# Chapter 8: Fundamental Networks

## IT Essentials: PC Hardware and Software v4.1

Cisco | Networking Academy®
Mind Wide Open™

# Chapter 8 Objectives

- 8.1 Explain the principles of networking
- 8.2 Describe types of networks
- 8.3 Describe basic networking concepts and technologies
- 8.4 Describe the physical components of a network
- 8.5 Describe LAN topologies and architectures
- 8.6 Identify standards organizations
- 8.7 Identify Ethernet standards
- 8.8 Explain OSI and TCP/IP data models
- 8.9 Describe how to configure a NIC and a modem
- 8.10 Identify names, purposes, and characteristics of other technologies used to establish connectivity
- 8.11 Identify and apply common preventive maintenance techniques used for networks
- 8.12 Troubleshoot a network

# Principles of Networking

- Networks are systems that are formed by links.
- People use different types of networks every day:
  - Mail delivery system
  - Telephone system
  - Public transportation system
  - Corporate computer network
  - The Internet


- Computers can be linked by networks to share data and resources.
- A network can be as simple as two computers connected by a single cable or as complex as hundreds of computers connected to devices that control the flow of information.

# Computer Networks

- A computer data network is a collection of hosts connected by networking devices such as computers, printers, scanners, smartphones and file and print servers.
- Resources shared across networks include different types of services, storage devices and applications.
- Network devices link together using a variety of connections:
  - Copper cabling
  - Fiber-optic cabling
  - Wireless connection
- Some benefits from networking includes:
  - Fewer peripherals needed
  - Increased communication capabilities
  - Avoid file duplication and corruption
  - Lower cost licensing
  - Centralized administration
  - Conserve resources

# Types of Networks

A computer network is identified by:

- The type of media used to connect the devices
- The type of networking devices used
- How the resources are managed
- How the network is organized
- How the data is stored
- The area it serves

# Types of Networks

- **LAN**: A group of interconnected computers under one administrative control group that governs the security and access control policies that are in force on the network.

- **WAN**: A networks that connects LANs in geographically separated locations.

- **WLAN**: Group of wireless devices that connect to access points within a specified area. Access points are typically connected to the network using copper cabling.

# Types of Networks (Continued)

- **Peer-to-peer networks**: Devices which are connected directly to each other without any additional networking devices between them. Each device has equivalent capabilities and responsibilities.

- **Client/server networks**: In a client/server model, the client requests information or services from the server. The server provides the requested information or service to the client.

# Bandwidth and Latency

- **Bandwidth** is the amount of data that can be transmitted within a fixed time period.
- Bandwidth is measured in bits per second and is usually denoted by the following:
  - bps - bits per second
  - Kbps - kilobits per second
  - Mbps - megabits per second
- **Latency** is the amount of time it takes data to travel from source to destination.
- Data is transmitted in one of three modes:
  - **Simplex** (Unidirectional transmission) is a single, one-way transmission.
  - **Half-duplex** allows data to flow in one direction at a time.
  - **Full-duplex** allows data to flow in both directions at the same time.

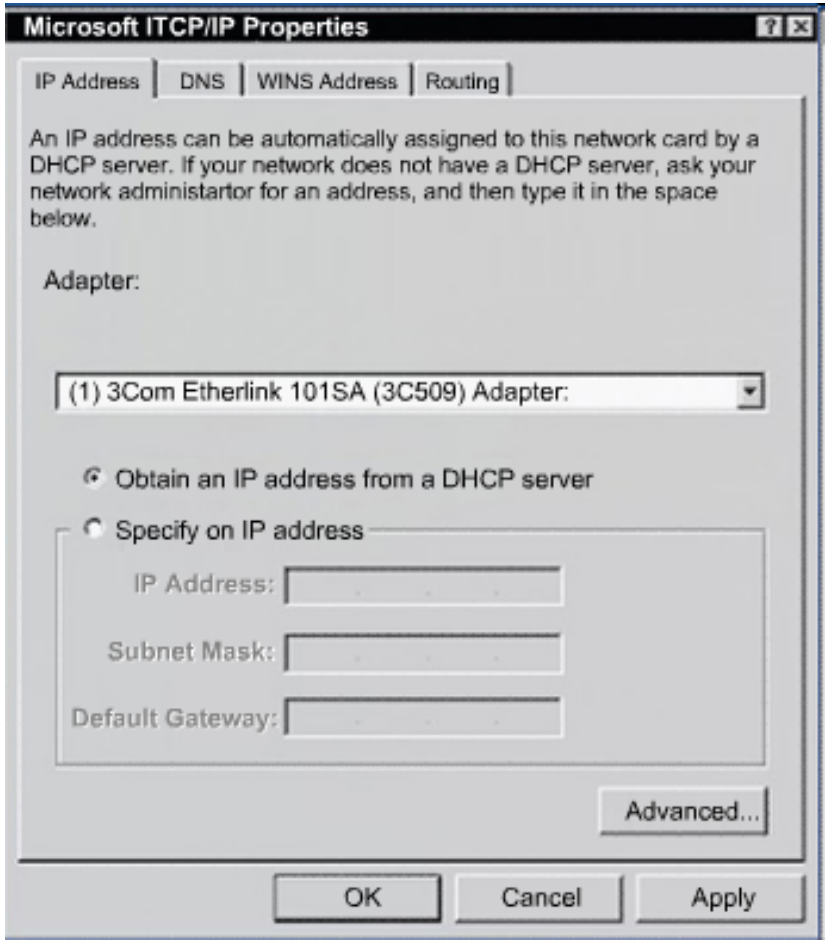
# IP Address

- An IP address is a unique number that is used to identify a network device and is represented as a 32-bit binary number, divided into four **octets** (groups of eight bits):
  - Example: 10111110.01100100.00000101.00110110
- An IP address is also represented in a **dotted decimal** format.
  - Example: 190.100.5.54
- When a host is configured with an IP address, it is entered as a dotted decimal number, such as 192.168.1.5. This IP address must be unique on a network to ensure data can be sent/received.
- IP Classes
  - Class A: Large networks, implemented by large companies and some countries
  - Class B: Medium-sized networks, implemented by universities
  - Class C: Small networks, implemented by ISP for customer subscriptions
  - Class D: Special use for multicasting
  - Class E: Used for experimental testing

# Subnet Masks

- IP address used to indicate the network and the host portion of an IP address.
- Usually, all hosts within a broadcast domain of a LAN (bounded by routers) use the same subnet mask.
- The default subnet masks for three classes of IP addresses.
- An IP address can be configured:
  - **Manually**: typing the proper IP address and subnet mask
  - **Dynamically**: Using a **Dynamic Host Configuration Protocol (DHCP)** server.
- **Network Interface Card (NIC)** is the hardware that enables a computer to connect to a network and it has two addresses:
  - The IP address is a logical address that can be changed.
  - The **Media Access Control (MAC)** address that is "burned-in" or permanently programmed into the NIC when manufactured.

# Dynamic Host Configuration Protocol (DHCP)




- DHCP automatically provides computers with an IP address.
- The DHCP server can assign these to hosts:
  - IP address
  - Subnet mask
  - Default gateway
  - Domain Name System (DNS) server address

# DHCP Process and Advantages

- DHCP process:
  1. DHCP server receives a request from a host.
  2. Server selects IP address information from a database.
  3. Server offers the addresses to requesting host.
  4. If the host accepts the offer, the server leases the IP address for a specific period of time.
- Advantages of DHCP:
  - Simplifies the administration of a network
  - Reduces the possibility of assigning duplicate or invalid addresses
- Configure the host to "Obtain an IP address automatically" in the TCP/IP properties of the NIC configuration window

# Internet Protocols

- A **protocol** is a set of rules. Internet protocols govern communication within and between computers on a network.
- Many protocols consist of a **suite** (or group) of protocols stacked in layers. These layers depend on the operation of the other layers in the suite to function properly.
- The main functions of protocols:
  - Identifying errors
  - Compressing the data
  - Deciding how data is to be sent
  - Addressing data
  - Deciding how to announce sent and received data
- Protocols used for browsing the web, sending and receiving e-mail, and transferring data files.
  - TCP/IP
  - NETBEUI and NETBIOS
  - IPX and SPX
  - FTP
  - SSH
  - Telnet
  - POP
  - IMAP
  - SMTP
  - HTTP and HTTPS

# Internet Control Message Protocol (ICMP)

- **Internet Control Message Protocol (ICMP)** is used by devices on a network to send control and error messages to computers and servers.
- **PING (Packet Internet Groper)** is a simple command line utility used to test connections between computers.
  - Used to determine whether a specific IP address is accessible.
  - Used with either the hostname or the IP address.
  - Works by sending an ICMP echo request to a destination computer.
  - Receiving device sends back an ICMP echo reply message.
- Four ICMP echo requests (pings) are sent to the destination computer to determine the reliability and reachability of the destination computer.

# Physical Network Components

- Network devices:
  - Computers
  - Hubs
  - Switches
  - Routers
  - Wireless access points
- Network media:
  - Twisted-pair copper cabling
  - Fiber-optic cabling
  - Radio waves

# Network Devices

- Hub
  - Extend the range of a signal by receiving then regenerating it and sending it out all other ports.
  - Allow a lot of **collisions** on the network segment and are often not a good solution.
  - Also called **concentrators** because they serve as a central connection point for a LAN.

- Bridges and Switches
  - A packet, along with its MAC address information, is called a **frame**.
  - LANs are often divided into sections called **segments** bounded by bridges.
  - A **bridge** has the intelligence to determine if an incoming frame is to be sent to a different segment, or dropped. A bridge has two ports.
  - A **switch** (multiport bridge) has several ports and refers to a table of MAC addresses to determine which port to use to forward the frame.

# Network Devices (Continued)

- Routers
  - Devices that connect entire networks to each other. They use IP addresses to forward packets to other networks.
  - A router can be a computer with special network software installed or can be a device built by network equipment manufacturers.
  - Routers contain tables of IP addresses along with optimal routes to other networks.

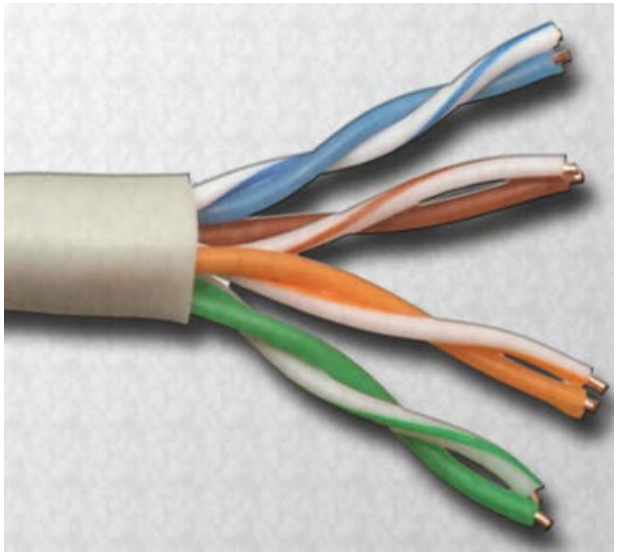
- Wireless Access Points
  - Provide network access to wireless devices such as laptops and PDAs.
  - Use radio waves to communicate with radios in computers, PDAs, and other wireless access points.
  - Have limited range of coverage.

# Network Devices (Continued)

- Multipurpose Devices
  - Perform more than one function.
  - More convenient to purchase and configure just one device.
  - Combines the functions of a switch, a router and a wireless access point into one device.
  - The Linksys 300N is an example of a multipurpose device.

# Twisted-Pair Cabling

- A pair of twisted wires forms a circuit that transmits data.
- The twisted wires provide protection against crosstalk (electrical noise) because of the cancellation effect.
- Pairs of copper wires are encased in color-coded plastic insulation and twisted together.



- An outer jacket of poly-vinyl chloride (PVC) protects the bundles of twisted pairs.
- There are two types of this cable:
  - **Unshielded twisted-pair (UTP)**

    (Cat 3, Cat 5, 5e and Cat 6)
  - **Shielded twisted-pair (STP)**

# Coaxial Cable

- A copper-cored network cable surrounded by a heavy shielding

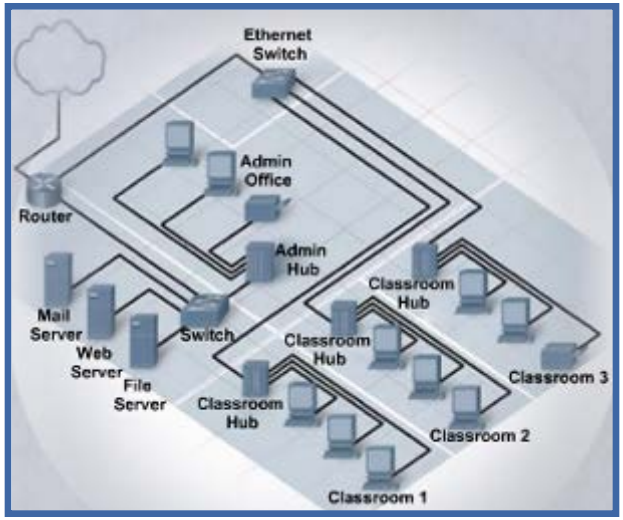
- Types of coaxial cable:
  - **Thicknet or 10Base5** - Coax cable that was used in networks and operated at 10 megabits per second with a maximum length of 500 m
  - **Thinnet or 10Base2** - Coax cable that was used in networks and operated at 10 megabits per second with a maximum length of 185 m
  - **RG-59** - Most commonly used for cable television in the US
  - **RG-6** - Higher quality cable than RG-59 with more bandwidth and less susceptibility to interference

# Fiber-Optic Cable

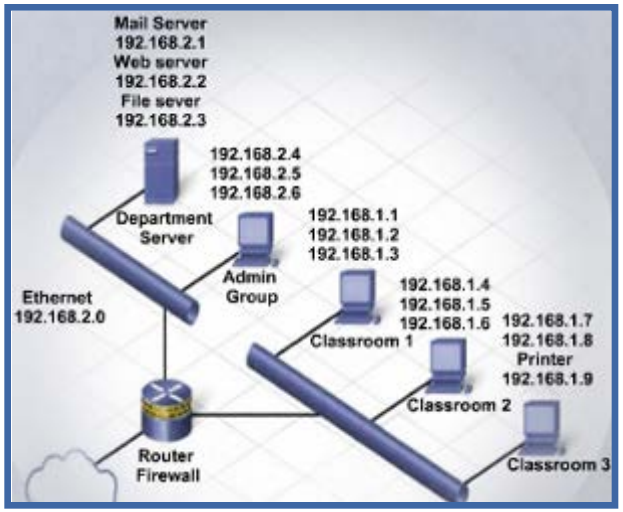
- A glass or plastic strand that transmits information using light and is made up of one or more optical fibers enclosed together in a sheath or jacket.
- Not affected by electromagnetic or radio frequency interference.
- Signals are clearer, can go farther, and have greater bandwidth than with copper cable.
- Usually more expensive than copper cabling and the connectors are more costly and harder to assemble.
- Two types of glass fiber-optic cable:

  **Multimode** and **Single-mode**

# Two Types of LAN Topologies




**Physical topology** is the physical layout of the components on the network




**Logical topology** determines how the hosts access the medium to communicate across the network

# LAN Physical Topologies

- A physical topology defines the way in which computers, printers, and other devices are connected to a network.
- **Bus**
  - Each computer connects to a common cable The ends of the cable have a **terminator** installed to prevent signal reflections and network errors.
  - Only one computer can transmit data at a time or frames will collide and be destroyed.
- **Ring**
  - Hosts are connected in a physical ring or circle.
  - A special frame, a **token**, travels around the ring, stopping at each host to allow data transmission.
  - There are two types of ring topologies:
    - Single-ring and Dual-ring

# LAN Physical Topologies (Continued)

- **Star**
  - Has a central connection point : a hub, switch, or router.
  - Easy to troubleshoot, since each host is connected to the central device with its own wire.
- **Hierarchical or Extended Star Topology**
  - A star network with an additional networking device connected to the main networking device to increase the size of the network.
  - Used for larger networks.
- **Mesh Topology**
  - Connects all devices to each other.
  - Used in WANs that interconnect LANs. The Internet is an example of a mesh topology.

# Logical Topologies

- The two most common types of logical topologies are broadcast and token passing.

  - In a **broadcast** topology, there is no order that the hosts must follow to use the network – it is **first come, first served** for transmitting data on the network.

  - **Token passing** controls network access by passing an electronic token sequentially to each host. When a host receives the token, it can send data on the network. If the host has no data to send, it passes the token to the next host and the process repeats itself.

# LAN Architecture

- Is the overall structure of a computer or communication system and determines the capabilities and limitations of the system. There are three most common LAN architectures:
- **Ethernet**
  - Based on the IEEE 802.3 standard, which specifies that a network use the Carrier Sense Multiple Access with the Collision Detection (CSMA/CD) access control method.
- **Token Ring**
  - Based on the token-passing access control method.
  - The Token Ring topology is referred to as a star-wired ring because the outer appearance of the network design is a star.
- **Fiber Distributed Data Interface (FDDI)**
  - A type of Token Ring network that runs on fiber-optic cable. It combines the high-speed performance and the token-passing advantage.
  - Normally, traffic flows only on the primary ring and uses a secondary ring is a backup.

# Standards Organizations

| | Name | Type | Standards | Established |
|---|---|---|---|---|
| ITU-T | ITU Telecommunication Standardization Sector (formerly CCITT) | one of the three Sectors of the International Telecommunication Union | Standards covering all fields of telecommunications | Became ITU-T in 1992 |
| IEEE | Institute of Electrical and Electronics Engineers | A non-profit, technical professional association | Standards for the computer and electronics industry | 1884 |
| ISO | International Organization for Standardization | A network of the national standards institutes of 157 countries | Promote the development of international standards agreements | 1947 |
| IAB | Internet Architecture Board | A committee; an advisory body | Oversees the technical and engineering development of the Internet | 1979; first named ICCB |
| IEC | International Electrotechnical Commission | Global organization | Standards for all electrical, electronic, and related technologies | 1906 |
| ANSI | American National Standards Institute | Private, non-profit organization | Seeks to establish consensus among groups | 1918 |
| TIA/EIA | Telecommunications Industry Association / Electronic Industries Alliance | Trade associations | Standards for voice and data wiring for LANs | After the deregulation of the U.S. telephone industry in 1984 |

# Ethernet Standards

- Ethernet protocols describe the rules that control how communication occurs on an Ethernet network.
- **IEEE 802.3** Ethernet standard specifies that a network implement the CSMA/CD access control method.
- In **CSMA/CD** all end stations "listen" to the network wire for clearance to send data. When the end station detects that no other host is transmitting, the end station will attempt to send data. Unfortunately collisions might occur.

# Ethernet Technologies

- **10BASE-T**
  - An Ethernet technology that uses a star topology.
  - The ten (10) represents a speed of 10 Mbps, the BASE represents baseband transmission and the T represents twisted-pair cabling.
- **100BASE-TX "FastEthernet"**
  - Has a theoretical bandwidth of 100 Mbps.
  - The "X" indicates different types of copper and fiber-optic can be used.
- **1000BASE-TX "Gigabit Ethernet"**
  - 1 Gbps is ten times faster than Fast Ethernet and 100 times faster than Ethernet.
  - Increased speed makes it possible to implement bandwidth-intensive applications, such as live video.

# Wireless Ethernet Standards

- **IEEE 802.11** is the standard that specifies connectivity for wireless networks.
- **Wi-Fi** (wireless fidelity), refers to the 802.11 family
  - **802.11** (the original specification)
  - **802.11b**
  - **802.11a**
  - **802.11g**
  - **802.11n**
- These protocols specify the frequencies, speeds, and other capabilities of the different Wi-Fi standards.

# Wireless Ethernet Standards

| | Bandwidth | Frequency | Range | Interoperability |
|---|---|---|---|---|
| **802.11a** | Up to 54 Mbps | 5 GHz band | 100 feet (30 meters) | Not interoperable with 802.11b, 802.11g, or 802.11n |
| **802.11b** | Up to 11 Mbps | 2.4 GHz band | 100 feet (30 meters) | Interoperable with 802.11g |
| **802.11g** | Up to 54 Mbps | 2.4 GHz band | 100 feet (30 meters) | Interoperable with 802.11b |
| **802.11n (Pre-standard)** | Up to 540 Mbps | 2.4 GHz band | 164 feet (50 meters) | Interoperable with 802.11b and 802.11g |
| **802.15.1 Bluetooth** | Up to 2 Mbps | 2.4 GHz band or 5 GHz band | 30 feet (10 meters) | Not interoperable with any other 802.11 |

# OSI and TCP/IP Data Models

- Architectural model
  - Separates functions of protocols into manageable layers
  - Each layer performs a specific function in network communication
- TCP/IP model
  - A four-layer model that explains the TCP/IP suite of protocols
  - TCP/IP is the dominant standard for transporting data across networks
- Open Systems Interconnect (OSI) model
  - Standards defining how devices communicate on a network
  - Ensures interoperability between network devices

# The TCP/IP Reference Model

- Frame of reference used to develop the Internet's protocols.
- Consists of layers that perform functions necessary to prepare data for transmission over a network.

| | Description | Protocols |
|---|---|---|
| **Application** | **Provides network services to user applications** | **HTTP, HTML, Telnet, FTP, SMTP, DNS** |
| **Transport** | **Provides end-to-end management of data and divides data into segments** | **TCP, UDP** |
| **Internet** | **Provides connectivity between hosts in the network** | **IP, ICMP, RIP, ARP** |
| **Network Access** | **Describes the standards that hosts use to access the physical media** | |

# The OSI Model

- The OSI model is an industry standard framework that is used to divide network communications into seven layers.
- Although other models exist, most network vendors today build their products using this framework.
- A **protocol stack** is a system that implements protocol behavior using a series of layers.

  Protocol stacks can be implemented either in hardware or software, or in a combination of both.

  Typically, only the lower layers are implemented in hardware, and the higher layers are implemented in software.

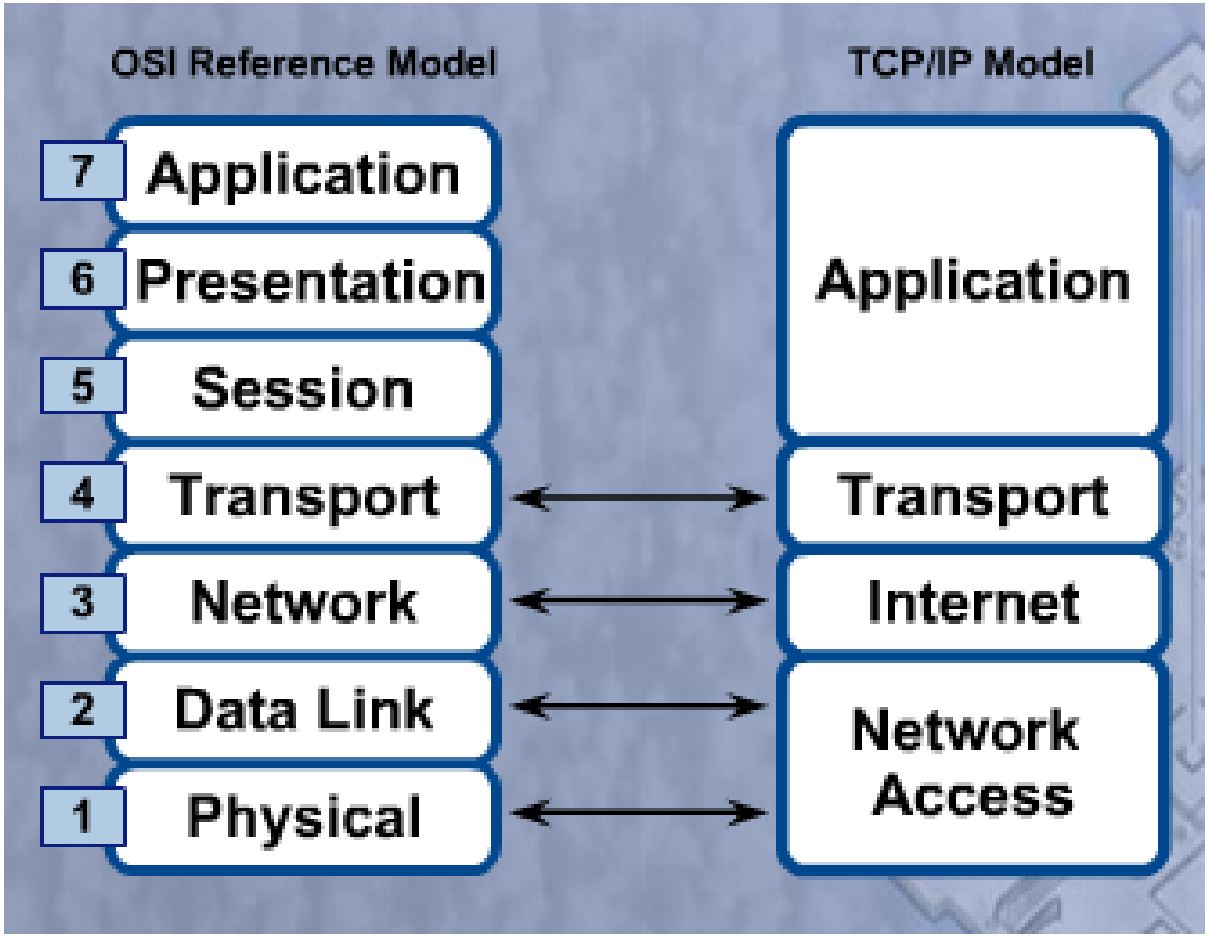
# The OSI Model

| | Layer | Description |
|---|---|---|
| **Application** | **7** | **Responsible for network services to applications** |
| **Presentation** | **6** | **Transforms data formats to provide a standard interface for the Application layer** |
| **Session** | **5** | **Establishes, manages and terminates the connections between the local and remote application** |
| **Transport** | **4** | **Provides reliable transport and flow control across a network** |
| **Network** | **3** | **Responsible for logical addressing and the domain of routing** |
| **Data Link** | **2** | **Provides physical addressing and media access procedures** |
| **Physical** | **1** | **Defines all the electrical and physical specifications for devices** |

Remember the OSI layers with this mnemonic:

"Please Do Not Throw Sausage Pizza Away"

# Compare OSI and TCP/IP Models



# Install or Update a NIC Driver

- Manufacturers publish new driver software for NICs.
  - May enhance the functionality of the NIC
  - May be needed for operating system compatibility
- When installing a new driver manually, there are a couple of things to keep in mind. For instance you will need to disable the virus protection and close all applications.
- Alternatively, you can click the Update Driver button in the toolbar of the Device Manager.
- If a new NIC driver does not perform as expected after it has been installed, the driver can be uninstalled, or rolled back, to the previous driver.

# Attach Computer to Existing Network

- After connecting the network cable, activity should be verified by looking at the LEDs.
- Every NIC must be configured with the following information:
  - Protocols
  - IP address
  - MAC address
- Networks connection should be tested. Commands are available to run this type of tests and to obtain information:
  - **ping**
  - **ipconfig**
  - **telnet**

# Modem Installation

- A **modem** is an electronic device that transfers data between one computer and another using analog signals over a telephone line.
  - A transmitting modem converts digital data to analog signals, called **mo**dulation.
  - The receiving modem reconverts the analog signals back to digital data, called **dem**odulation.
- An **internal** modem plugs into an expansion slot on the motherboard and a software driver is installed.
- **External** modems connect to a computer through the serial and USB ports and also require a software driver.

# Dial-up Networking (DUN)

- When computers use the public telephone system to communicate, it is called **dial-up networking** (**DUN**).
- Modems communicate with each other using audio tone signals. DUN creates a Point-to-Point Protocol (PPP) connection between two computers over a phone line.
- After the line connection has been established, a "handshaking sequence" takes place between the two modems and the computers.
- The digital signals from the computers must be converted to an analog signal to travel across telephone lines. They are converted back to the digital form, 1s and 0s, by the receiving modem so that the receiving computer can process the data.

# Other types of Connectivity

- Phone, cable, satellite, and private telecommunications companies provide Internet connections.
- In the 1990s, low-speed modems used the **plain old telephone system (POTS)** to send and receive data.
- Today, many businesses and home users have switched to high-speed Internet connections, which allows for transmission of data, voice and video.

# Integrated Services Digital Network (ISDN)

- A standard for sending voice, video, and data over telephone wires.
- Provides higher-quality voice and higher-speed data transfer than traditional analog telephone service.
- Three services offered by ISDN digital connections: Basic Rate Interface (BRI), Primary Rate Interface (PRI), and Broadband ISDN (BISDN).
- ISDN uses two different types of communications channels:

  "B" channel is used to carry the information - data, voice, or video.

  "D" channel is usually used for controlling and signaling, but can be used for data.

# ISDN Types

| Type | Description |
|---|---|
| **BRI** | ISDN Basic Rate Interface offers a dedicated 128 Kbps connection using two 64 Kbps B channels. ISDN BRI also uses on 16 Kbps D channel for call setup, control, and teardown. |
| **PRI** | ISDN Primary Rate Interface offers up to 1.544 Mbps over 23 B channels in North America and Japan or 2.048 Mbps over 30 B channels in Europe and Australia. ISDN PRI also uses one D channel for call maintenance. |
| **BISDN** | Broadband ISDN manages different types of service all at the same time. BISDN is mostly used only in network backbones. |

# Digital Subscriber Line (DSL)

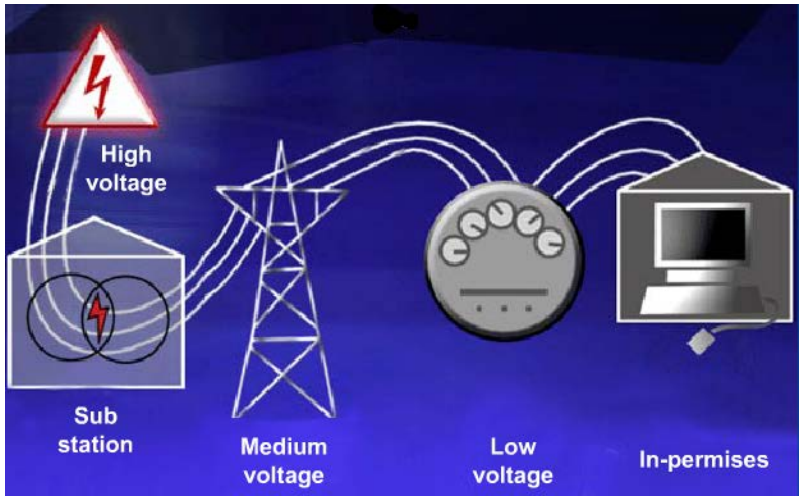
- An "always-on" technology; there is no need to dial up each time to connect to the Internet.
- Uses the existing copper telephone lines to provide high-speed data communication between end users and telephone companies.
- Asymmetric DSL (ADSL) is currently the most commonly used DSL technology.
  - Has a fast downstream speed, typically 1.5 Mbps.
  - Upload rate of ADSL is slower.
  - Not the best solution for hosting a web server or FTP server.

# DSL Types

| Type | Description |
|---|---|
| **ADSL** | Asymmetric DSL is most common. Downstream speed from 384 Kbps to 6 Mbps. Upstream speeds lower than downstream speeds. |
| **HDSL** | High Data Rate DSL provides equal bandwidth in both directions. |
| **SDSL** | Symmetric DSL provides the same speed, up to 3 Mbps, for uploads and downloads. |
| **VDSL** | Very High Data Rate DSL is capable of bandwidths between 13 and 52 Mbps downstream, and 16 Mbps upstream. |
| **IDSL** | ISDN DSL is DSL over ISDN lines. Uses ordinary phone lines. Requires ISDN adapters. |

# Power Line Communication (PLC)

- Uses power distribution wires (local electric grid) to send and receive data.
- May be available in areas without any other service and is faster than an analog modem.
- May cost less than other high-speed connections and in time it is expected to be more common.
- Can be used in a home or office environment through an electrical outlet and can control lighting and appliances.



# Broadband Connectivity

- **Broadband** is a technique used to transmit and receive multiple signals using multiple frequencies over one cable.
- Broadband uses a wide range of frequencies that may be further divided into **channels**.
- Some common broadband network connections include:
  - Cable
  - Digital Subscriber Line (DSL)
  - Integrated Services Digital Network (ISDN)
  - Satellite

# Bluetooth Technology

- A Bluetooth device can connect up to seven other Bluetooth devices to create a Wireless Personal Area Network (WPAN).
- Bluetooth devices are divided into three classifications:
  - Class 1: has a range of approximately 100 m (330 ft)
  - Class 2: has a range of approximately 10 m (33 ft)
  - Class 3: has a range of approximately 1 m (3 ft)
- Bluetooth devices operate in the 2.4 to 2.485 GHz radio frequency range, which is in the Industrial, Scientific, and Medical (ISM) band.

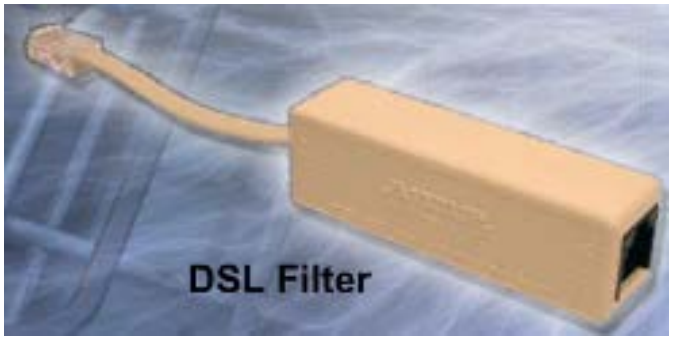
# Cellular Technology

- Cellular technology enables the transfer of voice, video, and data. With a cellular WAN adapter installed, a laptop user can access the Internet over the cellular network.
- Although slower than DSL and cable connections, cellular WANs are still fast enough to be classified as a high-speed connection.
- Different Generations has been released:
  - G1
  - G2
  - G2.5
  - G3
  - G3.5

# Cable Modem

- A **cable modem** connects your computer to the cable company using the same coaxial cable that connects to your cable television.
  - You can connect the computer directly into the cable modem.
  - You can connect a router, switch, hub, or multipurpose network device so multiple computers can share the Internet connection.

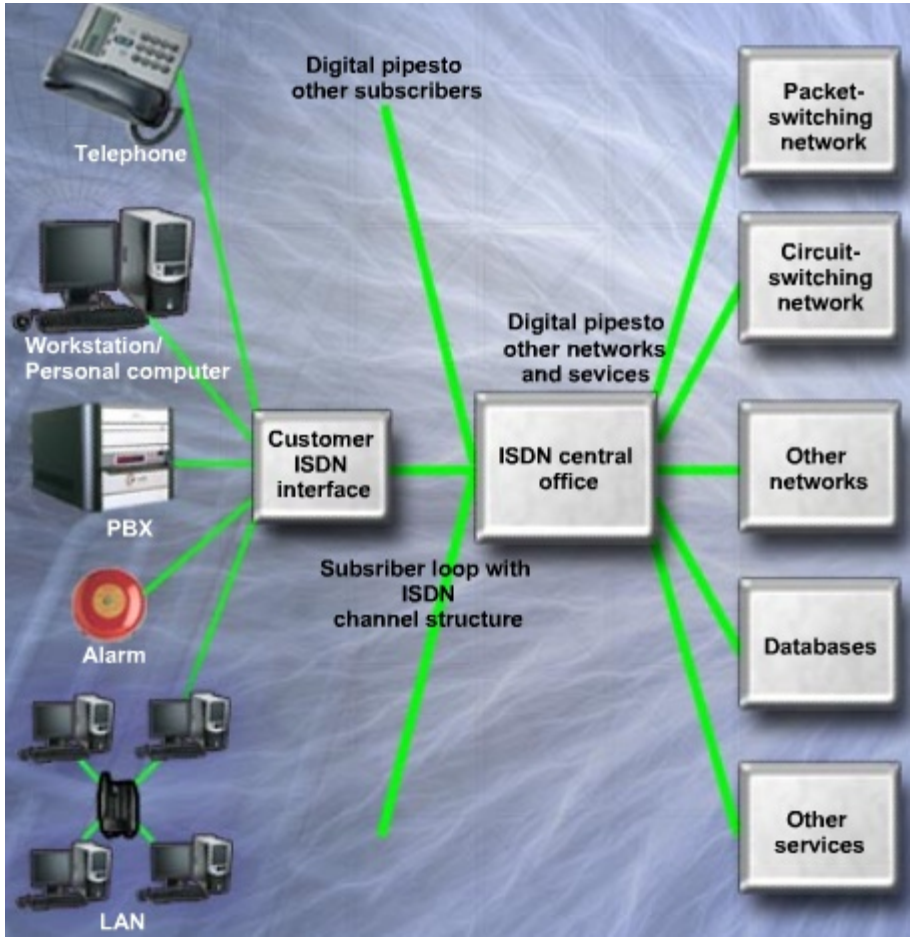
# DSL Modem and Filter




- Voice and data signals are carried on different frequencies on the copper telephone wires.
- A filter is used to prevent DSL signals from interfering with phone signals. Plug the filter into a phone jack and plug the phone into the filter.
- The DSL modem does not need a filter. A DSL modem can connect directly to your computer, or it can be connected to a networking device to share the Internet connection between multiple computers.

# A Typical ISDN Connection

- ISDN uses multiple channels and can carry voice, video, and data.
- ISDN is considered a type of broadband.



# Broadband Satellite

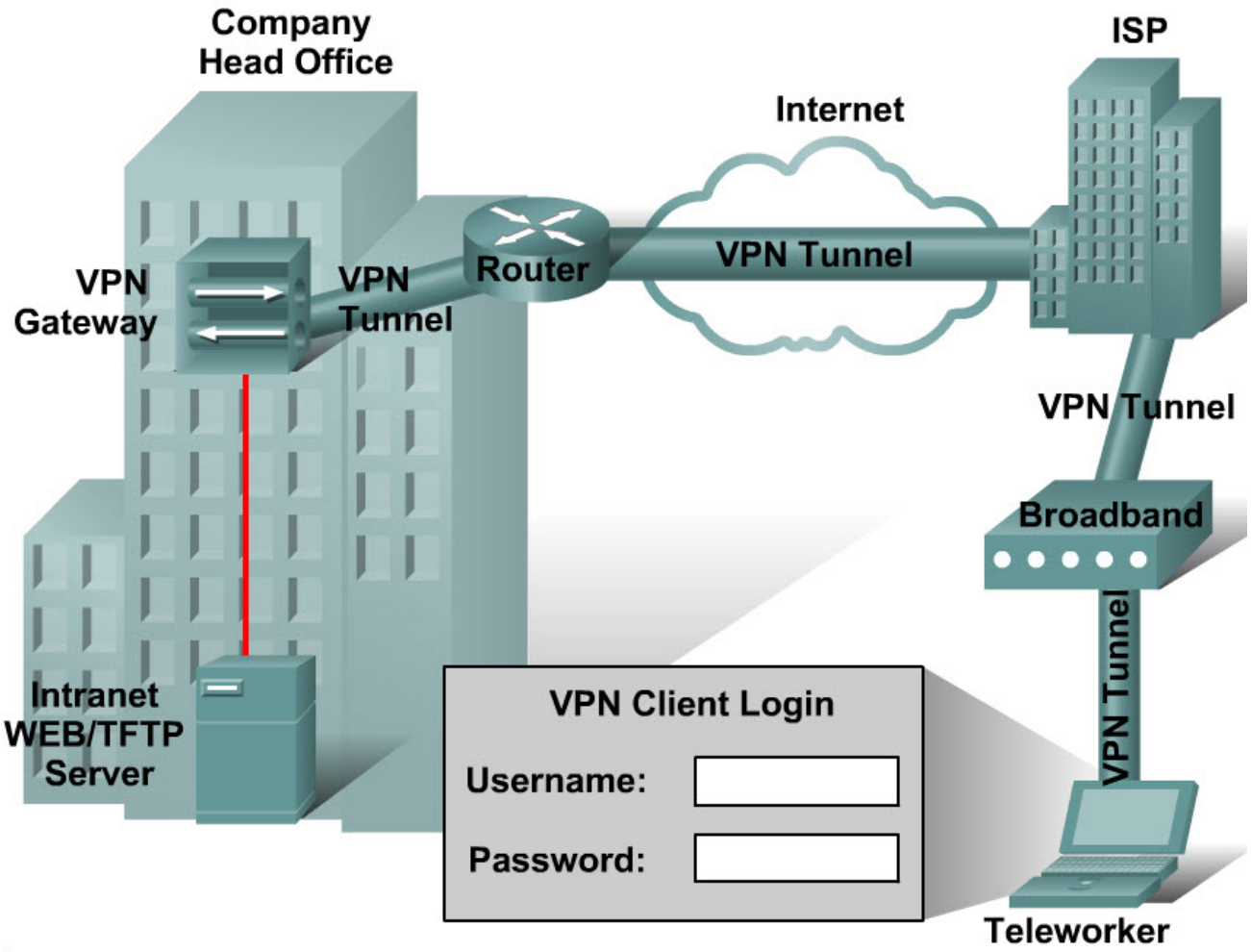
- Uses a satellite dish for two-way communication.
- Download speeds are typically up to 500 Kbps, while uploads are closer to 56 Kbps.
- People in rural areas often use satellite broadband because it is a faster connection than dial-up and no other broadband connection may be available.

# Voice over IP (VoIP)

- Is a method used to carry telephone calls over data networks and the Internet.
- Converts the analog signals of voices into digital information that is transported in IP packets.
- Can also use an existing IP network to provide access to the public switched telephone network (PSTN).
- Depends on a reliable Internet connection. When a service interruption occurs the user cannot make phone calls.

# Virtual Private Network (VPN)

- A Virtual Private Network (VPN) is a private network that uses a public network, like the Internet, to connect remote sites or users together



# Preventive Maintenance for Networks

- Common preventive maintenance techniques should continually be performed for a network to operate properly.
  - Keep network rooms clean and change air filters often.
  - Checking the various components of a network for wear.
  - Check the condition of network cables because they are often moved, unplugged, and kicked.
  - Label the cables to save troubleshooting time later. Refer to wiring diagrams and always follow your company's cable labeling guidelines.
  - AC power adapters should be checked regularly.
  - The **uninterruptible power supply (UPS)** should be tested to ensure that you have power in the case of an outage.

# Troubleshooting Printers and Scanners

**Step 1** Identify the problem

**Step 2** Establish a theory of probable causes

**Step 3** Determine an exact cause

**Step 4** Implement a solution

**Step 5** Verify solution and full system functionality

**Step 6** Document findings

# Step 1- Identify the Problem

- System Information
  - Manufacturer, model, OS, network environment, connection type
- Open-ended questions
  - What problems are you experiencing with your computer?
  - What software has been changed recently on your computer?
  - What were you doing when the problem was identified?
  - What error messages have you received on your computer?
  - What type of network connection is the computer using?
- Closed-ended questions
  - Has anyone else used your computer recently?
  - Can you see any shared files or printers?
  - Have you changed your password recently?
  - Can you access the Internet?
  - Are you currently logged into the network?

# Step 2 - Establish a Theory of Probable Causes

- Problem may be simpler than the customer thinks.
- Create a list of the most common reasons why the error would occur.
  - Loose cable connections
  - Improperly installed NIC
  - ISP is down
  - Low wireless signal strength
  - Invalid IP address

# Step 3 - Determine the Exact Cause

- Testing your theories of probable causes one at a time, starting with the quickest and easiest.
  - Check that all cables are connected to the proper locations.
  - Unseat and then reconnect cables and connectors.
  - Reboot the computer or network device.
  - Login as a different user.
  - Repair or re-enable the network connection.
  - Contact the network administrator.
  - Ping your default gateway.
  - Access a remote web pages.
- Exact cause of the problem has not been determined after you have tested all your theories, establish a new theory of probable causes and test it.

# Step 4 - Implement a Solution

- Sometimes quick procedures can determine the exact cause of the problem or even correct the problem.
- If a quick procedure does not correct the problem, you might need to research the problem further to establish the exact cause.
- Divide larger problems into smaller problems that can be analyzed and solved individually.

# Step 5 - Verify Solution and System Functionality

- Verifying full system functionality and implementing any preventive measures if needed.
  - **Ping** is used to check network connectivity.
  - **Nslookup** is used to query Internet domain name server.
  - **Tracert** is used to determine the route taken by packets when they travel across the network.
  - **Net View** is used to display a list of computers in a workgroup.
- Have the customer verify the solution and system functionality.

# 6. Document Findings

- Discuss the solution with the customer
- Have the customer confirm that the problem has been solved
- Document the process
  - Problem description
  - Solution
  - Components used
  - Amount of time spent in solving the problem

# Common Problems and Solutions

- Printer and scanner problems can be attributed to hardware, software, networks, or some combination of the three. You will resolve some types of printer and scanner problems more often than others.

# Chapter 8 Summary

- A computer network is composed of two or more computers that share data and resources.
- A Local Area Network (LAN) refers to a group of interconnected computers that are under the same administrative control.
- A Wide Area Network (WAN) is a network that connects LANs in geographically separated locations.
- In a peer-to-peer network, devices are connected directly to each other. A peer-to-peer network is easy to install, and no additional equipment or dedicated administrator is required. Users control their own resources, and a network works best with a small number of computers. A client/server network uses a dedicated system that functions as the server. The server responds to requests made by users or clients connected to the network.

# Chapter 8 Summary (Continued)

- A LAN uses a direct connection from one computer to another. It is suitable for a small area, such as in a home, building, or school. A WAN uses point-to-point or point-to-multipoint, serial communications lines to communicate over greater distances. A WLAN uses wireless technology to connect devices together.
- The network topology defines the way in which computers, printers, and other devices are connected. Physical topology describes the layout of the wire and devices, as well as the paths used by data transmissions. Logical topology is the path that signals travel from one point to another. Topologies include bus, star, ring, and mesh.
- Networking devices are used to connect computers and peripheral devices so that they can communicate. These include hubs, bridges, switches, routers, and multipurpose devices. The type of device implemented depends on the type of network.

# Chapter 8 Summary (Continued)

- Networking media can be defined as the means by which signals, or data, are sent from one computer to another. Signals can be transmitted either by cable or wireless means. The media types discussed were coaxial, twisted-pair, fiber-optic cabling, and radio frequencies.
- Ethernet architecture is now the most popular type of LAN architecture. Architecture refers to the overall structure of a computer or communications system. It determines the capabilities and limitations of the system. The Ethernet architecture is based on the IEEE 802.3 standard. The IEEE 802.3 standard specifies that a network implement the CSMA/CD access control method.
- The OSI reference model is an industry standard framework that is used to divide the functions of networking into seven distinct layers. These layers include Application, Presentation, Session, Transport, Network, Data Link, and Physical. It is important to understand the purpose of each layer.

# Chapter 8 Summary (Continued)

- The TCP/IP suite of protocols has become the dominant standard for the Internet. TCP/IP represents a set of public standards that specify how packets of information are exchanged between computers over one or more networks.
- A NIC is a device that plugs into a motherboard and provides ports for the network cable connections. It is the computer interface with the LAN.
- A modem is an electronic device that is used for computer communications through telephone lines. It allows data transfer between one computer and another. The modem converts byte-oriented data to serial bit streams. All modems require software to control the communication session. The set of commands that most modem software uses is known as the Hayes-compatible command set.

# Chapter 8 Summary (Continued)

- The three transmission methods to sending signals over data channels are simplex, half-duplex, and full-duplex. Full-duplex networking technology increases performance because data can be sent and received at the same time. DSL, two-way cable modem, and other broadband technologies operate in full-duplex mode.
- Network devices and media, such as computer components, must be maintained. It is important to clean equipment regularly and use a proactive approach to prevent problems. Repair or replace broken equipment to prevent downtime.
- When troubleshooting network problems, listen to what your customer tells you so that you can formulate open-ended and closed-ended questions that will help you determine where to begin fixing the problem. Verify obvious issues and try quick solutions before escalating the troubleshooting process.