Lesson 2: Getting Connected

Lesson Objectives

In this lesson you will examine the hardware, media and configuration settings that are required to connect to an organization's network or to the Internet. On successful completion, you will be familiar with:

- ☐ the advantages of networking
- ☐ common network speeds
- ☐ common networking models
- ☐ the role of TCP
- ☐ local area networks (LANs)
- ☐ how wired and wireless connections work
- ☐ addresses used on the LAN
- ☐ wide area networks (WANs)
- ☐ analog and digital signaling
- ☐ methods for connecting to the Internet
- ☐ the role of the domain name system (DNS)
- ☐ the need for security
- ☐ the role of firewalls and gateways
- ☐ the use of virtual private networks (VPNs)
- ☐ basic troubleshooting techniques

Defining a Network

IC³ **Exam 3 - Objective 2.1**

Today, the word "network" is used almost daily in reference to a wide range of technologies. At its very basic definition, a network is a system for moving objects or information.

For example, the Pony Express of 1860-1861 was a U.S. network of stations, riders and horses that moved information (delivered mail) across a 2,000-mile trail that stretched from St. Joseph, Missouri to Sacramento, California. Another example is the public switched telephone network (PSTN), which has been moving information (by way of voice) from coast to coast and around the world since 1915.

In modern computing terms, a network is a group of two or more computers connected in such a way that they can communicate, share resources and exchange data with one another. This definition can include a small business network in one room, or a worldwide network connecting millions of users, such as the Internet.

Advantages of Using a Network

The advantages of using a network include the ability to:

- share files
- use network resources (such as printers)
- access the Internet

Before the days of modern networking, if you wanted to share a file with another user you had to save the file to removable media (in the past this was usually a floppy disk), and then deliver the media to the other user. In an office, you could walk down the hall and hand the disk to someone else. But this method of file sharing was particularly inconvenient if another user was miles (or countries) away.

Sharing resources like printers saves money and allows people to be productive without being overcrowded by redundant equipment.

Network Speeds

A network's speed is determined by its capacity to move information. Capacity is measured in bits, and the speed or data transfer rate of a network is measured in bits per second (bps). As with storage capacities, data transfer speed is often measured in thousands, millions or even billions of bits per second, as shown in the following table:

Measurement	Equal to…
bps	Bits per second
Kbps	Thousand bits per second
Mbps	Million bits per second
Gbps	Billion bits per second

Many factors affect the speed at which data travels across a network. These include:

- type of transmission media (copper wire, fiber-optic cable, free space)
- the network standard used (different standards support different speeds)
- amount of traffic on the network
- speed of networking devices on the network (network card, modem, hub, switch)

A network's capacity for transferring data is also referred to as its bandwidth. Throughout this lesson you will learn about network speeds and factors that can affect performance.

Networking Models

Two networking models have been in common use for several years. These are the client/server model and the peer-to-peer model. A third networking model – the Web-based model – is emerging and becoming more prevalent as the Internet stretches to the far reaches of the globe.

Client/Server Model

Many corporate networks are structured using the client/server model. These networks are also called *server-based* networks. In a server-based network, individual computers and devices interact with one another through a central server through which they are all connected.

In a typical server-based network, the individual PCs are *client* systems. These are the systems used to browse the Internet, check email or print to a network printer. The services requested by the client systems (e.g. Internet access, email or access to network resources) are provided by the server. The *server* is more powerful than the clients connected to it.

Server-based networks are generally more secure than peer-to-peer networks because a central server controls access to all the network resources. To access the network from a client system, users must log on to the network by providing a user name and password.

Peer-to-Peer Model

A *peer-to-peer network* is one in which all the participating computers are more or less equal, and there is no central server. In a peer-to-peer network, each computer connected to the network is called a *host*. Hosts in a peer-to-peer network can share files, an Internet connection, a printer, a scanner or other peripheral devices. A Windows 7 HomeGroup (or in previous versions of the Windows operating system, a Microsoft Windows Workgroup) is an example of a peer-to-peer network.

Web-based Model

Today, because of the global availability of the Internet, companies and individuals can use the Internet as their network "backbone" and connect with other people around the globe. Networking over the Internet is called internetworking, and is becoming more and more common.

Individuals need only a browser and an Internet connection to share files, download applications, watch videos or participate in distance learning.

TCP/IP and Networking

In order for any computing device to communicate with any other device, the two devices must have a common communication scheme. This communication scheme is called a *protocol*. A protocol is simply a set of rules that enable devices to communicate with one another in an agreed-upon manner.

All major operating systems (Windows, Mac OS, UNIX/Linux) support a networking protocol called *Transmission Control Protocol/Internet Protocol (TCP/IP)*. TCP/IP is the standard protocol for both local and wide area networking, and is required for Internet access.

TCP/IP is a collection or suite of protocols that provide services for many things users do on the Web—from downloading email to following hyperlinks and downloading data from an FTP site. The component protocols of the TCP/IP suite are also commonly referred to as a protocol stack. Any network that uses TCP/IP as its networking protocol is referred to as a TCP/IP network.

Local Area Networks (LANs)

Exam 3 - Objective 2.2, 2.3

A *local area network (LAN)* is a group of computers that are connected within a relatively small geographic area, such as a home, office or small group of buildings. A LAN can consist of as few as two computers, or any number of systems up to hundreds of computers and servers. LANs are commonly used for communication between users within an office.

A home network consisting of two computers and a shared printer is a common example of a small LAN. Usually, there is no server involved in a home network and the connected PCs are generally peers.

A corporate office within a building is an example of a larger LAN. Usually, corporate LANs are server-based networks. Users must log on to the network providing a recognized user name and password. Once logged on, a user gains access to the network services and resources.

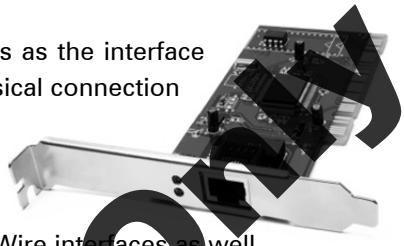
The majority of LANs in use today adhere to a networking standard known as Ethernet. Ethernet is a family of networking technologies for local area networks.

Connecting to the LAN

Whether your LAN is a server-based network or a peer-to-peer network, you must connect to it in order to participate. A connection to the LAN requires:

- a network interface card (NIC)
- a transmission medium (wired or wireless)

Network Interface Card (NIC)



Also called a *network adapter card*, the NIC is a device that serves as the interface between the computer and the network (that is, it provides the physical connection between the computer and the network cabling or wireless signal).

Modern computers include NIC hardware integrated into the motherboard, but it is still common to find NICs that reside in a motherboard PCI expansion slot too. NICs come with USB and FireWire interfaces as well. Laptops often use PCMCIA NICs, which are NICs that you can insert into a special slot on the laptop.

A NIC includes a port for connecting a network cable. A network cable connects the NIC to the network. The other end of the network cable plugs into a port that leads into the network. NICs also come in wireless varieties, allowing you to connect to a Wi-Fi network. Wireless NICs do not include a port for connecting a network cable.

Transmission Medium

In order to send and receive data, a transmission medium must exist. In corporate environments, the most common medium is copper wire in the form of a twisted pair cable (although coaxial and fiber optic cable can also be used). In home networks, a wireless medium is commonly used.

Common LAN Devices

The transmission medium (network cable) provides the physical pathway for information to travel around the network. One end of a network cable plugs into the NIC on a computer; the other end plugs into a port on a connection device on the LAN. LAN connection devices provide a central point of communication, and make it possible for systems connected to it to communicate with one another.

Connection devices can connect individual systems to one another, and can connect separate networks to one another.

The following are common connection devices found on the LAN.

Switches/Hubs

A hub connects computers in a network so they can exchange information. A hub has several ports and each computer attached to the network plugs into a port on the hub using a network cable. Hubs are an old and slow technology, and have largely been replaced by switches or by switch/hub combination devices.

A switch connects either individual systems or multiple networks. Switches include multiple Ethernet ports and different sized switches offer a varying number of ports. The figure shows a 24-port switch.

Routers

Routers can be used to connect networks to one another. Within a LAN, internal routers connect separate portions of the LAN. At the edges of a LAN, a router is used to connect to a public carrier (phone company or Internet Service Provider). That is, a router receives the connections that form a WAN link.

Because a router connects different networks, it serves as the entry point and exit point for each network, and is aptly referred to as a *gateway*.

An organization typically has one router that connects to a public carrier's lines to access the Internet. This type of router is called an *access router* because it provides access to the Internet. The access router provides the path outside the LAN. Because it acts as the gateway to the Internet, this router is referred to on the network as the "*default gateway*."

Wired Connections

Wired LANS use a cable to connect systems to the network. The most common type of cable used in an Ethernet wired LAN is called a twisted pair cable. Other common names for twisted pair cable include: Ethernet cable, patch cable, straight-through cable, network cable and RJ-45 cable.

This is the cable that you plug into your NIC. You plug the other end of the network cable into a network port in order to connect to the network. Depending upon the setup of your LAN, the network port may be located on a wall jack, or located on a hub, switch, broadband router, or DSL or cable modem (modulator/demodulator).

Regardless of the location of the network port, the key is that computers connect to a central device that makes communication possible. For example, in a home network consisting of two PCs, each user might plug in to a port on a broadband router. The broadband router is the central device that makes communication between the two systems possible. In a corporate office, two or three users might connect their PCs to a port on a switch or hub.

Wired Ethernet LANs can move data at rates of 10 Mbps (million bits per second), 100 Mbps, 1 Gbps (billion bits per second), or even 10 Gbps. Wired connections are more secure than wireless connections which are subject to eavesdropping and other illicit activity.

Wireless Connections

In wireless LANs (WLANs), the open air is the connection medium and wireless signals are radio waves sent through the air. Because WLAN signals are radio waves, they can be easily intercepted by unauthorized users, and many network administrators do not allow wireless connections to their corporate LANs. Proper steps must be taken to secure a wireless network. You will learn about WLAN security later in this lesson.

Many modern laptops include built-in wireless NICs, although it is still quite common to see removable wireless NICs in the form of PCMCIA cards and USB devices.

Computers (PCs and laptops) that include a wireless NIC also include a standard NIC that uses a network cable, allowing you a choice in the way you connect. Many users will use a wireless connection when they are computing in a remote area (that is, an area in which there are no network ports available), and then switch to a wired connection when they are back in their office space.

Just as wired connections must ultimately terminate at a central device, wireless LAN connections use a central connection point as well. In wireless LANs, a wireless access point is the central device through which wireless systems connect to the network. The wireless access point itself, however, connects to the LAN through a wired connection.

Wireless connections are most common in homes and small offices, and they are convenient because users can access the network from different locations within the home or office, allowing the user greater mobility. However, wireless connections are slower than wired connections. Common speeds for today's wireless networks are 11 Mbps, 54 Mbps and 300 Mbps, depending on the WLAN standard in use.

Addressing on the LAN

In order for the computers connected to a network to communicate with one another, each computer requires a unique address. There are two types of addresses that are used on a LAN—a MAC address and a network (IP) address.

MAC Address

Every NIC has a unique address permanently burned into it by the manufacturer. This address is the *Media Access Control (MAC) address*. This address is also referred to as the physical address or the hardware address. MAC addresses are used for addressing only by devices within the same LAN, not outside the LAN. For data to be sent outside the LAN, an IP address is used.

Internet Protocol (IP) Addresses

It is a useful and common practice to connect one LAN to another LAN. While MAC addresses are used for addressing by devices within the same LAN, an Internet Protocol (IP) address is used for addressing between devices on different LANs.

Internet Protocol (IP) is the protocol in the TCP/IP suite that is responsible for addressing. Each computer on a TCP/IP network (or on the Internet) has an Internet address that distinguishes it from all other computers on the network. This Internet address is called an *IP address*.

There are two versions of Internet Protocol (IP)—version 4 (IPv4) and version 6 (IPv6). The differences between the versions are not important to our discussion, and IPv4 is still used predominantly.

All addressable devices on a network, including network printers, routers, etc., must have an IP address.

Following are some important points to understand about IP addresses:

- An IPv4 address is a 32-bit address written as a series of numbers divided into four segments with each segment separated by a dot. A sample IPv4 address might be: 200.168.212.226.
- An IP address is not permanent; IP addresses are leased to computers on the network for a specified period of time. If you were to move a computer from one network to another, its IP address would change.
- An IP address provides two pieces of information: it identifies the network on which the host resides, and it identifies the particular host on the network.
- A computer must have an IP address to connect to the Internet.
- An IP address must be unique within the network. When a system is connected to the Internet, its IP address must be unique on the Internet.

Network and host portions

An IP address identifies the network on which a host resides, and it identifies the particular host on the network. To identify these elements, an IP address includes two portions:

- A **network** portion – also called the network identifier, the network ID, or the network prefix. The network portion is indicated by a certain number of bits (starting from the left-most bit).

- A **host** portion – the remaining bits (after the network prefix) identify the specific host on the network.

A special notation called slash notation can be used to indicate how many bits are used for the network prefix. For example, in the IP address 200.168.212.226/24, the network prefix is 200.168.212 (the first 24 bits), and the host ID (consisting of the remaining 8 bits) is 226.

Networking devices use the network and host portions of an IP address to determine which network a particular host resides, and to determine whether that network is local or remote.

What determines an IP address?

A system's IP address is determined by the network on which it resides. That is, all hosts on the same network share the same network address, but must have a unique host number. For example, three nodes on the 200.168.212 network might be 200.168.212.226, 200.168.212.228 and 200.168.212.300.

IP addresses may be manually assigned and configured by a network administrator, or they can be assigned and configured automatically through a service called *Dynamic Host Configuration Protocol (DHCP)*. Many networks (including home broadband networks) use the DHCP service to automatically assign IP addresses to their hosts. In most cases a host leases an IP addresses from a DHCP server when it logs on to the network.

Where do IP addresses come from?

A company or individual cannot merely select an IP address and begin using it. To ensure that each user on the Internet has a unique IP address, addresses are issued by the Internet Corporation for Assigned Names and Numbers (ICANN).

The ICANN allocates blocks of IP addresses to Internet Service Providers (ISPs), which in turn allocate addresses to their customers. When you purchase Internet service, you purchase the right to use a specific IP address (or in the case of a large company, a range of IP addresses) that has been allocated to your service provider.

Other required addressing information

In addition to an IP address, each host on a network must be configured with the following information:

Subnet Mask	A 32-bit number (similar to an IP address) that networking devices use to determine whether a destination system is local (on the same LAN) or remote. If an incorrect subnet mask is specified in a system's network configuration settings, the system will not be able to communicate with other systems on the network.
Default Gateway	Default gateway – this number is the IP address of a networking device that provides access outside the local LAN. The default gateway is usually a router. In order to access the Internet, your system must know the address of the default gateway.

Reserved Address Ranges

The ICANN is in charge of assigning and coordinating IP addresses around the world, and the IP addresses allocated to service providers for distribution to their customers are public IP addresses. Public IP addresses can be used to access and participate on the Internet.

The ICANN has also reserved specific ranges of IP addresses as private IP addresses. A private IP address is an IP address that can be used for communication within the confines of a LAN, but is not routable or addressable over the Internet. Private IP addresses are for local use (*local* means within the LAN).

The following address ranges are reserved as private IP addresses:

- 10.0.0.0 to 10.255.255.255
- 172.16.0.0 to 172.31.255.255
- 192.168.0.0. to 192.168.255.255

Most residential networks use private addresses in the 192.168.0.0. to 192.168.255.255 range.

Private Addresses and Connecting to the Internet

It may be difficult at first to see the advantage to using private IP addresses on your LAN or home network if these addresses cannot be used on the Internet.

In a typical residential LAN setting for example, the home owner purchases Internet service from an Internet Service Provider, and one Internet-addressable IP address is included with the purchased Internet service. The Internet service comes into the home through either a DSL or cable modem or modem/router combination. The modem/router performs several functions, including (but not limited to) the following:

- It assigns private network addresses to the systems connected to it (usually 192.168.1.x), thus establishing an internal LAN.
- It uses a technology called network address translation (NAT) to replace the private IP address used by a system on the LAN with the Internet-addressable IP address that was provided with the purchase of Internet service.

Private network addresses are also commonly used inside corporate LANs. A corporation likely leases several public IP addresses that can be used on the Internet, and then translates private network addresses into public ones when Internet access is required. Network address translation occurs in the same way as it does on a home network, although a corporate LAN might use different hardware (proxy servers, firewalls, etc.).

Connecting LANs Together

It is often useful to connect one LAN to another LAN. For example, if different divisions of a company within a large business each have their own LAN, connecting the LANs allows the divisions to share data and resources.

LANs can be connected to one another using privately-owned communication lines, or they can be connected using communication lines provided by a public carrier such as the phone company or an ISP. When two or more LANs are connecting using a public network, a WAN is created.

Wide Area Networks (WANs)

Exam 3 - Objective 2.2

A *wide area network (WAN)* consists of two or more LANs that cover a wide geographic area (for example, a city, state or country), that are connected using the lines of a public carrier. A public carrier is a telecommunications service provider that is regulated by the government. Examples of public carriers in the United States include AT&T, MCI and Western Union.

Consider a large business with offices in several locations worldwide. Each office has its own LAN which it can use to share resources and data locally. However, if the company needs to share resources with other offices, the LANs can be connected using communication lines provided by a public carrier (such as the phone company or an Internet service provider). When two or more LANs are connected using a public network, a WAN is created. The largest WAN on the planet is the Internet.

The main features that distinguish LANs from WANs are:

- A LAN is confined to local cabling that you install in your home, or that an IT department has routed through the office. In a LAN, the organization owns all the components. In a WAN, an organization leases some of the necessary components that are required to transmit data (such as high-speed telecommunications lines).
- LANs are also usually much faster than WANs. For example, most Ethernet cards transfer data at 10 or 100 Mbps, and in installations using Gigabit Ethernet, data moves at 1 Gbps. A typical WAN connection might run at 1.5 Mbps – 44.736 Mbps.

Public carriers provide services that allow you to send messages and documents over a telephone line to other users.

Public Switched Networks

Exam 3 - Objective 2.2

A public switched network is any carrier network that provides switched services for the purposes of sending communications messages. Phone companies, Western Union and cellular providers all maintain public switched networks. They hire their services out to the public.

The Public Switched Telephone Network (PSTN)

No discussion of networking can ignore the importance of the PSTN. The *public switched telephone network (PSTN)* provides telephone service around the world and is integral to wide area networking because of its infrastructure. Infrastructure is the basic underlying physical structure or framework needed for the operation of a service or enterprise.

Telecommunications companies worldwide have been building the infrastructure of the PSTN for nearly a hundred years installing countless thousands of miles of telephone cable, switches, trunk lines and fiber optic cable. Internetworking depends on connections which are provided by the infrastructure built by these telecommunications providers.

Public carriers often lease their lines for private use to companies or individuals. These leased lines offer high speed data transfer and guaranteed capacity (bandwidth). While Internet Service Providers (ISPs) provide access to the Internet to their customers, this access is often made available through high-speed lines that are leased from public carriers. Usually transparent to the individual user, public carriers furnish most of the long-distance connections that power the Internet

Analog and Digital Signals

Two types of signals are used to transfer information electronically – analog and digital.

Analog signals are electrical signals that vary in amplitude and frequency. These signals are measured in cycles per second, or Hertz (Hz). Broadcast radio and television, and cable TV traditionally use analog signals. And originally, all telephone service was analog as well.

Digital signals are electrical signals that contain one of two values – 1 or 0. Digital signals are measured in bits per second (bps).

Digitizing is the process of converting analog signals into digital signals. Hardware devices such as modems, or signal processing software can easily digitize analog signals.

The Digital Phone Network

Today, the PSTN is almost entirely digital, except for the small portion that extends from the telephone company's central office (CO) to users' homes and offices. The central office is a building where subscriber telephone lines are connected to switching equipment for local and long-distance calls. The small portion of the network that extends from the CO to users homes is called the local loop or the "last mile" and is usually an analog line that provides what is known as plain old telephone service (POTS).

On a POTS line, a telephone conversation begins with an analog signal as voice information is spoken into the receiver. The analog signal travels down the local loop until it reaches the CO. Here, the analog signal passes through a switch and is digitized and sent into the digital heart of the telephone network.

The information remains in its digital format until it reaches the CO for the party receiving the call. Here is it modulated back into an analog signal and sent down the local loop to the receiving party.

Circuit Switching

Circuit switching is a technology that uses a dedicated physical path to send and receive information. The PSTN uses circuit switching.

Consider what happens when you make a phone call.

1. You pick up the receiver and open a connection to the local telephone switch.
2. You dial a number, and the switch then connects to other switches along the PSTN, forming a physical pathway between your telephone and the telephone of the person you are calling. This pathway will be used to transfer voice information back and forth between the two telephones.
3. When the person you are calling answers the phone, a circuit is established and will remain open for the duration of your call. As long as the circuit remains open, no one else can use the telephone line. All the switches and wire pathways involved in the connection remain in use for the entire duration of the call. All the voice information that is exchanged between the calling party and the receiving party travels along this same path (circuit).
4. When you hang up the phone, the circuit is disconnected, and the switches and wire pathways that had been dedicated to your phone call are now free again for other people to use.

Several Internet connection technologies use circuit switching. These include: POTS, ISDN, and leased lines.

Packet Switching

Packet switching is a technology for transferring information which does not rely on a dedicated physical path. In a packet switched network, information is broken down into discrete units called "packets" and addressing information is included in each packet, allowing the packet to be routed to its intended destination. All packets are routed through the network based on their addressing information.

Data networks use packet switching to transfer information between hosts on the network. The Internet also uses packet switching to transfer information between hosts.

Two familiar Internet connection technologies – Digital Subscriber Line (DSL) and cable Internet – also rely on packet switching.

Connecting to the Internet

Exam 3 - Objective 2.1

As you have learned, the Internet is the largest WAN on the planet. As such, you must use a WAN connection to participate on the Internet.

You can purchase a connection through either a telecommunications company or an ISP. Some providers offer dial-up connections, and most offer direct connections through DSL or cable.

Dial-Up Connections

Dial-up connections are very slow and rarely used anymore. However, some users still use dial-up because it is the least expensive method of obtaining Internet access.

POTS Connection

As you have learned, the local loop to users' homes and offices is usually an analog POTS line, which operates at 64 Kbps.

Dial-up connections on a POTS line require the use of a modem which enables computers to transmit data over the analog telephone line. A modem converts (modulates) digital data from a computer into an analog signal which is transmitted over the local loop. (This analog signal is then digitized at the CO and sent through the digital portion of the phone network. When it reaches the CO at the receiving end, the digitized signal is modulated back into an analog signal and sent up the local loop.) The analog signal then passes through another modem on the receiving end of the connection. The receiving modem converts the analog signal back into a digital signal (demodulates) and transmits it to the receiving computer. This type of modem is called a traditional or analog modem.

Note: Today the term modem is widely used and refers to any device that adapts a computer to a telecommunications line or cable TV network.

The modem physically connects to the telephone network using a standard telephone wire. When you use a dial-up connection, your computer uses the modem to dial the access number required to connect to your ISP. When a modem at the ISP "answers" the call, a connection (circuit) is established and maintained for the duration of the data transfer. That is, the phone line remains in use until you disconnect. When you finish your online session, you disconnect from the ISP by hanging up the line.

If you use a dial-up connection, you must establish a connection each time you want to access the Internet. Once your Internet session is complete, you disconnect (hang up).

The maximum possible speed for data transfer over a standard analog telephone line (allowing time for modulation and demodulation) is 56 Kbps.

Integrated Services Digital Network (ISDN)

An *Integrated Services Digital Network (ISDN)* line is a digital telephone line. Because the line is digital, no conversion from analog to digital is required. However, you must still establish a connection when you want to access the Internet, and then hang up when you are done. ISDN transfers data at 128 Kbps.

ISDN has been available throughout most of the world. Today, ISDN has been largely superseded by cable and DSL services.

Direct Connections – Broadband

In contrast to dial-up connections, which require activation for each usage, direct connections provide continuous access to the Internet through permanent network connections. That is, direct connections are always active.

Direct connections are more desirable than dial-up connections because they are generally capable of handling high bandwidth. Direct connections can be obtained in various ways, including leased lines, cable Internet service, digital subscriber lines, and LAN connections.

Often direct connections are referred to as broadband connections. Broadband is a technology that divides the available media bandwidth into multiple channels, and each channel carries a separate signal. This allows a single wire to carry several communications (e.g. voice, fax, data) simultaneously. At one time, broadband systems carried only analog signals. Today, broadband signals can be analog or digital.

Today, the term broadband is used loosely to describe any connection that is always "on" and that provides speeds of 1.544 Mbps or higher.

Leased Lines

A leased line is a permanent connection between two or more locations that consumers can lease (rent) from a phone company. When you lease a line, you do not share it with other consumers; it is available exclusively to you. Typically, leased lines are used by businesses to connect offices that are geographically far apart. Leased lines are also commonly used by companies for Internet access because they offer high bandwidth and are cost-effective for heavy Internet traffic.

Because leased lines are private, they provide a company with a way to expand its private network beyond its immediate geographic area by forming a secure wide area network. Leased lines are reliable and secure, but they are expensive. Competing technologies such as DSL and cable are more cost-effective for small businesses.

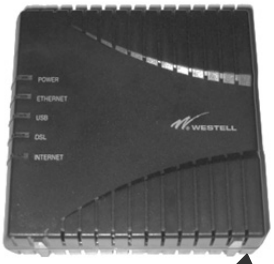
Digital Subscriber Line (DSL)

A *digital subscriber line (DSL)* is a high-speed all-digital connection that uses digital phone lines and a DSL modem. DSL service is provided by the phone company. Several channels are carried over a single wire. DSL service can run on existing copper telephone lines if the lines are in good condition. DSL is a broadband technology; it divides the media bandwidth into multiple channels through multiplexing. DSL is offered by the phone company or telecom provider and is the main competitor to cable Internet connections.

DSL and other broadband modems are not modems in the traditional sense; that is, they do not convert digital signals to analog ones. Broadband modems provide a way to attach a computer to a public carrier's network. These devices are called "modems" because they connect computers to the phone network or to a cable TV network (which have traditionally carried analog signals).

DSL service provides users with a dedicated connection to the provider's digital network. When you have a dedicated connection, you do not share the available bandwidth with anyone else; the connection is all yours. For this reason, DSL subscribers do not experience a slowdown in network response time when more users connect to the network (as is the case with cable Internet subscribers).

Inside the customer's premises, a DSL modem is used to connect to the digital telephone circuit using a telephone cable. The modem also includes an Ethernet port. You attach the modem to your computer using an Ethernet cable by plugging one end of the cable into the Ethernet port on the modem and the other end of the cable into the Ethernet port on your NIC. (Some DSL modems also include a USB port for connecting to the computer.) The picture on the right shows a typical DSL modem.



DSL Availability

Your distance from the provider's central office determines whether you can receive DSL service. If your home or office is too far away from the central office, DSL service will not be available to you. The distance limit for ADSL service is 18,000 feet (5,460 meters).The telephone company's use of loading coils and bridge taps to provide service to a remote area can also disqualify that area for DSL service, as these devices are not compatible with DSL equipment. You must check with a service provider to find out if DSL is available in your area.

DSL Speeds

Different speeds are available with DSL service, depending upon the type of service you use and how far you are from the provider's central office. The farther you are, the more the signal quality decreases and the slower the connection speed gets. The quality of the copper lines also affects signal quality and speed.

There are two speed measurements for DSL service – downstream and upstream. Data moves downstream as it reaches you from another location (for example, when a web server sends a web page that you have requested). The term downloading refers to the downstream flow of data. Data moves upstream when you send or upload information (for example, when you enter a URL in the browser's address bar or submit an online form).

Asymmetric DSL (ADSL)

Asymmetric DSL (ADSL) is the type of DSL service used by most homes and small businesses. ADSL divides the frequencies available on the line in an unequal manner—providing more frequencies for downloading than for uploading. Accordingly, when you use ADSL, your download speed is usually much faster than your upload speed.

ADSL can provide a maximum download speed of 8 Mbps (at 6,000 feet from the central office), and a maximum upload speed of 640 Kbps. In general usage, download speeds are closer to 1.5 Mbps, and upload speeds vary between 64 and 640 Kbps.

Some enhanced services such as ASDL and ASDL+ improve performance. ASDL increases download to 12 Mbps and upstream to 1 Mbps, and ASDL+ improves downstream to as much as 24 Mbps and upstream to 3 Mbps.

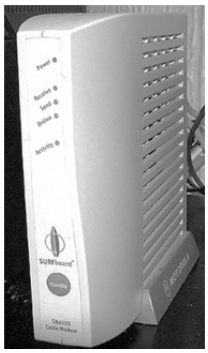
Symmetric DSL (SDSL) service is also available, and is used mainly by businesses. This type of service does not allow you to use the phone at the same time, but the upstream and downstream speeds are the same.

Cable

Cable Internet service is another broadband technology and is a direct competitor to ADSL. Instead of copper phone lines, a cable TV (CATV) system uses coaxial ("coax") cables to transmit signals. You can connect to the Internet through the CATV system using a cable modem.

Outside the customer's premises, the cable modem connects to the provider's cable modem termination system (CMTS), which generally supports several subscribers within the neighborhood. The CMTS connects a group of cable subscribers to the Internet.

Inside the subscriber's premises, the cable modem attaches to the cable service via a coaxial cable (the same type of cable you attach to your television set). The cable modem includes a jack for the coax cable and it also includes an Ethernet port. You attach the modem to your computer using an Ethernet cable by plugging one end of the cable into the Ethernet port on the modem and the other end of the cable into the Ethernet port on your NIC.



The picture to the left shows a cable modem. Although you cannot see the ports, the modem is connected to the cable service through a standard cable TV coaxial cable.

Cable providers generally route a coax loop through a neighborhood to support the subscribers in the general vicinity. Because cable modem users share this network loop (that is, they share the available bandwidth), performance slows down as new users come online.

Cable modem technology will theoretically support speeds of around 30 Mbps. However, actual speeds vary widely. Most providers offer services between 1–6 Mbps downstream, and 128–768 Kbps upstream.

Broadband Routers

In residential and small office networks, the DSL or cable modem provides the connection to the service provider's network, and therefore, to the Internet. These devices are considered routers because they connect a computer or network to the Internet, and are often referred to as residential gateways.

In many cases, these modems allow several users to share one Internet connection. These modems include more than one Ethernet port (or support wireless connections), allowing multiple users to plug in an Ethernet cable and connect to the Internet.

If your DSL or cable modem includes only one Ethernet port (allowing just one connection), you can purchase a separate broadband router and use it on your network to allow multiple users to share one Internet connection.

A broadband router, such as the one shown in the following figure, includes several Ethernet ports. One port is designated as the WAN port (or Internet port). You connect the router to your modem by attaching one end of an Ethernet cable to the router's WAN port, and the other end of the cable to the Ethernet port on your DSL or cable modem. This connection allows the router access to your Internet service.

The other Ethernet ports on the broadband router are LAN ports. When you want to connect other computers to the network, you attach them (via Ethernet cable) to the LAN ports.

Other Factors Affecting Performance

While various WAN technologies (DSL, cable, POTS) determine the top theoretical connection speed, several factors can affect the actual performance of your Internet connection. These include:

- Network traffic – if several users are sharing an Internet connection simultaneously, then the available bandwidth must be shared. This is especially noticeable to cable users. Usually an entire neighborhood shares a cable loop. As more users come online, performance can decrease dramatically.

- Wireless vs. Wired connections – most wireless LANs transmit at 54 Mbps, which is substantially slower than the average 100 Mbps rate for a wired Ethernet connection. Some older WLANs transmit and receive data at 11 Mbps. Newer wireless LANs (called "Wireless N LANs" or "802.11n LANs) operate at 300 Mbps.
- On slower connections, especially dial-up connections, large files such as photographs or audio or video files can seriously slow the loading of a web page. Some dial-up users configure their browsers to suppress the display of images in order to speed up page loading.
- Multiple open tabs – browsers provide for tabbed browsing, which means that you can have several web pages open at one time. Each open web page represents an open connection with a web server, and as such, each open tab uses a certain amount of network resources. On slow connections, working with multiple open tabs can decrease browsing speed.

Addressing on the Internet

Exam 3 - Objective 2.2

You already learned that every computer connected to the Internet must have a unique IP address. This means that web servers (the computers that host web sites) must have IP addresses too.

IP addresses are required if systems on the network are to communicate. For any one computer on the Internet to communicate with another computer on the network, it must know the IP address of the computer with which it wants to communicate.

Have you ever typed an IP address into the address bar of your browser? Chances are you haven't.

Most people type a URL into the browser address bar. The typical URL consists of a protocol identifier and a domain name. How then, does your computer know the IP address of the desired web server when all you type into the address bar is the domain name?

The answer is by using DNS.

Domain Name System (DNS)

The Domain Name System (DNS) is a service that maps unique domain names to specific IP addresses. These mappings are stored on records in a DNS database. Every domain consists of DNS records. A *DNS record* is an entry in a DNS database.

DNS resolves IP addresses into their text-based names. For example, you can access the CCI Learning Solutions web server at IP address 96.53.76.108 by typing: *www.ccilearning.com* in your browser's address bar. In other words: 96.53.76.108 = www.ccilearning.com.

Both the domain name and the IP address refer to the same resource, but the domain name is easier to remember. Without DNS, you would need to enter an IP address any time you wanted to access a resource on the Internet.

DNS Servers

The DNS service is made possible through DNS name servers, which are servers on the Internet whose sole function is to resolve domain names into their IP addresses. For example, when you enter a URL such as www.ccilearning.com into your browser's address bar, the browser contacts a domain name server to obtain the IP address related to this domain name. When the browser receives the IP address 96.53.76.108 from the domain name server, the CCI Learning Solutions site displays on the screen.

Aside from being an integral part of the Internet infrastructure, DNS servers are also used in both enterprise and small business networks. When home users enter a URL into a browser address bar, the host names are resolved to IP addresses by the ISP's DNS server.

If a DNS server is unreachable, you will not be able to navigate to a web site by entering its URL in the browser address bar. You can, however, still reach the site if you know its IP address.

The Need for Security

Exam 3 - Objective 2.1, 2.2

Remember that a LAN is a private network. The systems within a LAN can communicate with one another, but cannot communicate with any system outside the LAN. Systems outside the LAN cannot communicate with a system inside the LAN. All of this changes, however, when a WAN link is added.

Once a LAN is connected to a WAN link, the LAN is connected to the outside world. The systems inside the LAN can communicate with systems outside the LAN, and systems outside the LAN can communicate with systems inside the LAN. This makes the systems inside the LAN vulnerable to malicious activity.

For example, unauthorized users might try to access the network and its resources, or steal data, or introduce viruses to systems within the LAN. Any person who attempts to gain unauthorized access to a computer system is known as a *hacker*. Hackers employ many different methods to obtain what they want. For this reason, network administrators must focus on keeping systems within the LAN secure from unauthorized access and unwanted activity. To combat these risks, IT professionals design and implement specific policies related to security.

When you connect a computer to a network, the information stored on that networked computer can, in theory, be accessed by any computer connected to the network. When you connect a computer to the Internet, you have connected it to the largest network on earth. In theory, any other user on the Internet can (try to) connect to your computer.

As an individual Internet subscriber, you must also take steps to protect your systems from unwanted connections or attack.

Private vs. Public

The systems within a LAN are part of a private network, and are considered trusted systems. However, any system outside the LAN is not trusted. Any system connecting to the LAN over the Internet is especially untrusted.

Because the Internet is not centrally controlled or owned, anyone can access it. For this reason, the Internet is referred to as "the public network." Because there is no central control or ownership over the Internet, no one can "police" the Internet to protect the people who use it. For this reason, the Internet is also referred to as "the open network" or "the untrusted network."

In network diagrams, the Internet is often represented by a cloud, because its contents are unknown.

Authentication and Access Control

Network administrators use authentication and access control to manage network resources and keep the network secure.

Authentication is the process of verifying the identity of a user who logs on to a system or network. The simplest method of authentication is the use of user names and passwords. Access control is the process of controlling who may access particular network resources or services. Access control is usually accomplished by associating specific permissions to each user account. For example, Alice may have permission to access the company web server and the company personnel database, while Bob may have permission to access only the Accounting folder on the network.

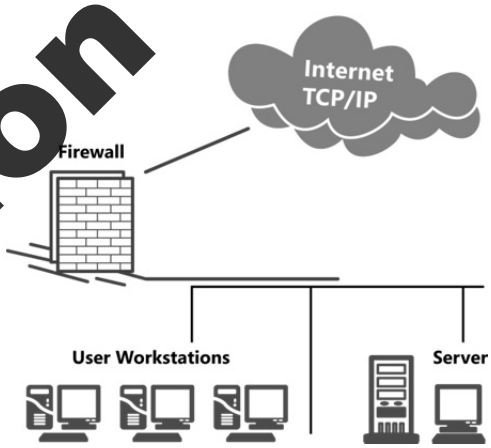
Authentication and access control provide a measure of security within the LAN, but most network security measures are focused on preventing outsiders from accessing the LAN illegitimately.

Firewalls/Gateways

Network professionals use firewalls to protect the LAN from unauthorized access from outside.

A *firewall* is a security barrier that controls the flow of information between the Internet and a private network. A firewall can be a dedicated computer system, a specialized firewall appliance, or it can be implemented on a networking device such as a router. In a home or small office networking environment where a broadband router is used, a firewall is usually built in to the broadband router.

A firewall protects your network from malicious activity coming from outside your network, and provides a "door" through which people can communicate between a secured network (the LAN) and the open, unsecured Internet. A network firewall is most commonly placed between a corporate LAN and the Internet.



By connecting to the Internet through corporate firewalls, no computer on the LAN is actually connected to the Internet, and any requests for information must pass through the firewall. This feature allows users on the LAN to request information from the Internet, but to deny any requests from outside users for information stored on the LAN.

Gateways and Packet Filtering

You have already learned that routers are referred to as gateways. Remember, a router is the entry point into a network, and all incoming traffic comes through the router. From a security standpoint, a gateway is a router that has been configured to protect the network by examining each packet coming into (or out of) the network. The gateway can check each packet against a defined list of rules for what should be allowed in and what should be rejected.

Gateways use a process called *packet filtering* to determine what should be allowed into the network, and what should be rejected.

A packet filtering gateway inspects each data packet as it arrives and then uses simple rules to determine whether that packet should be allowed to pass through to the network. For example, you could examine packets coming from a specific IP address, or destined for a specific IP address. Packet filtering is fast and inexpensive, but it is not a particularly flexible method, nor is it foolproof. Packet filtering is therefore considered the first line of defense in protecting the network.

Advanced Firewall Functions

While gateways can be configured to perform packet filtering only, firewalls can use other methods (in addition to packet filtering) to control traffic flowing in to and out from the network, including:

Stateful Inspection	Stateful inspection firewalls build upon packet filters by having the firewall maintain information about the state of each active connection. When a new packet arrives at the firewall, the filtering mechanism first checks to determine whether the packet is part of a current active (and previously authorized) connection. If the packet is not on the list of active connections, then the firewall checks it against its rules and determines whether the packet should be allowed in. Stateful inspection firewalls are very efficient and cost-effective and the most commonly used firewalls in enterprises.
Proxy service	A proxy replaces the internal network IP addresses with a single IP address which multiple systems can use. Through network address translation (NAT), you can effectively hide the systems connected to your internal network from the outside world.

Desktop Firewalls

Firewalls can also be implemented through software. Also known as personal firewalls, desktop firewalls offer protection for an individual system instead of an entire network. Tools such as Norton 360 or ZoneAlarm Internet Security Suite can detect and respond to attacks on a computer system.

Desktop firewalls offer many firewall features, such as inspection of all incoming transmissions for security threats. When a firewall is used in conjunction with antivirus software, a personal computer is very secure, provided that the user updates these applications frequently.

Many operating systems now include built-in (native) desktop firewall software. Windows, for example, includes Windows Firewall which is enabled by default. You can customize the settings for Windows Firewall just as you can for third-party firewall applications.

Firewall Ports

One of the ways that firewalls determine whether specific data packets should be allowed into the network is by examining the source and destination port of the packet.

Computers use ports for communication, and ports are numbered from 0 to 65,535. Specific applications and services (such as HTTP, DNS, or email) use a specific port number. For example, any request or response for a web page uses the HTTP protocol, and HTTP communications use port 80. Any requests or responses for DNS services use port 53.

One way of securing a network is to block all incoming ports on the firewall, and then open only the specific ports that correspond to the types of communications the network administrator wants to allow into the network. If users inside the LAN will be allowed to view web pages, then the administrator must open port 80 on the firewall. Since DNS helps us locate web pages, the administrator will also have to open port 53.

The configuration of the firewall ports affects all communications coming into and going out from the LAN. An improperly configured firewall can block out phone service, prevent web access, block video and audio from web sites, or disallow instant messaging communications.

Firewall Challenges

Firewalls can present challenges to network users. Sometimes firewall settings block access to particular web sites, or block streaming audio or video from coming into a network. If your corporate system is behind a firewall and you have difficulty connecting to specific Internet sites or services, you may need to contact a network administrator, who can then adjust the firewall configuration.

You may also learn, however, that the service or web site you want to access conflicts with your organization's security policy.

Virtual Private Networks (VPN)

Network administrators put a lot of effort into blocking unauthorized connections from the outside into the LAN. However, they must also provide a method for allowing authorized connections from the outside. Connecting from outside the network is known as remote access.

Security is an especially important component of remote access because communication across a public network (such as the Internet) is vulnerable to interception or eavesdropping. For this reason, remote access methods must provide for authentication and encryption. Authentication is the process of confirming the identity of a user or computer system. Encryption is the process of converting data into an unreadable form of text, which then requires a decryption key in order to be read.

In the past, remote access was provided through remote access servers, modems and dedicated phone lines. In most modern networks, however, access is obtained using a virtual private network (VPN) connection.

A VPN is an encrypted connection between two computers. VPNs allow secure communications across long distances using the Internet as the pathway for communication instead of using a dedicated private line.

VPNs make it possible for telecommuters and traveling employees to establish a secure connection to the company network from outside the company premises. VPNs also make it possible for a company with several satellite offices to establish secure connections between all their locations.

Using VPN

In order for a network to support VPN connections, a VPN server must be set up to receive incoming connections. Any user who wants to make a VPN connection from a remote location (e.g. from home or from a hotel room) must install and then launch VPN client software to open a connection with the VPN server.

Users must log on (authenticate) using a valid user name and password, just as if they were logging on to the network from inside the corporate office.

Wireless Security

Because wireless networks use radio waves to send and receive information, they are susceptible to eavesdropping and unauthorized access. For example, a hacker who is within range of your wireless transmissions can intercept them. User names and passwords should never be sent over unencrypted wireless communications.

Additionally, an unauthorized user can obtain "free" Internet access through your wireless access point if you do not take steps to secure it. Securing your access point and your transmissions is accomplished through wireless encryption.

Wireless Encryption

As you read earlier, encryption is the process of converting data into an unreadable form of text. If a hacker intercepts an encrypted transmission, the encrypted data is useless to him. Decryption is the process of converting encrypted data back into its original readable form.

Encryption and decryption are accomplished through keys. A key is a mathematical algorithm. The more complex the key, the harder it is to decipher the encrypted message without access to the key.

When you configure encryption on a wireless access point, each wireless client that wants to gain access to the wireless network must present an appropriate passphrase when first connecting to the access point. The presentation of the correct passphrase is like entering the correct password when you log on to a network. Only wireless clients that have been configured to supply the correct passphrase will be granted access to the network. The process of gaining access to the wireless network is called authentication.

During the authentication process, the appropriate keys are exchanged so that encrypted transmissions can take place.

Wireless encryption mechanisms include the following:

Wired Equivalent Privacy (WEP)	The original security mechanism for wireless networks. WEP encrypts all data packets sent between the client and the access point, but uses unencrypted exchanges during the authentication process. Today, WEP is considered obsolete and administrators use more advanced security schemes. However, some very old wireless hardware will not support advanced security schemes, and so WEP is the only alternative.
WiFi Protected Access (WPA)	WPA provides better security than WEP, without requiring that wireless networking hardware (NICs and access points) be updated. That is WPA works with most older wireless devices.
WiFi Protected Access 2 (WPA2)	WPA2 provides the most secure encryption, however it requires modern wireless equipment. All new wireless networking hardware supports WPA2 (and some older hardware supports it as well).

You should always use the strongest encryption mechanism supported by your wireless hardware whenever possible.

Network Troubleshooting

Exam 3 - Objective 2.3

Troubleshooting is the process of resolving problems by logically eliminating possible causes, and then finding and correcting the actual cause of the problem. Understanding how network hardware, network addressing and DNS work may help you troubleshoot some common Internet connectivity problems.

If you successfully eliminate the possible causes of a problem at your end of the connection and still cannot connect to the Internet, the problem may lie with your service provider. Call your ISP to see if there is a service outage, or to report one if they are unaware of a problem. If your service provider cannot verify that there is a service outage, you will most likely be connected to a Help Desk professional who will walk you through additional troubleshooting steps to help you resolve your connectivity issue.

Reviewing the Basics

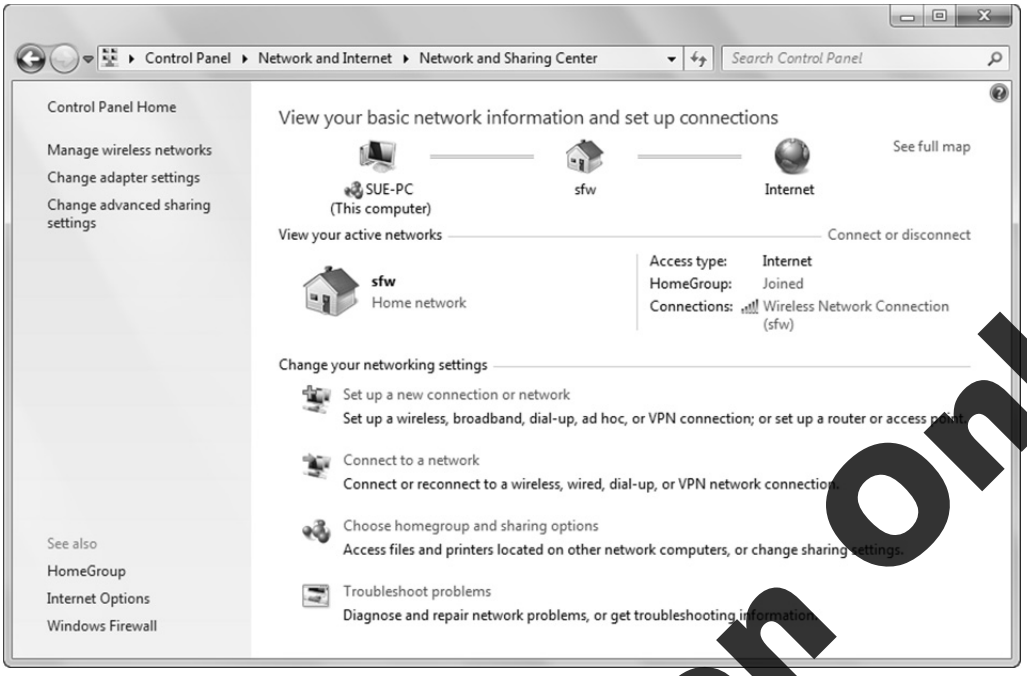
This section will review the concepts covered in this lesson.

- In order for any computer to participate on a network, it needs a valid IP address.
- IP addresses are allocated to ISPs, who in turn allocate them to subscribers. When you (or your organization) purchase Internet service, your ISP gives you an IP address (or a range of IP addresses) to use. The IP address may be configured on the computer manually, but is generally leased to hosts automatically through the use the Dynamic Host Configuration Protocol (DHCP). Most server-based networks such as those used in companies and organizations support their own DHCP server. In home networks, the broadband modem or broadband router provides DHCP service and leases addresses to the systems connected to it automatically, so the user does not have to configure the address.
- Other required addressing information includes the default subnet mask and the address of the default gateway. The networking devices use the subnet mask to determine on which network a particular host resides. If the subnet mask is configured incorrectly, the computer will not be able to communicate with other hosts on the network. The address of the default gateway is the address of the device (usually a router) that leads outside the network. A system must know the address of the default gateway in order to access the Internet.
- In order for a computer to participate on an IP network, it needs a way to connect to the network. This is accomplished through a network interface card (either wired or wireless) and a transmission medium (either a cable or the open air).
- Network hosts connect to one another through a central connection device. In office or school settings, this is often a switch, switching hub or port in a wall jack. In home network settings, the central connection device is often a broadband modem or router. Most broadband modems and routers offer both wired and wireless connectivity.
- Domain Name System (DNS) is a service that allows you to enter user-friendly URLs instead of IP addresses into a browser address bar in order to locate web sites on the Internet. DNS maps domains to IP addresses. If the DNS server on your company network (or on your ISP's network) is down, you will not be able to navigate to web sites using URLs.
- To check if you are connected to a network, you can use the Network Sharing Center to view what connections are available to you and the status of the networks. Within this feature of the Control Panel, you can also view the IP address or DNS Server, as well as change the connection from one network to another, e.g. LAN to wireless.

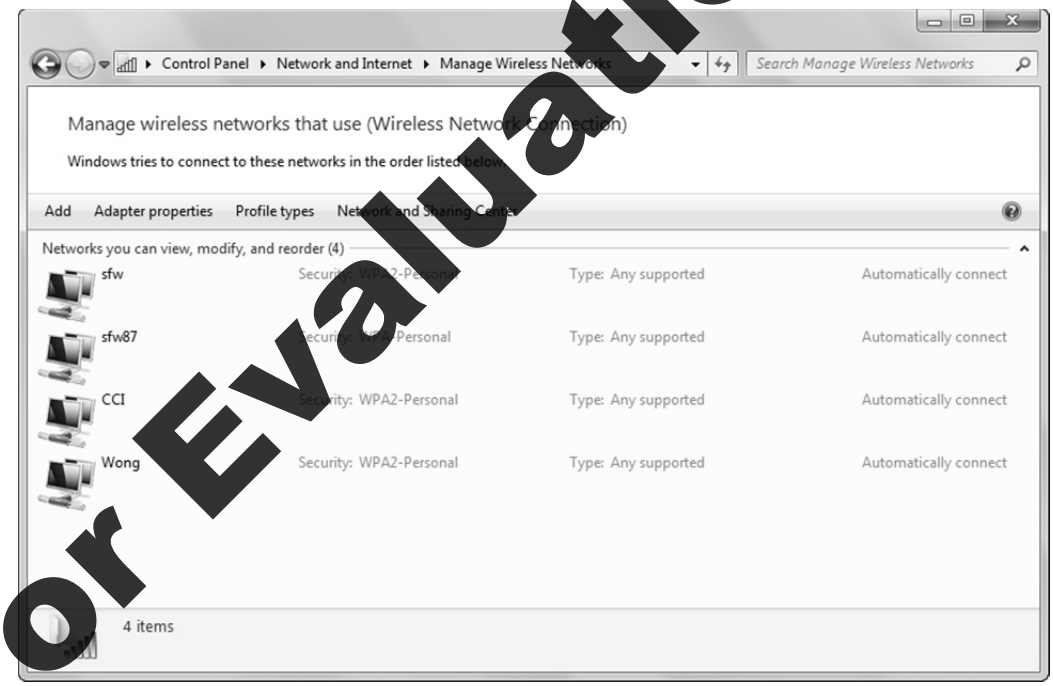
EXERCISE

In this exercise you will use the Network Sharing Center to check on the status of the connection for your computer, and view general information about the connections. The images provided in this exercise are meant for demonstration and comparison purposes; they will differ from what has been set up on your computer.

1. Click the **Start** button and click **Control Panel**. Then click **View network status and tasks**.



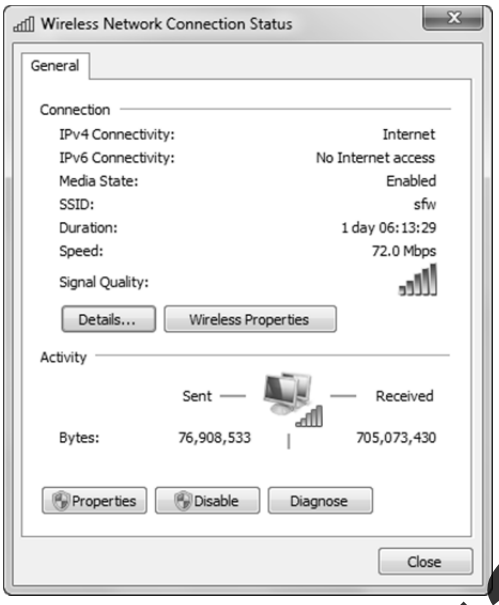
2. If there are any wireless connections available for your computer, click **Manage wireless networks** from the options in the left panel.



In this window, you can change the order of available wireless connections, add a new wireless connection, or view or change properties for the connection. Notice in our example that each of the connections has security set up where a password is required to be able to connect when within connection distance.

3. Click the **Back** button to go back one window.
4. Click **Change adapter settings** from the options in the left panel.

5. Click an active connection in the list and then on the Command bar, click the **View status of this connection**.



6. Click the **Details** button to view more information on the status of your connection.
7. Click **Close** to exit all windows.

Troubleshooting Hardware Issues

Although network hardware is required to support Internet access, most users seldom examine the devices to which they are connected. Even though the average user cannot repair hardware that is not functioning properly, anyone can examine simple indicators to help determine what particular issue might be causing a connectivity problem.

Indicator Lights

Almost all networking devices (NICs, hubs, switches, broadband routers/modems) include one or more indicator lights that relay information about how the device is performing.

Every NIC includes a green light emitting diode (LED) that flashes intermittently as information is transferred to and from the computer through the NIC. If you are unable to access the network, you can first visually examine the NIC to see if it is functioning. USB NICs are the easiest to see, and laptops and netbooks also include an indicator (usually on the keyboard) that is illuminated when the wireless NIC is active.

Most hubs and switches include an LED indicator for each connection port, and the indicator lights up when a device is properly connected to a port (through a network cable). Most broadband routers also include a green LED for each wired port, and the indicator lights up when a device is plugged into the port. If you are experiencing connectivity problems, trace your network cable to the router and ensure that the LED is lit on the port to which you are connected. If it is not, unplug the cable and plug it in again to create a secure connection. If the port LED still does not light up, try connecting to a different port. Depending on whether you are working on an organization's network or your home network, you should either notify someone in the IT department about the connection problem, or plan to purchase a new broadband router.

If a broadband router also functions as a wireless access point, the WLAN indicator light will be illuminated when the wireless function is turned on. If your wireless device cannot find the access point, make sure that the access point is turned on.

Broadband modems also include indicator lights for the following conditions: power on, sending signal, receiving signal, PC activity (this light comes on when the computer is connected to the modem), and Online (this light indicates that the modem has negotiated a successful connection with the provider's network). Visually inspect the modem to ensure all appropriate lights are on.

Firmware Updates

When you use a direct connection, such as DSL or cable, it is not uncommon for your service provider to periodically send firmware updates to your modem. Firmware updates affect the way in which hardware functions. Sometimes the modem will not function correctly after the installation of a firmware update until the device is powered off and then restarted. This process is similar to rebooting a computer system; power off the modem, wait a few moments, and then power it back on again.

There is no easy way to tell when a firmware update has been installed; therefore, if a modem was functioning properly and then suddenly stops working, the solution may be as simple as restarting it.

If you find it necessary to restart your broadband modem, it is considered best practice to also restart any other networking hardware devices connected to it – including broadband routers and VoIP devices or analog phone adapters.

Signal Quality Issues

The transmission of network signals is dependent on the transmission medium. The connections between the wires in an Ethernet cable and the contacts in the connector can sometimes work loose, or a wire may break somewhere in the middle of the cable. A damaged cable will not transmit signals. If you suspect that a cable is damaged, replace it with a new one. Ethernet cables are relatively inexpensive, and connecting and disconnecting an Ethernet cable is a simple matter of plugging it in or pulling it out (just like a telephone cord.)

An Ethernet cable that is not fully and securely connected cannot transmit signals correctly either. If you are experiencing network connectivity issues, a simple troubleshooting measure is to check the connections. If the cable is not plugged in properly, disconnect it and then reconnect it.

Certain conditions can also affect the strength and quality of wireless signals. Wireless signals can pass through office walls in most buildings, but the environment in which a wireless device operates limits its range. For example, a wireless access point operating in the open air might have a range of between 120 and 200 meters, but in a closed environment where signals must pass through wood or brick walls, the range is reduced to between 15 and 25 meters. In an environment where the signal must pass through metal reinforced walls, ceilings and elevator shafts, the signal range is reduced to 10 meters, and in some cases, the access point may not be able to sustain a connection at all.

In a corporate environment, the IT staff may consider adding more access points, placed at strategic positions throughout the workplace to boost the wireless signals. In a home environment, if you find that the wireless signal is not strong enough, you can try repositioning the antennas on the access point or moving the wireless client closer to the access point.

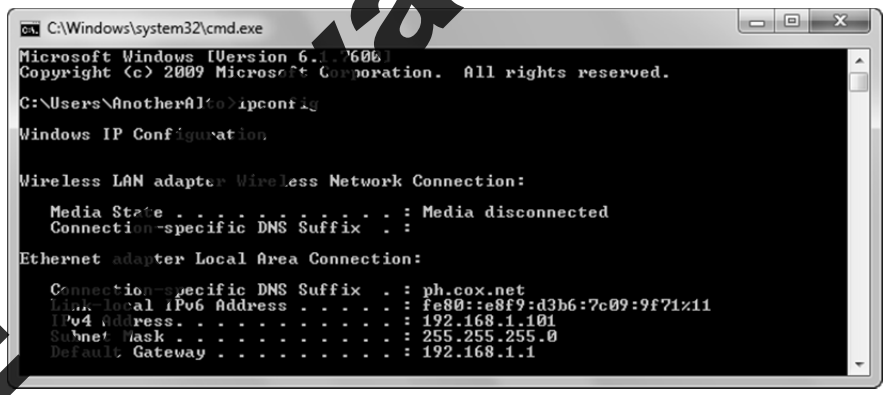
Wireless communications are also subject to interference from other devices (e.g. microwave ovens, garage door openers, baby monitors) operating in the same frequency range. If you believe other devices are interfering with your wireless signals, avoid operating these devices, and/or move your wireless client further from the sources of the interfering signals.

To test what may be affecting your connection to the Internet try to connect to a LAN using an Ethernet cable only. If you can connect to the Internet in this way, then there may be an issue with the wireless router and you can begin troubleshooting steps to determine and resolve the issue.

Troubleshooting Addressing Issues

In order to participate successfully on the Internet, a computer must be configured with the proper IP address, subnet mask and default gateway. Together with other values, these three items constitute your system's network configuration settings.

End users do not normally specify these settings, and seldom make changes to them. In most cases, a computer automatically obtains these settings from a DHCP server. You may, however, be asked by a member of the IT staff or a member of your ISP's Help Desk team to view these settings and report on their current values. You can check your network configuration settings using a utility called IPCONFIG.



To use the IPCONFIG utility, perform the following steps:

1. Click **Start**.
2. In the Search box, type: `cmd` and press Enter.

   This step opens a command prompt window.
3. In the command prompt window, type: `ipconfig` and press Enter.
4. Look for the line that begins "IPv4 Address …" to find the three required settings.

Even though you may not know what your IP address should be, you can easily recognize two IPv4 addresses that indicate a problem. These are:

0.0.0.0

169.254.x.x (where *x* can be any number between 0 and 255)

The 0.0.0.0 address is a special initialization address a system uses when it is trying to obtain an IP address from a DHCP server. If your system is using 0.0.0.0 as its IP address, it means that it was unable to reach the DHCP server and does not have a valid IP address.

If your system is using 169.254.x.x as its IP address (along with the subnet mask 255.255.0.0), it means that it was unable to reach the DHCP server and it has configured itself with an IP address using the Windows Automatic Private IP Addressing (APIPA) feature.

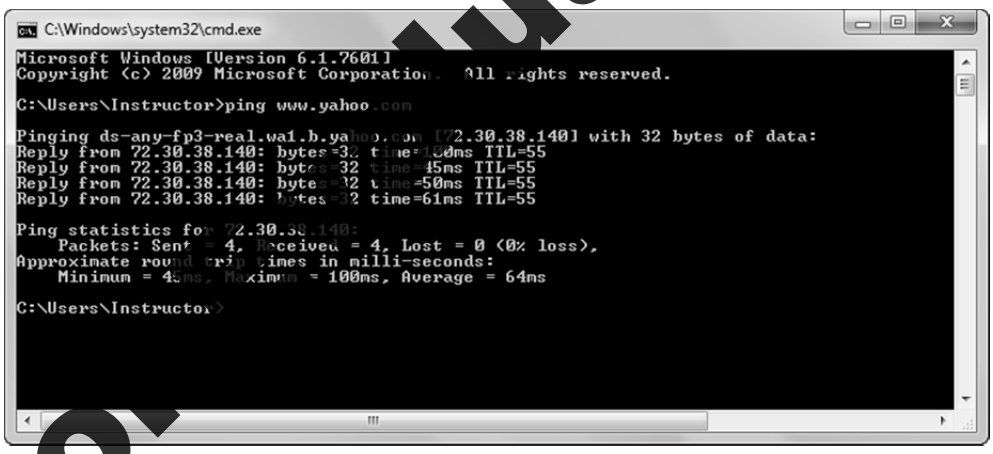
The APIPA address range (169.254.0.1 through 169.254.255.254) is a range of private IP addresses that cannot be used on the Internet. The system uses the self-configured IP address until a DHCP server becomes available.

If you check your configuration settings and see that your system is using either an initialization address or an APIPA address, it means that your system is unable to contact the DHCP server on the network.

Check first to ensure that your network cable is plugged in. If the cable is plugged in, and you are connected to your organization's network, your next step should be to the IT department. If you are working on a home network, you may need to restart your broadband modem or router.

Testing Connectivity with Addresses

In the previous lesson, you used the PING utility to test Internet connectivity. If you receive one or more reply messages, then connectivity is confirmed.



You can ping specific addresses to help determine where a break in connectivity may lie.

For example, if your NIC and network cable are functioning correctly, you should be able to successfully ping your own IP address.

If the NIC and cable are good and your network configuration settings are correct, you should be able to successfully ping other computer systems on the local network, and you should be able to ping the default gateway.

Further, if your Internet connection is functioning, you should be able to ping your ISP or your favorite web site by its IP address, assuming that the web site is configured to respond to ping requests. At the time of this writing, the web servers at Yahoo.com (www.yahoo.com) and CCI Learning (www.ccilearning.com) are configured to respond to ping requests, and you can ping them to test for Internet connectivity.

If you cannot ping the Yahoo or CCI Learning servers by domain name, try pinging them by IP address. The IP address for Yahoo is 72.30.38.140. The IP address for CCI Learning is 96.53.76.108. If you can successfully ping a web site by its IP address but not by its domain name, then the network (or ISP) DNS server is not functioning or is unreachable.

To use the ping utility, perform the following steps:

1. Click **Start**.
2. In the Search box, type: `cmd` and press Enter. This step opens a command prompt window.
3. In the command prompt window, type: `ping [ip_address]` (where ip_address is the IP address of the system you are trying to reach) and press Enter.
4. Look for reply messages to verify connectivity.

Troubleshooting Security Settings

Security settings can also cause connectivity issues.

Wireless Security

Most wireless LANs use an encryption scheme to protect access to the network and the network resources. Even hotels that offer free WiFi to guests may require that you enter a passphrase when attempting to connect to the network.

If you are having difficulty gaining access to a wireless network, make sure that you know the correct passphrase and that you are entering it correctly.

Participating on an encrypted wireless network requires that both the client and the access point are using the same encryption scheme (WEP, WPA or WPA2). Some wireless clients require that you specify which encryption scheme to use. Be sure that you specify the correct scheme. Ask the network administrator is you need assistance.

Firewall Configuration

Firewalls protect a computer system by blocking potentially dangerous communications from the outside. Determining what is "dangerous" is often a matter for the network administrator.

If you are using a system at your school or workplace and cannot use particular Internet applications, such as Instant Messaging, or cannot view videos from the Internet, ask the network administrator if these applications are blocked.

Depending on the company security policy and your ability to justify your need to use these blocked applications, the administrator may adjust the firewall settings to allow you to use these applications.

On a home network, you decide what is allowed through the firewall. When you install Internet-based programs, the installation procedure often opens the appropriate ports on the Windows firewall (assuming you have sufficient rights to install software).

If you experience problems using Internet-based applications, you can look on the vendor's web site for information on known issues concerning firewall settings, and then make the appropriate changes to the firewall.

EXERCISE

In this exercise, you will troubleshoot basic connectivity issues in your classroom. You will also consider specific scenarios and describe the steps required to resolve the problems described in each one.

Optional: During a break, your instructor will create connectivity problems for certain classroom systems. If your instructor has elected not to perform this part of the exercise, begin at Step 5.

1. As a class, work with your instructor to identify the problem on each of the affected systems.
2. Use the process of elimination to try to isolate the cause of each problem.
3. When you have isolated the cause of each problem, take the required steps to resolve the problem.
4. Test each system to confirm that the problem has been resolved.
5. As a class, consider the following scenarios, and identify the required steps to identify and resolve each problem.

   Scenario 1: Your home Internet connection has been functioning for months, and then one morning you discover that you cannot get out onto the Internet.

   Use the ipconfig command to discover the IP address, subnet mask and default gateway. Make sure that the system is not using an initialization address or an APIPA address. If your system is using either of these addresses, try rebooting the modem, router and computer system.

   If your system has a valid IP address, ping other systems on the local network or ping the default gateway to make sure the local hardware is functioning properly.

   If you can ping other systems on the network or your default gateway, try to ping your ISP. If you can ping the default gateway, but not your ISP, try rebooting modem, router and the computer system.

   If you reboot all the devices and still cannot obtain Internet access, call your ISP.

   Scenario 2: You have just begun working for a new company. On your first day at work, you successfully log on to the network, and then successfully get out to the Internet. You download and install Windows Live Messenger, but when you try to log in to Messenger, you cannot connect to the Windows Live Messenger server.

   Since you can log on to the network and to the Internet, you already know that the networking hardware is functioning properly and that Internet connectivity is not the issue.

   Ask your supervisor or someone in the IT department if instant messaging applications are allowed in the workplace. If they are not, you can to make a case for why they should be allowed.

   Scenario 3: Your company has just expanded its office space and your entire department has been relocated to a different floor in the building. When you get to your new office, you discover that you cannot log on to the company network or get on to the Internet.

   See if your co-workers are having the same problem. If more than one person is having connectivity problems, the problem may lie with some of the networking devices.

If no one else is having difficulty, check your network cable to make sure it is connected properly. If only one person in a local group is experiencing connectivity problems, it is likely that the problem lies with the individual computer system. After a moving an entire department, it is possible that an IT staff person forgot to connect your network cable.

Lesson Summary

In this lesson you examined the hardware, media and configuration settings that are required to connect to an organization's network or to the Internet. You should now be familiar with:

- ☑ the advantages of networking
- ☑ common network speeds
- ☑ common networking models
- ☑ the role of TCP
- ☑ local area networks (LANs)
- ☑ how wired and wireless connections work
- ☑ addresses used on the LAN
- ☑ wide area networks (WANs)
- ☑ analog and digital signaling
- ☑ methods for connecting to the Internet
- ☑ the role of the domain name system (DNS)
- ☑ the need for security
- ☑ the role of firewalls and gateways
- ☑ the use of virtual private networks (VPNs)
- ☑ basic troubleshooting techniques

Review Questions

1. Which of the following data transfer speeds is the fastest?
   a. 3 Gbps
   b. 300 Mbps
   c. 300 Kbps
   d. 3,000,000 bps
2. Which of the following statements is true of an IP address?
   a. It is permanent.
   b. It is burned onto a NIC by the manufacturer.
   c. It identifies the network on which a host resides, and it identifies the particular host on the network.
   d. It is not required for Internet access.
3. Which of the following statements is true of a wide area network (WAN)?
   a. A WAN is usually confined to a small geographic area.
   b. A WAN is formed when two or more LANs are connected using a public network.
   c. A WAN is almost always faster than a LAN.
   d. A WAN is confined to the local cabling you install in your home or office.
4. What do POTS, ISDN and leased lines have in common?
   a. They all use circuit switching.
   b. They all use packet switching.
   c. They are all dial-up connections.
   d. They are all direct connections.
5. The term broadband refers to:
   a. any high-speed connection that uses circuit switching.
   b. any high-speed connection that is always "on".
   c. any high-speed dial-up connection.
   d. any type of connection that provides access to the Internet.

6. Which of the following can improve browsing performance on a dial-up connection?
   a. Suppressing the display of images.
   b. Opening multiple browser tabs to distribute the page loading task.
   c. Sharing the dial-up Internet connection with several computers.
   d. Opening an instant messaging application while browsing.
7. Which service enables users to access web sites by domain name instead of by IP address?
   a. DHCP
   b. DNS
   c. DSL
   d. APIPA
8. Which of the following statements accurately describes gateways and firewalls?
   a. Gateways use packet filtering to protect a network; firewalls can use packet filtering as well as more advanced techniques for controlling traffic flow.
   b. Firewalls use packet filtering to protect a network; gateways can use packet filtering as well as more advanced techniques for controlling traffic flow.
   c. Firewalls protect network resources while gateways protect sensitive information.
   d. Gateways protect network resources while firewalls protect sensitive information.
9. What does a virtual private network (VPN) provide?
   a. A security barrier that blocks incoming communication requests.
   b. Secure access into a private network from the outside.
   c. Security for wireless networks.
   d. An increase in web browsing performance.
10. Which wireless encryption scheme provides the strongest level of protection?
    a. WEP
    b. WEP2
    c. WPA
    d. WPA2