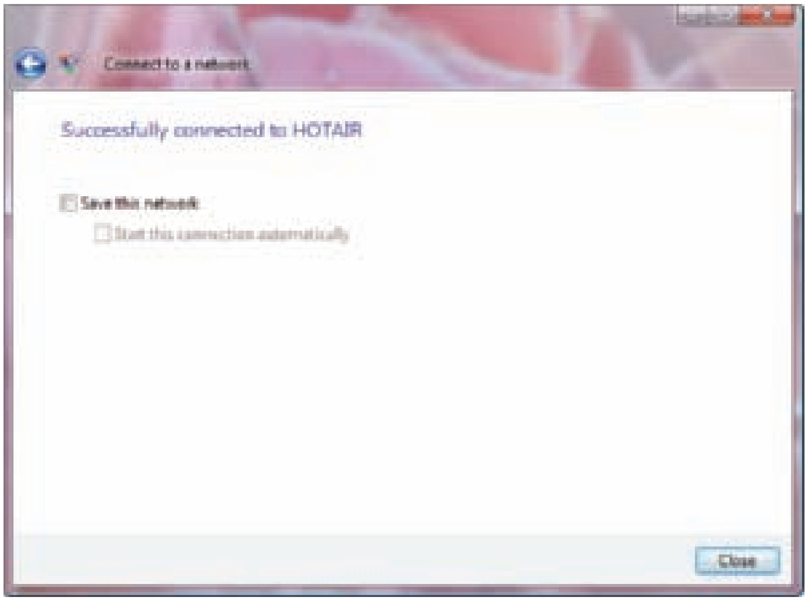
Wireless Network Connection

HOTAIR Unsecured network

Set up a connection or network
Open Network and Sharing Center
Connect
Cancel

Figure 17-64 Select a wireless network
Courtesy: Course Technology/Cengage Learning

6. Vista reports the connection is made using the window in Figure 17-65. If you are comfortable with Vista automatically connecting to this network in the future, check **Save this network**. Close the window. If you hover your mouse pointer over the network icon in the notification area or double-click it, you can see the network to which you are connected (see Figure 17-66).


Connect to a network

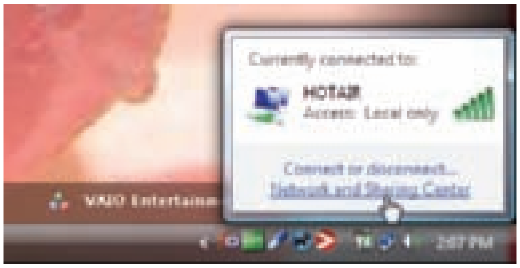
Successfully connected to HOTAIR

□ Save this network

□ Start this connection automatically

Figure 17-65 Decide if you want to save this network connection
Courtesy: Course Technology/Cengage Learning

A+
220-701
1.10
3.2

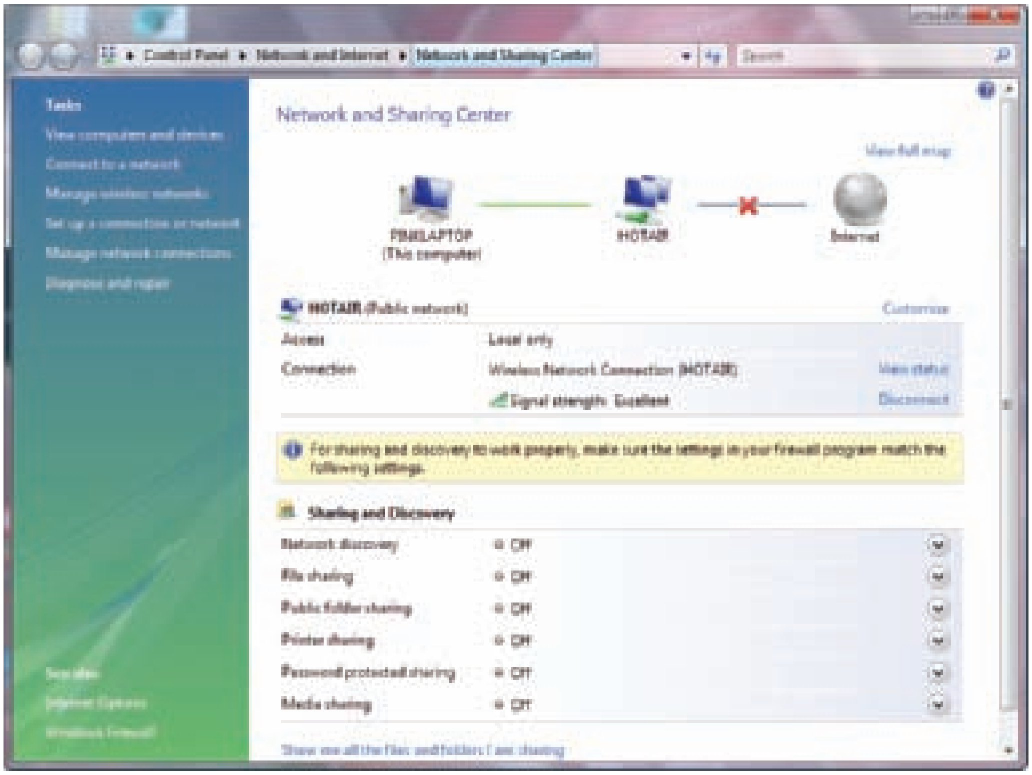


Currently connected to:

HOTAIR
Access: Local only

Figure 17-66 Find out to which network you are connected
Courtesy: Course Technology/Cengage Learning

7. To verify firewall settings and check for errors, open the Network and Sharing Center window (see Figure 17-67). Verify that Vista has configured the network as a public network and that Sharing and Discovery settings are all turned off. If Vista reports it has configured the network as a Private network, click **Customize** and change the setting to Public. In the figure, you can see there is a problem with the Internet connection from the HOTAIR network to the Internet.



Network and Sharing Center

HOTAIR (Public network)

Access	Local only
Connection	Wireless Network Connection (HOTAIR)
	Signal strength: Excellent

For sharing and discovery to work properly, make sure the settings in your firewall program match the following settings.

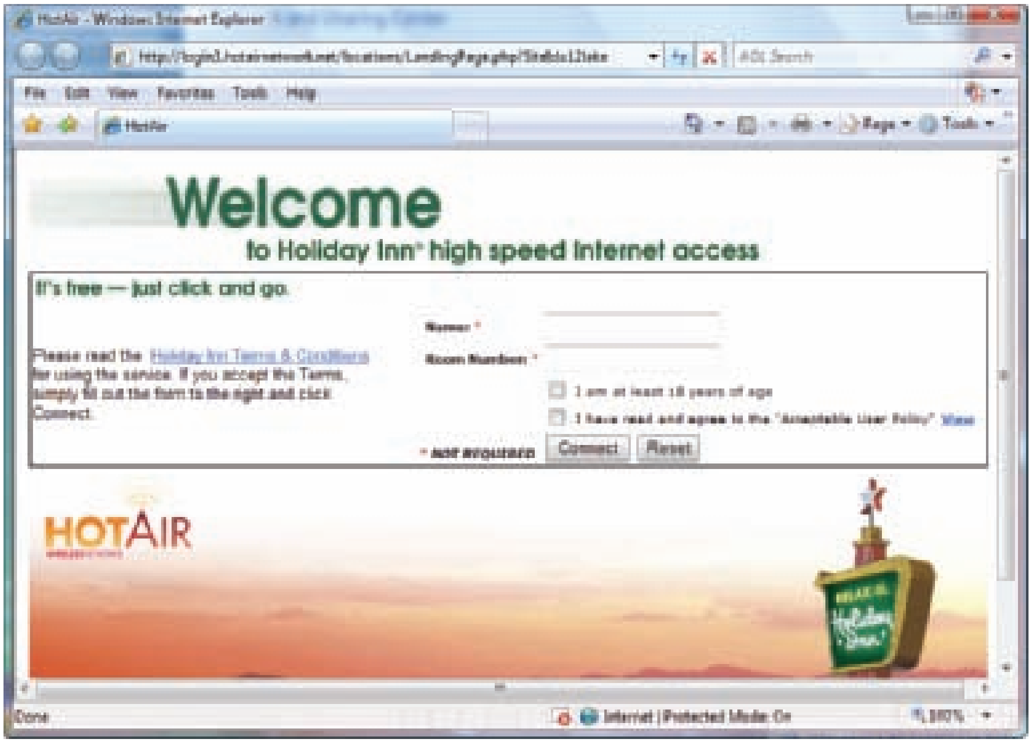
Sharing and Discovery

Network discovery	● Off
File sharing	● Off
Public folder sharing	● Off
Printer sharing	● Off
Password protected sharing	● Off
Media sharing	● Off

Figure 17-67 Verify that your connection is secure
Courtesy: Course Technology/Cengage Learning

8. Open your browser to test the connection. For some hotspots, a home page appears and you must enter a code or agree to the terms of use (see Figure 17-68).

A+
220-701
1.10
3.2


HotAir - Windows Internet Explorer
File Edit View Favorites Tools Help
HotAir
Page
Tools
HOTAIR
Done
Internet | Protected Mode: On
100%

Welcome
to Holiday Inn® high speed Internet access

It's free — just click and go.

Please read the Holiday Inn Terms & Conditions for using the service. If you accept the Terms, simply fill out the form to the right and click Connect.

Name: *

Room Number: *

□ I am at least 18 years of age

□ I have read and agree to the "Acceptable User Policy" View

* field required

Figure 17-68 This hotspot requires you agree to the terms of use
Courtesy: Course Technology/Cengage Learning

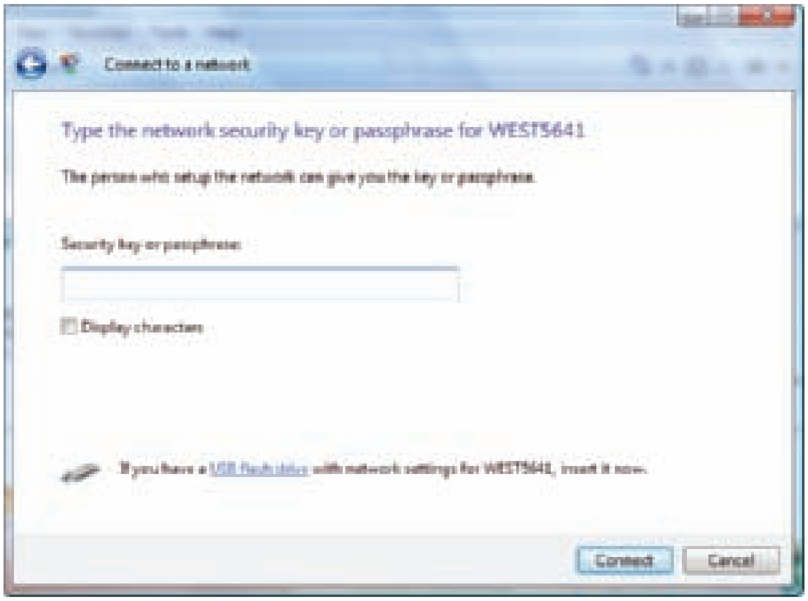
When selecting a public hotspot, watch out for rogue hotspots trying to trick you into using them. For example, suppose you sit down at a coffee shop with your laptop to surf the Web. When you try to connect to the free hotspot provided by the coffee shop, you see two unsecured hotspots available. One is named JoesCoffeeShop and the other is named FreeInternet. Most likely the first one is provided by the coffee shop and is the one to choose. However, if you're not sure, ask an employee. The danger in connecting to unknown hotspots is that malware and hackers might be waiting for unsecured computers to connect.

CONNECT TO A PRIVATE WIRELESS NETWORK

When connecting to a private and secured wireless access point, you must provide the information that proves you have the right to use the network. If the network is protected with an encryption key, when you first attempt to connect, a screen similar to that in Figure 17-69 appears so that you can enter the key. If the access point is not broadcasting its SSID, the name of the wireless network will appear as "Unnamed Network." When you select this network, you are given the opportunity to enter the name of the network. If you don't enter the name correctly, you will not be able to connect. It is also possible that a private and secured wireless access point has been configured for MAC address filtering in order to control which wireless adapters can use the access point. Check with the network administrator to determine if this is the case; if necessary, give the administrator the adapter's MAC address to be entered into a table of acceptable MAC addresses.

To know the MAC address of your wireless adapter, for an external adapter, you can look on the back of the adapter itself (see Figure 17-70) or in the adapter documentation. Also, if the adapter is installed on your computer, you can open a command prompt window and enter the command **ipconfig/all**, which displays your TCP/IP configuration for all network connections. The MAC address is called the Physical Address in the display (see Figure 17-71).

A+
220-701
1.10
3.2



Type the network security key or passphrase for WEST5641

The person who setup the network can give you the key or passphrase.

Security key or passphrase:

☐ Display characters

If you have a USB flash drive with network settings for WEST5641, insert it now.

Figure 17-69 To use a secured wireless network, you must know the encryption key
Courtesy: Course Technology/Cengage Learning

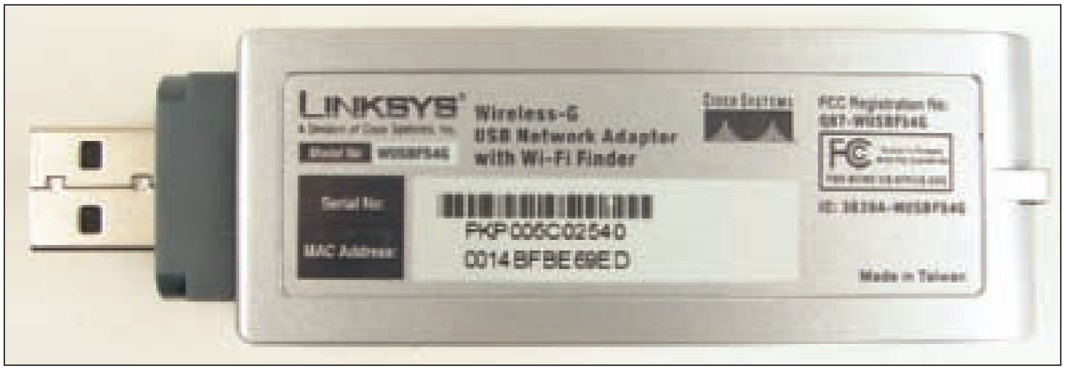
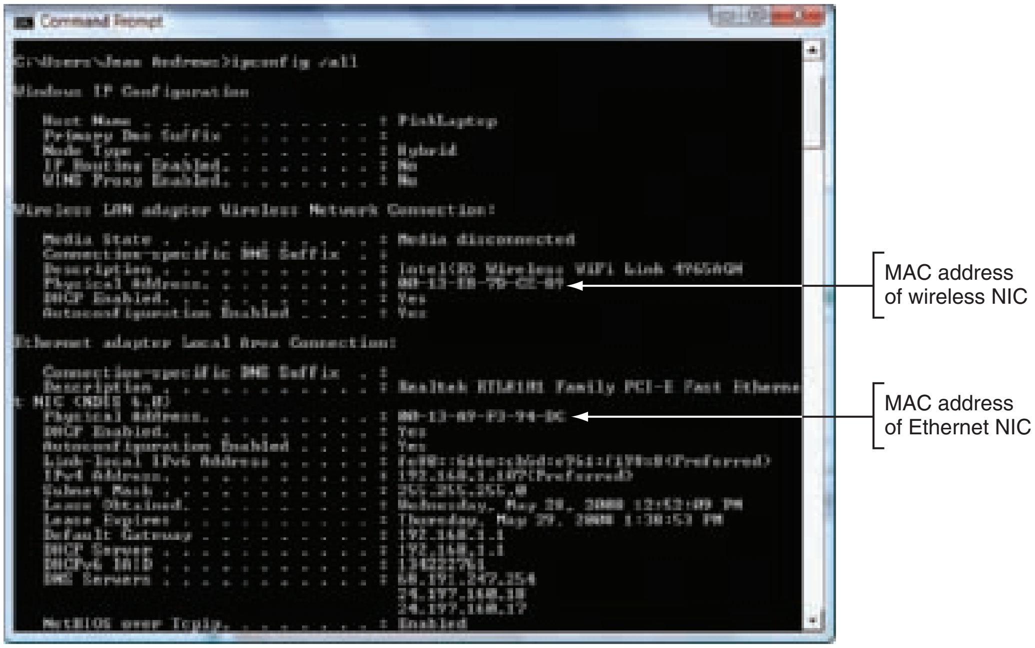


Figure 17-70 The MAC address is printed on the back of this USB wireless adapter
Courtesy: Course Technology/Cengage Learning



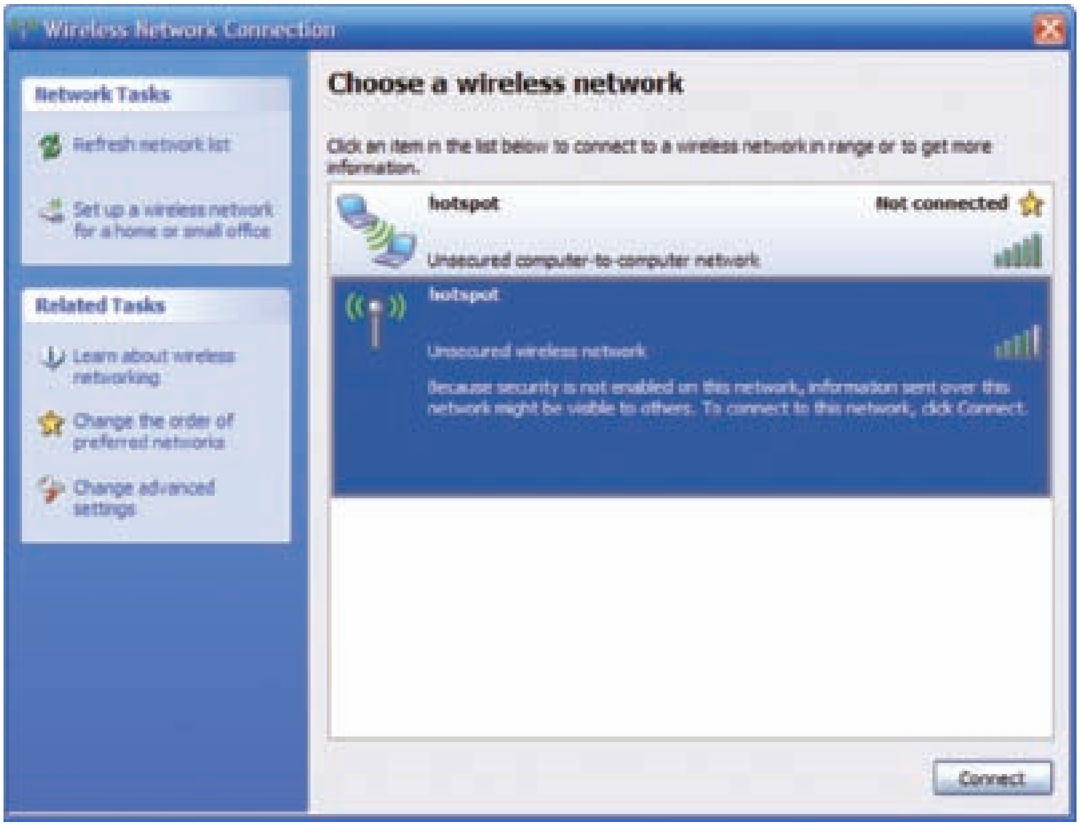
```
C:\Users\Jean Andrews>ipconfig /all

Windows IP Configuration

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

Wireless LAN adapter Wireless Network Connection:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :
   Description . . . . . . . . . . . : Intel(R) Wireless WiFi Link 4965AGN
   Physical Address. . . . . . . . . : 00-13-E8-79-CE-89
   DHCP Enabled. . . . . . . . . . . : Yes
   Autoconfiguration Enabled . . . . : Yes

Ethernet adapter Local Area Connection:

   Connection-specific DNS Suffix  . :
   Description . . . . . . . . . . . : Realtek RTL8101 Family PCI-E Fast Etherne
t NIC (NDIS 6.0)
   Physical Address. . . . . . . . . : 00-13-A9-F3-94-DC
   DHCP Enabled. . . . . . . . . . . : Yes
   Autoconfiguration Enabled . . . . : Yes
   Link-local IPv6 Address . . . . . : fe80::646e:cb6d:e761:f198%8(Preferred)
   IPv4 Address. . . . . . . . . . . : 192.168.1.107(Preferred)
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Lease Obtained. . . . . . . . . . : Wednesday, May 28, 2008 12:52:09 PM
   Lease Expires . . . . . . . . . . : Thursday, May 29, 2008 1:38:53 PM
   Default Gateway . . . . . . . . . : 192.168.1.1
   DHCP Server . . . . . . . . . . . : 192.168.1.1
   DHCPv6 IAID . . . . . . . . . . . : 134222761
   DNS Servers . . . . . . . . . . . : 68.191.247.254
                                       24.197.160.18
                                       24.197.160.17
   NetBIOS over Tcpip. . . . . . . . : Enabled
```

Figure 17-71 Use the ipconfig /all command to display TCP/IP configuration data
Courtesy: Course Technology/Cengage Learning

A+
220-701
1.10
3.2

Here are the steps to connect to a public or private hot spot when using Windows XP:

1. Right-click **My Network Places** and select **Properties**. The Network Connections window opens. Right-click the **Wireless Network Connection** icon and select **View Available Wireless Networks** from the shortcut menu. The Wireless Network Connection window opens (see Figure 17-72). Select an unsecured network from those listed and click **Connect**.


Wireless Network Connection
Network Tasks
Refresh network list
Set up a wireless network for a home or small office
Related Tasks
Learn about wireless networking
Change the order of preferred networks
Change advanced settings
Connect

Choose a wireless network

Click an item in the list below to connect to a wireless network in range or to get more information.

hotspot — Not connected
Unsecured computer-to-computer network

hotspot
Unsecured wireless network
Because security is not enabled on this network, information sent over this network might be visible to others. To connect to this network, click Connect.

Figure 17-72 Available wireless hot spots
Courtesy: Course Technology/Cengage Learning

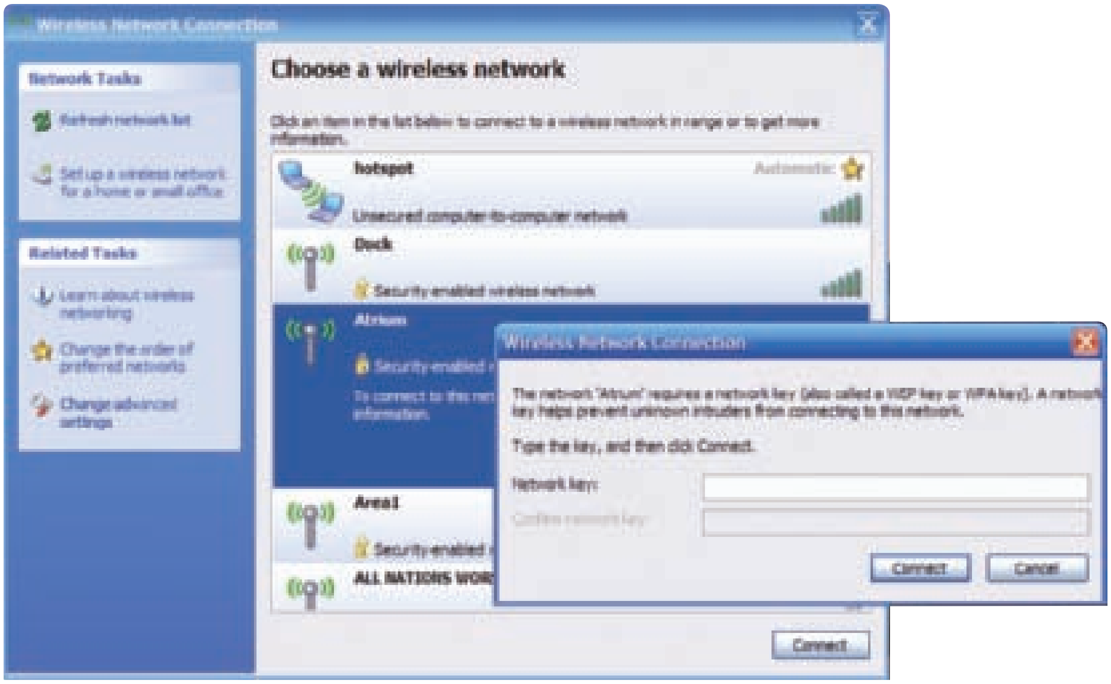
2. When you select a secured network from the list, you must enter the key in a dialog box, as shown in Figure 17-73.

If you're having a problem making the connection and you know the SSID of the hot spot, you can enter the SSID. Click **Change advanced settings** in the Network Connections window. The Wireless Network Connection Properties dialog box opens. Click the **Wireless Networks** tab (see Figure 17-74). Click **Add**.

The Wireless network properties window opens (see Figure 17-75). Enter the SSID of the network and make sure that Network Authentication is set to **Open** and Data encryption is set to **Disabled**. Click **OK**. When a dialog box opens to warn you of the dangers of disabling encryption, click **Continue Anyway**. Click **OK** to close the Wireless Network Connection Properties dialog box. Try again to connect to the hot spot.

Video
Installing a Wireless NIC

A+
220-701
1.10
3.2


Wireless Network Connection
Network Tasks
Refresh network list
Set up a wireless network for a home or small office
Related Tasks
Learn about wireless networking
Change the order of preferred networks
Change advanced settings
Automatic
Connect
Wireless Network Connection
Network key:
Confirm network key:
Connect
Cancel
Connect

Choose a wireless network

Click an item in the list below to connect to a wireless network in range or to get more information.

hotspot
Unsecured computer-to-computer network

Dock
Security-enabled wireless network

Atrium
Security-enabled
To connect to this net
information.

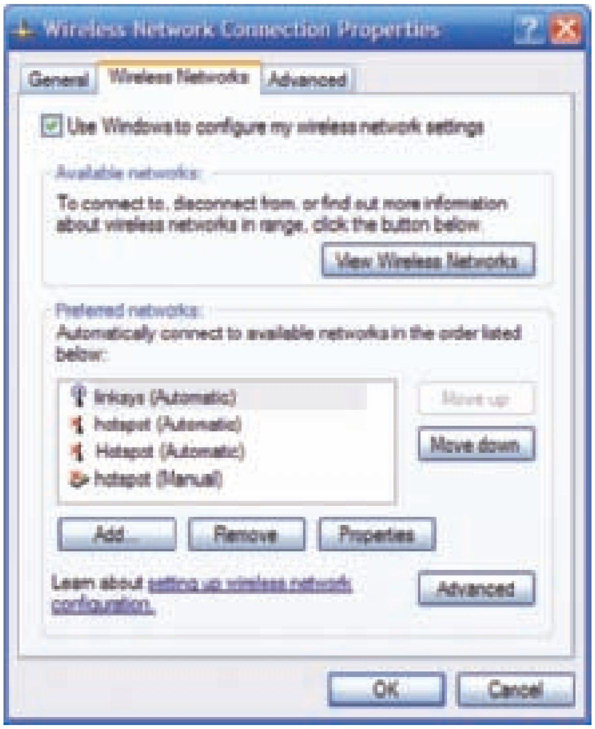
Area1
Security-enabled

ALL NATIONS WOR

The network 'Atrium' requires a network key (also called a WEP key or WPA key). A network key helps prevent unknown intruders from connecting to this network.

Type the key, and then click Connect.

Figure 17-73 To use a secured wireless network, you must know the encryption key
Courtesy: Course Technology/Cengage Learning



☑ Use Windows to configure my wireless network settings

To connect to, disconnect from, or find out more information about wireless networks in range, click the button below.

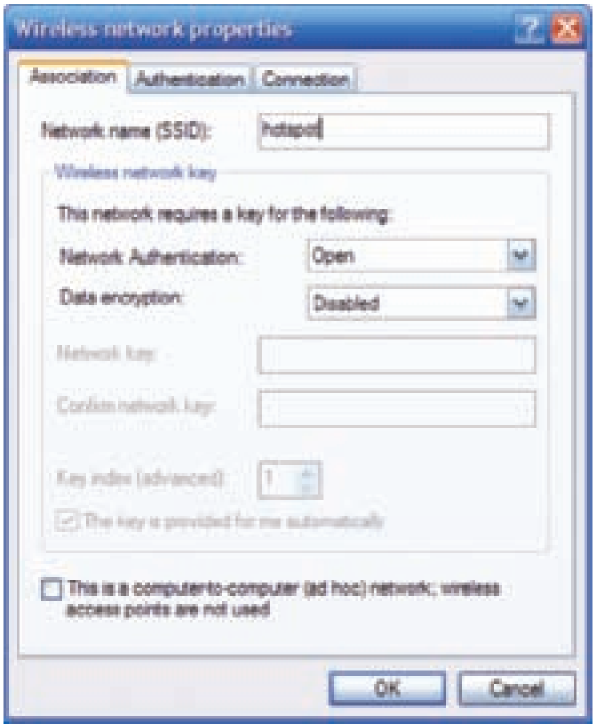
Automatically connect to available networks in the order listed below:

linksys (Automatic)
hotspot (Automatic)
Hotspot (Automatic)
hotspot (Manual)

Learn about setting up wireless network configuration.

Figure 17-74 Manage wireless hot spots using the Wireless Network Connection Properties box
Courtesy: Course Technology/Cengage Learning

A+
220-701
1.10
3.2



Network name (SSID): hotspot

Wireless network key

This network requires a key for the following:

Network Authentication: Open

Data encryption: Disabled

Network key:

Confirm network key:

Key index (advanced): 1

☑ The key is provided for me automatically

□ This is a computer-to-computer (ad hoc) network; wireless access points are not used

Figure 17-75 Enter the SSID of a hot spot to which you want to connect
Courtesy: Course Technology/Cengage Learning

>> CHAPTER SUMMARY

- Networks are categorized in size as a PAN, LAN, Wireless LAN, MAN, or WAN.
- Performance of a network technology is measured in bandwidth and latency.
- The two most popular ways to connect to the Internet are cable modem and DSL. Other methods used include satellite, dedicated fiber optic, dial-up, and wireless technologies such as WiMAX and a cellular WAN.
- Security is a major issue for wireless networks. Security measures used include encryption, disabling SSID broadcasting, and filtering MAC addresses. Encryption standards used include WEP, WPA, and WPA2.
- Technology used by cell phones that allows us to browse the Web, stream music and video, play online games, and use chat and video conferencing is called 3G.
- Bluetooth is a wireless standard used for personal networks such as connecting a PDA to a laptop.
- An Internet card or air card makes it possible to connect a laptop to the Internet using a cellular WAN normally used by cell phones.
- Networking hardware used on local networks includes a network adapter, cables and connectors, wireless access points, routers, switches, and hubs.
- Most wired local networks use twisted-pair cabling which can be unshielded twisted pair (UTP) cable or shielded twisted pair (STP) cable. UTP is rated by category: CAT-3, CAT-5, CAT-5e, and CAT-6.

- A multifunction router can also be a switch, proxy server, DHCP server, wireless access point, firewall, or Internet access restriction device.
- Networking communication happens at three levels: hardware, operating system, and application levels.
- Ways of addressing networks, computers, and applications include domain names, IP addresses, ports, computer names, and NetBIOS names.
- TCP/IP uses protocols at the application level (such as FTP, HTTPS, HTTP, and Telnet), at the TCP level (using TCP or UPD), and at the IP level.
- Classes of IP addresses that can be used by the public include Class A, Class B, and Class C. Some IP addresses are private IP addresses that can be used only on intranets.
- A computer is configured to use dynamic or static IP addresses.
- A PC support person needs to know how to make a wired or wireless connection to an existing network and troubleshoot a connection that is giving problems.

>> KEY TERMS

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

100BaseT
10Base2
10Base5
10BaseT
3G (Third Generation)
802.11b/g/n
access point (AP)
adapter address
AirPort
Automatic Private IP Address (APIPA)
bandwidth
base station
best-effort protocol
Bluetooth
BNC connector
broadband
cable modem
CAT-3 (Category 3)
CAT-5
CAT-6
CDMA (Code Division Multiple Access)
cellular network
cellular WAN
classful subnet masks
classless subnet masks
client/server applications
coaxial cable
computer name
connectionless protocol
connection-oriented protocol
crossover cable
data throughput
default gateway
DHCP (Dynamic Host Configuration Protocol)
dial-up networking
DNS (Domain Name System or Domain Name Service)
DNS server
domain name
DSL (Digital Subscriber Line)
dynamic IP address
enhanced CAT-5 (CAT-5e)
Fast Ethernet
fiber optic
fiber-optic cable
firewall
FTP (File Transfer Protocol)
full-duplex
fully qualified domain name (FQDN)
gateway
Gigabit Ethernet
GSM (Global System for Mobile Communications)
half-duplex
hardware address
host name
Hosts file
HTTP (Hypertext Transfer Protocol)
HTTPS (HTTP secure)
hub
IMAP4 (Internet Message Access Protocol, version 4)
Institute of Electrical and Electronics Engineers (IEEE)
Internet card
Internet Service Provider (ISP)
intranet
IP address
ISDN (Integrated Services Digital Network)
LAN (local area network)
latency
MAC (Media Access Control) address
MAN (metropolitan area network)
multicasting
multiple input/multiple output (MIMO)
name resolution
NAT (Network Address Translation)
NetBIOS (Network Basic Input/Output System)
NetBIOS name
network adapter
Network Address Translation (NAT)
network interface card (NIC)
octet
packet
PAN (personal area network)
patch cable
physical address
Ping (packet internet groper)
POP3 (Post Office Protocol, version 3)
port
port address
port number
PPP (Point-to-Point Protocol)
private IP addresses
public IP addresses
RJ-11
RJ-45

router
Service Set Identifier (SSID)
shielded twisted pair (STP) cable
SMTP (Simple Mail Transfer Protocol)
SMTP AUTH (SMTP Authentication)
status light indicators
subnet mask
switch
TCP (Transmission Control Protocol)
TCP/IP (Transmission Control Protocol/Internet Protocol)
TDMA (Time Division Multiple Access)
Telnet
ThickNet
ThinNet
UDP (User Datagram Protocol)
unshielded twisted pair (UTP) cable
virtual private network (VPN)
WAN (wide area network)
WEP (Wired Equivalent Privacy)
Wi-Fi (Wireless Fidelity)
wireless LAN (WLAN)
WPA (Wi-Fi Protected Access)
WPA2 (Wi-Fi Protected Access 2)

>> REVIEWING THE BASICS

1. Place the following networking technologies in the order of their highest speed, from slowest to fastest: fiber optic, dial-up networking, cable modem, Fast Ethernet
2. What is the difference between ADSL and SDSL?
3. Among satellite, cable modem, and DSL, which technology experiences more latency?
4. When using DSL to connect to the Internet, the data transmission shares the cabling with what other technology?
5. When using a cable modem to connect to the Internet, the data transmission shares the cabling with what other technology?
6. Which version of 802.11 technologies can use two antennas at both the access point and the network adapter?
7. Which wireless encryption standard is stronger, WEP or WPA?
8. What is the name of the port used by an Ethernet cable? What is the name of the port used by a dial-up modem?
9. If you want to upgrade your 100BaseT Ethernet network so that it will run about 10 times the current speed, what technology would you use?
10. What is the maximum length of a cable on a 100BaseT network?
11. What does the 100 in the name 100BaseT indicate?
12. Which type of networking cable is more reliable, STP or UTP?
13. Which is more expensive, UTP CAT5e cabling or STP CAT5e cabling?
14. How can you tell the difference between a patch cable and a crossover cable by examining the cable?
15. What type of server serves up IP addresses to computers on a network?
16. What type of protocol is used to present a public IP address to computers outside the LAN to handle requests to use the Internet from computers inside the LAN?
17. How many bits are in an IPv4 IP address?
18. What port does the SMTP protocol use by default?
19. Which protocol does a Web server use when transmissions are encrypted for security?
20. What type of server resolves fully qualified domain names to IP addresses?
21. What is the maximum length of a NetBIOS name?

22. What is the name of the file that keeps associations between computer names and IP addresses on the local computer?

23. What protocol is replacing the POP protocol used to receive e-mail?

24. Approximately how many IP addresses are available for a single Class A IP license? Class B? Class C?

25. What are IP addresses called that begin with 10, 172.16, or 192.168?

26. In what class is the IP address 185.75.255.10?

27. In what class is the IP address 193.200.30.5?

28. Describe the difference between public and private IP addresses. If a network is using private IP addresses, how can the computers on that network access the Internet?

29. Why is it unlikely that you will find the IP address 192.168.250.10 on the Internet?

30. If no DHCP server is available on a network, what type of configuration must computers on the network use for assignments of IP addresses?

31. If a computer is found to have an IP address of 169.254.1.1, what can you assume about how it received that IP address?

32. What command can be used to cause Windows to release its IP address?

33. What is the purpose of the command, ping 127.0.0.1?

>> THINKING CRITICALLY

1. You have just installed a network adapter and have booted up the system, installing the drivers. You open My Network Places on a remote computer and don't see the computer on which you just installed the NIC. What is the first thing you check?

   a. Is File and Printer Sharing installed?

   b. Is the NetBEUI protocol installed?

   c. Are the lights on the adapter functioning correctly?

   d. Has the computer been assigned a computer name?

2. Your job is to support the desktop computers in a small company of 32 employees. A consulting firm is setting up a private Web server to be used internally by company employees. The static IP address of the server is 192.168.45.200. Employees will open their Web browser and enter *personnel.mycompany.com* in the URL address box to browse this Web site. What steps do you take so that each computer in the company can browse the site using this URL?

3. Linda has been assigned the job of connecting five computers to a network. The room holding the five computers has three network jacks that connect to a switch in an electrical closet down the hallway. Linda decides to install a second switch in the room. The new switch has four network ports. She uses one port to connect the switch to a wall jack. Now she has five ports available (two wall jacks and three switch ports). While installing and configuring the NICs in the five computers, she discovers that the PCs connected to the two wall jacks work fine, but the three connected to the switch refuse to communicate with the network. What could be wrong and what should she try next?

>> HANDS-ON PROJECTS

PROJECT 17-1: Investigating Your PC

If you are connected to the Internet or a network, answer these questions:

1. What is the hardware device used to make this connection (network card, onboard port, wireless)? List the device's name as Windows sees it.
2. If you are connected to a LAN, what is the MAC address of the NIC? Print the screen that shows the address.
3. What is the IP address of your PC?
4. What Windows utilities did you use to answer the first three questions?

PROJECT 17-2: Researching IP Address Classes

Use the Web site *www.flumps.org/ip/* by Paul Rogers to answer these questions:

1. List three companies that have a Class A IP address license.
2. List three companies that have a Class B IP address license.
3. Who owns IP address class license 9.x.y.z?
4. Find another Web site on the Internet that gives similar information. How does the information on the new site compare with the information on the *www.flumps.org/ip/* site?

PROJECT 17-3: Researching Switches

A PC support technician is often called on to research equipment to maintain or improve a PC or network and make recommendations for purchase. You have been asked to upgrade a small network that consists of one switch and four computers from 100BaseT to Gigabit Ethernet. The switch connects to a router that already supports Gigabit Ethernet. Do the following to price the hardware needed for this upgrade:

1. Find three switches by different manufacturers that support Gigabit Ethernet and have at least five ports. Print the Web pages describing each switch.
2. Compare the features and prices of the two switches. Which switch would you recommend for a small business network? What information might you want to know before you make your recommendation?
3. Find three network adapters by different manufacturers to install in the desktop computers that support Gigabit Ethernet. Print Web pages for each NIC.
4. Compare features of the three network adapters. Which one would you recommend and why?
5. What is the total price of the upgrade, including one switch and four network adapters?

PROJECT 17-4: Researching a Wireless LAN

Suppose you want to connect two computers to your company LAN using a wireless connection. Use the Internet to research the equipment needed to create the wireless LAN, and answer the following:

1. Print a Web page showing an access point device that can connect to an Ethernet LAN.
2. How much does the device cost? How many wireless devices can the access point support at one time? How is the device powered?
3. Print three Web pages showing three different network adapters a computer can use to connect to the access point. Include one external device that uses a USB port and one internal device. Verify the devices use the same technology standards as the access point. How much does each device cost?
4. Which technology standards did you match to make sure the adapters and access point are compatible?
5. What is the total cost of implementing a wireless LAN with two computers using the wireless access point?

>> REAL PROBLEMS, REAL SOLUTIONS

REAL PROBLEM 17:1 Setting Up a Small Network

You've been using a Windows 2000 desktop computer for several years, but finally the day has come! You purchase a wonderful and new Windows Vista notebook computer complete with all the bells and whistles. Now you are faced with the task of transferring all your e-mail addresses, favorite Web site links, and files to your notebook.

Your old desktop doesn't have a CD burner, so burning a CD is out of the question. You considered the possibility of e-mailing everything from one computer to another or using floppy disks, but both solutions are not good options. Then the thought dawns on you to purchase a crossover cable and connect the two computers in the simplest possible network. Practice this solution by using a crossover cable to connect two computers and share files between them.

This page intentionally left blank