

Chapter 10

Overview

By definition, a computer network has two or more devices linked together for the purpose of sharing information and resources. This module provides the student with an overview of how networks work and how they share services. The types of networks that are detailed in this module include peer-to-peer, client/server, local-area network (LAN), and wide-area network (WAN). Additionally, the difference between a circuit-switched and a packet-switched network is explained as well as the topology or the way the network is setup. You will learn how to add the network interface card, the physical components of a network, and the important utilities that are used in troubleshooting.

LAN Architectures

Architecture refers to the overall structure of a computer or communication system. It determines the capabilities and limitations of the system.

The Ethernet architecture is now the most popular type of LAN architecture.

Ethernet

The Ethernet architecture is based on the IEEE 802.3 standard. The IEEE 802.3 standard specifies that a network implements the Carrier Sense Multiple Access with the Collision Detection (CSMA/CD) access control method. CSMA/CD uses baseband transmission over coaxial or twisted-pair cable that is laid out in a bus topology, either a linear or star bus. Standard transfer rates are 10 Mbps or 100 Mbps, but new standards provide for Gigabit Ethernet, which is capable of attaining speeds up to 1 Gbps over fiber-optic cable or other high-speed media.

Token Ring

IBM originally developed Token Ring as reliable network architecture based on the token-passing access control method. It is often integrated with IBM mainframe systems such as the AS400. It was intended to be used with PCs, minicomputers, and mainframes. It works well with Systems Network Architecture (SNA), which is the IBM architecture used for connecting to mainframe networks.

Token Ring is so named because of its logical topology and its media access control method of token passing. The transfer rate for Token Ring can be either 4 Mbps or 16 Mbps.

The Monitor of the Ring

In a Token Ring network, the first computer that comes online becomes the “monitor” and must keep track of how many times each frame circles the ring. It has the responsibility of ensuring that only one token is out on the network at a time.

Data Transfer

A Token Ring network uses a token, that is, a special signal, to control access to the cable. A token is initially generated when the first computer on the network comes online. When a computer wants to transmit, it waits for and then takes control of the token when it comes its way. The token can travel in either direction around the ring, but only in one direction at a time. The hardware configuration determines the direction of travel.

Fibre Distributed Data Interface (FDDI)

FDDI is a type of Token Ring network. Its implementation and topology differ from the IBM Token Ring LAN architecture

As its name implies, FDDI runs on fiber-optic cable. FDDI combines high-speed performance with the advantages of the token-passing ring topology. FDDI runs at 100 Mbps, and its topology is a dual ring. The outer ring is called the primary ring and the inner ring is called the secondary ring.

Normally, traffic flows only on the primary ring. If it fails, then the data automatically flows onto the secondary ring in the opposite direction. When this occurs, the network is said to be in a wrapped state. This provides fault tolerance for the link.

Introduction to PC Networking

A network is a connected system of objects or people. The most common example of a network is the telephone system, which is widely known as the Public Switched Telephone Network (PSTN). The PSTN allows people in virtually every corner of the world to communicate with anyone who has access to a telephone.

A computer network works similar to the PSTN. It allows users to communicate with other users on the same network by transmitting data on the cables used to connect them. A computer network, as illustrated in Figure , is defined as having two or more devices such as workstations, printers, or servers. These devices are linked together for the purpose of sharing information, resources, or both. Network links are made using copper cables, fiber-optic cables, or wireless connections. Wireless connections use radio signals, infrared technology (laser), or satellite transmissions. The information and resources shared on a network can include data files, application programs, printers, modems, or other hardware devices.

File, print, and application services

The need to share information is an important part of the development of computer networks. In networks, different computers take on specialized roles or functions. Once they are connected, one or more computers in the network can function as network file servers. The server is a repository for files that can be accessed and shared across the network by many users. This avoids duplication, conserves resources, and allows for the management and control of key information. Network administrators can grant or restrict access to files. They also regularly copy the files to back up systems in case of problems or failures.

All network operating systems offer file and print services. Sharing information, collaborating on projects, and providing access to input and output devices are common services of computer networks. Network users can share more than information and special devices. They can also share applications, such as word processing programs, that are installed on the server. Users can run the shared applications from a server without using space on their local hard disks for the program files.

Software licensing agreements may require the purchase of additional licenses for each workstation that uses a network application. This is necessary even though only one copy is actually installed and

Simplex, half-duplex, and full-duplex transmission

A data channel, over which a signal is sent, can operate in one of three ways: simplex, half-duplex, or full-duplex. Full-duplex is often just called duplex. The distinction is in the way that the signal can travel.

Simplex Transmission — is a single one-way base band transmission. Simplex transmission, as the name implies, is simple. It is also called unidirectional because the signal travels in only one direction. An example of simplex transmission is the signal sent from the TV station to the home television.

Half-duplex transmission — is an improvement over simplex because the traffic can travel in both directions. Unfortunately, the road is not wide enough to accommodate bidirectional signals simultaneously. This means that only one side can transmit at a time. Two-way radios, such as police or emergency communications mobile radios, work with half-duplex transmissions. Modems are half-duplex devices. They can send and receive, but not at the same time.

Full-duplex transmission — operates like a two-way, two-lane street. Traffic can travel in both directions at the same time. A land-based telephone conversation is an example of full-duplex communication. Both parties can talk at the same time, and the person talking on the other end can still be heard by the other party while they are talking. Although both parties talking at the same time might be difficult to understand what is being said.

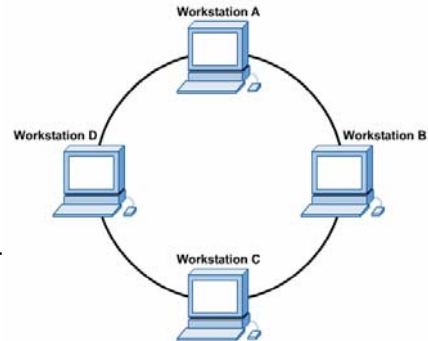
Full-duplex networking technology increases performance because data can be sent and received at the same time. Digital subscriber line (DSL), two-way cable modem, and other broadband technologies operate in full-duplex mode. With DSL, for example, users can download data to their computer at the same time they are sending a voice message over the line.

Types of Networks

By using LAN and WAN technologies, many computers are interconnected to provide services to their users. In providing services, networked computers take on different roles or functions in relation to each other.

Peer-to-peer networks

In a peer-to-peer network, the networked computers act as equal partners, or peers, to each other. As peers, each computer can take on the client function or the server function. At one time Workstation A, for example, may make a request for a file from Workstation B, which responds by serving the file to Workstation A. Workstation A functions as client, while Workstation B functions as the server. At a later time, Workstation A and B can reverse roles. Workstation B could be the client, making a request of Workstation A, and Workstation A, as server, responds to the request of Workstation B. Workstations A and B stand in a reciprocal, or peer, relationship to each other.

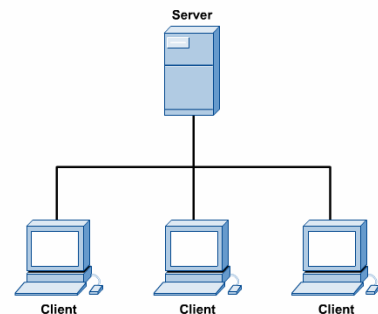


In a peer-to-peer network, individual users control their own resources. They may decide to share certain files with other users and may require passwords before they allow others to access their resources. Since individual users make these decisions, there is no central point of control or administration in the network.

Client/server networks

In a client/server network arrangement, network services are located in a dedicated computer whose only function is to respond to the requests of clients. The server contains the file, print, application, security, and other services in a central computer that is continuously available to respond to client requests. Most network operating systems adopt the form of client/server relationships. Typically, desktop computers function as clients and one or more computers with additional processing power, memory, and specialized software function as servers.

Servers are designed to handle requests from many clients simultaneously. Before a client can access the server resources, the client must identify itself and be authorized to use the resource. An account name and password is assigned to each user for this purpose. A specialized authentication server acts as an entry point, guarding access to the network, and verifies this account information. By centralizing user accounts,



Local-area networks (LANs)

A LAN can connect many computers in a relatively small geographical area. These areas can be in a home, an office, or a campus. It allows users to access high bandwidth media like the Internet and allows users to share devices such as printers.

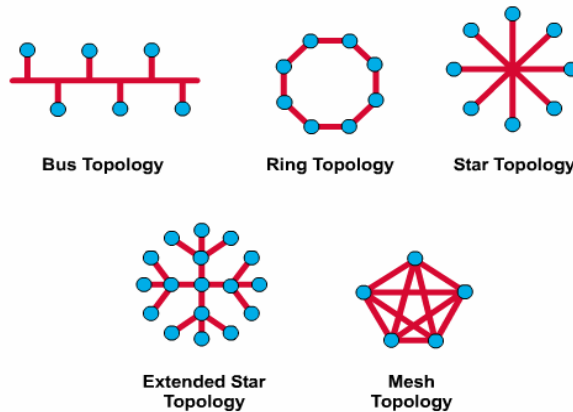
A LAN connects each computer to each of the others by using a separate communications channel. A direct connection from one computer to another is called a point-to-point link. If the network were designed using point-to-point links. For each new computer, the network would need a new separate connection to each of the other computers. This approach would be very costly and difficult to manage.

In the late 1960s and early 1970s, network engineers designed a new form of network. This network enabled many computers in a small area to share a single communications channel by taking turns using it.

The general shape or layout of a LAN is called its topology. Topology defines the structure of the network. This includes the physical topology, which is the actual layout of the wire or media. It also includes the logical topology, which is how the hosts access the media.

Network topologies

The network topology defines the way in which computers, printers, and other devices are connected. A network topology describes the layout of the wire and devices as well as the paths used by data transmissions. The topology greatly influences how the network functions.



Bus Topology — Commonly referred to as a linear bus, all the devices on a bus topology are connected by one single cable. Figure illustrates the bus topology. This cable proceeds from one computer to the next like a bus line going through a city. The main cable segment must end with a terminator that absorbs the signal when it reaches the end of the line or wire. If there is no terminator, the electrical signal representing the data bounces back at the end of the wire, causing errors in the network. Only one packet of data can be transmitted at a time. If more than one packet is transmitted, they collide and have to be resent. A bus topology that has many hosts can be very slow due to these collisions. This topology is rarely used and would only be suitable for a home office or small business with a few hosts.

Star Topology — is the most commonly used architecture in Ethernet LANs. When installed, the star topology resembles spokes in a bicycle wheel. It is made up of a central connection point that is a device such as a hub, switch, or router. All of the cabling segments actually meet at this central connection point. Each host in the network is connected to the central device with its own cable.

A star topology costs more to implement than the bus topology. This is because more cable is used in a star topology. Also, a central device is needed such as a hub, switch, or router. However, the advantages of a star topology are worth the additional costs. Since each host is connected to the central device with its own wire, if there is a problem with that cable, only that host is affected. The rest of the network is operational. This benefit is extremely important. It is the reason why virtually every newly designed network has this topology.

Extended Star Topology — When a star network is expanded to include an additional networking device that is connected to the main networking device, it is called an extended star topology. Larger networks, like those of corporations or schools, use the extended star topology. This topology can be used with network devices that filter frames or packets, like bridges, switches, and routers. This topology, when used with these devices, significantly reduces the traffic on the wires by sending packets only to the wires of the destination host.

Ring Topology — The ring topology is another important topology in LAN connectivity. It is important to know the advantages and disadvantages of choosing a ring topology. As the name implies, hosts are connected in the form of a ring or circle. Unlike the bus topology, it has no beginning or end that needs to be terminated. Data is transmitted in a way that is unlike the bus or the star topology. A frame travels around the ring, stopping at each node. If a node wants to transmit data, it adds the data as well as the destination address to the frame.

Mesh topology — The mesh topology connects all devices, nodes, to each other for redundancy and fault tolerance as shown in Figure . It is used in WANs to interconnect LANs and for mission critical networks like those used by governments. Implementing the mesh topology is expensive and difficult.

Hybrid Topology — The hybrid topology combines more than one type of topology. When a bus line joins two hubs of different topologies, this configuration is called a star bus. Businesses or schools that have several buildings, known as campuses, sometimes use this topology. The bus line is used to transfer the data between the star topologies.

Wide-area networks (WANs)

For economic and technical reasons, LANs are not suitable for communications over long distances. On a LAN, the computers must coordinate their use of the network and this coordination takes time. Long distances have greater delays in communication. The computers would take more time coordinating the use of the shared medium and less time sending data messages. In addition, the costs of providing high-speed media over long distances are much greater than in the case of LANs. For these reasons, WAN technologies differ from LANs. A WAN, as the name implies, is designed to work over a larger area than a LAN.

A WAN uses point-to-point or point-to-multipoint, serial communications lines. Point-to-point lines connect only two locations, one on each side of the line. Point-to-multipoint lines connect one location on one side of the line to multiple locations on the other side. They are called serial lines because the bits of information are transmitted one after another in a series.

The following are some of the more common WAN technologies:

- Modems
- Integrated Services Digital Network (ISDN)
- DSL
- Frame Relay
- Asynchronous Transfer Mode (ATM)
- The T (US) and E (Europe) Carrier series (T1, E1, T3, E3)
- Synchronous Optical Network (SONET)
-

Typically, individuals and companies do not build their own WAN connections. Government regulations only allow utility companies to install lines on public property. Therefore, wide area connections make use of the communications facilities put in place by utility companies, called common carriers, such as the telephone company.

Circuit-Switched versus Packet-Switched Networks

The public telephone system, sometimes referred to as plain old telephone service (POTS), is a circuit-switched communications network. When a telephone call is placed in this type of network, only one physical path is used between the telephones for the duration of that call. This pathway, called a circuit, is maintained for the exclusive use of the call, until the connection is ended and the telephone is hung up. Figure illustrates this concept with one route on the map. It is the only way to get from one place to another.

If the same number were called tomorrow from the same location as the call from today, the path would probably not be the same. The circuit is created by a series of switches that use currently available network paths to set up the call end-to-end. This explains why callers can get a clear connection one day, and noise and static on another. This demonstrates that a circuit-switched connection is end-to-end or point-to-point.

This is different from a packet-switched network, where each individual packet of data can take a different route. Also, with a packet-switched network, no dedicated pathway or circuit is established. The different routes that are shown on the map in Figure illustrate this concept. Using a packet-switched network to transfer data enables each individual packet to take a different route when going from one computer to another. Although it all arrives at the same destination, it does not all travel the same path to get there. Internet traffic uses packet-switching technology.

The difference between circuit and packet-switching can be compared to the different ways in which a large group of people travel to the same destination. For example, circuit-switching is similar to loading the entire group on a bus, a train, or an airplane. The route is plotted out, and the whole group travels over that same route.

Packet-switching is comparable to people traveling in their own automobiles. The group is broken down into individual components just as the data communication is broken into packets. Some travelers can take interstate highways, and others can use back roads. Some can drive straight through, and others can take a more roundabout path. Eventually, they all end up at the same destination. The group is put back together, just as packets are reassembled at the endpoint of the communication.

Adding a Network Interface Card (NIC)

A network interface card (NIC) shown in Figure is a device that plugs into a motherboard and provides ports for the network cable connections. It is the computer interface with the LAN. The NIC communicates with the network through serial connections and communicates with the computer through parallel connections.

Setting the IP Address

In a Transmission Control Protocol/Internet Protocol (TCP/IP) LAN, PCs use IP addresses to identify each other. These addresses allow computers that are attached to the network to locate each other. An IP address is a 32-bit binary number. This binary number is divided into four groups of eight bits known as octets. A decimal number in the range of 0 to 255 represent each octet. The octets are separated by decimal points. The combination 190.100.5.54 is an example of an IP address. This type of address is described as a dotted decimal representation. Each device on the network that has an IP address is known as a host or node.

Subnet Mask

A secondary dotted decimal number, known as the subnet mask, always accompanies an IP address. The dotted decimal number 255.255.0.0 is a subnet mask. The subnet mask is used by network computers to determine whether a particular host IP address is local or remote. A local host is on the same network segment, while a remote host is on another segment.

DHCP Servers

The most common and efficient way for computers on a large network to obtain an IP address is through a Dynamic Host Configuration Protocol (DHCP) server. DHCP is a software utility that runs on a computer and is designed to assign IP addresses to PCs. The computer running the software is known as a DHCP server. DHCP servers hand the IP addresses and TCP/IP configuration information to computers that are configured as DHCP clients. This dynamic process eliminates the need for manual IP address assignments. However, any devices requiring a static, or permanent, IP address must still have their IP address manually assigned.

The use of this system simplifies the administration of a network because the software keeps track of IP addresses. Automatically configuring TCP/IP also reduces the possibility of assigning duplicate IP addresses or invalid IP addresses. For a computer on the network to take advantage of the DHCP server services, it must be able to identify the server on the local network. This is accomplished by choosing to obtain an IP address automatically on the client software through its TCP/IP Properties dialog box. In other cases, an operating system feature called Automatic Private IP Addressing (APIPA) enables a computer to assign itself an address if it is unable to contact a DHCP server.

Default Gateway

A computer located on one network segment trying to talk to another computer across the router, sends the data through a default gateway. The default gateway is the "near side" interface of the router. That is the interface on the router where the network segment or wire of the local computer is attached. For each computer to recognize its default gateway, the corresponding near side router interface IP address has to be entered into the host TCP/IP Properties dialog box. This information is stored on the NIC.

DNS (Domain Name System)

If a LAN is large or is connected to the Internet, it is often challenging to remember the IP addresses of hosts. Most hosts are identified on the Internet by friendly computer names known as domain names. The DNS is used to translate computer names such as cisco.com to their corresponding unique IP address. The DNS software runs on a computer that acts as a network server for handling the address translations. DNS software may be hosted on the network by itself or by an ISP. Address translations are used each time the Internet is accessed. The process of translating names to addresses is known as name resolution. Figure illustrates how the DNS server resolves the post office name of an e-mail address.

The DNS server keeps records that map the computer host names and their corresponding IP addresses. These record types are all combined in the DNS table. When a hostname needs to be translated to its IP address, the client contacts the DNS server. A hierarchy of DNS servers exists on the Internet. Different servers maintain DNS information for their own areas of authority, called zones. A DNS server, when consulted by a computer, may not have an IP mapping for the hostname sought. If this happens, it will pass the query to another DNS server until the information is obtained.

Physical Components of a Network

Networking Media

Networking media can be defined simply as the means by which signals, the data, are sent from one computer to another. This can be done either by cable or wireless means. There is a wide variety of networking media in the marketplace.

Coaxial cable

Coaxial cable is a copper-cored cable surrounded by a heavy shielding as shown in Figure . It is used to connect computers in a network. There are several types of coaxial cable, including thicknet, thinnet, RG-59, and RG-6. RG-59 is the standard for cable TV, while RG-6 is used in video distribution.

Twisted Pair

Twisted-pair is a type of cabling that is used for telephone communications and most modern Ethernet networks. A pair of wires forms a circuit that can transmit data. The pairs are twisted to provide protection against crosstalk, the noise generated by adjacent pairs. Pairs of copper wires that are encased in colour-coded plastic insulation are twisted together. All the twisted-pairs are then protected inside an outer jacket.

Fiber-Optic Cable

Fibre-optic cable is a networking medium capable of conducting modulated light transmissions. To modulate light, is to manipulate it so that it travels in the way that it transmits data. Fibre-optic refers to cabling that has a core of strands of glass or plastic, instead of copper, through which light pulses carry signals.

Wireless

Sometimes the cost of running cables is too high or computers need to be movable without being tethered to cables. When this is the case, wireless is an alternative method of connecting a LAN. Wireless networks use radio frequency (RF), laser, infrared (IR), and satellite/microwaves to carry signals from one computer to another without a permanent cable connection.

Common Networking Devices

Networking devices are used to connect computers and peripheral devices so they can communicate.

Hubs

A hub is a device that when used, extends an Ethernet wire allowing more devices to communicate with each other. When using a hub, the network topology changes from a linear bus, where each device plugs directly into the wire, to a star.

Data arriving over the cables to a hub port is electrically repeated on all the other ports that are connected to the same Ethernet LAN. That happens except for the port on which the data was received. Sometimes hubs are called concentrators, because they serve as a central connection point for an Ethernet LAN. Hubs are most commonly used in Ethernet 10BASE-T or 100BASE-T networks, although there are other network architectures that use them.

Bridges and Switches

Bridges connect network segments. The basic functionality of the bridge resides in its ability to make intelligent decisions about whether to pass signals on to the next segment of a network. When a bridge sees data being sent from one computer to another on the network, it looks at the destination address. The bridge compares this address to the forwarding table to determine whether to filter, flood, or copy the data onto another segment.

A typical bridge may have just two ports, linking two systems on the same network. A switch is a more sophisticated device than a bridge. The basic function of the switch is deceptively simple. It is to choose a port to forward data to its destination.

Routers

Routers are sophisticated internetworking devices. They are slower than bridges and switches, but make "smart" decisions on how to route, or send, packets received on one port to a network on another port. Where each port is attached to a network segment is described as a router interface. Routers can be computers with special network software installed on them or they can be other devices built by network equipment manufacturers. Routers contain tables of network addresses along with optimal destination routes to other networks.

Networking Protocols and the OSI Model

The Open Systems Interconnection (OSI) reference model is an industry standard framework that is used to divide the functions of networking into seven distinct layers. It is one of the most commonly used teaching and reference tools today in networking. The International Organization for Standardization (ISO) developed the OSI model in the 1980s.

What is a protocol?

A protocol is a controlled sequence of messages that are exchanged between two or more systems to accomplish a given task. Protocol specifications define this sequence together with the format or layout of the messages that are exchanged. Protocols use control structures in each system to coordinate the exchange of information between the systems. They operate like a set of interlocking gears. Computers can precisely track protocol connection points as they move through the sequence of exchanges. Timing is crucial to network operation. Protocols require messages to arrive within certain time intervals, so systems maintain one or more timers during protocol execution. They also take alternative actions if the network does not meet the timing rules. To do their work, many protocols depend on the operation of other protocols in the group or suite of protocols. Protocol functions include the following:

- Identifying errors
- Applying compression techniques
- Deciding how data is to be sent
- Addressing data
- Deciding how to announce sent and received data

Transmission Control Protocol/Internet Protocol

The TCP/IP suite of protocols has become the dominant standard for internetworking. TCP/IP represents a set of public standards that specify how packets of information are exchanged between computers over one or more networks.

The TCP/IP protocol suite includes a number of major protocols and each performs a specific function.

Application Protocols

The application layer is the fourth layer in the TCP/IP model. It provides the starting point for any communication session.

Hypertext Transfer Protocol (HTTP) – HTTP governs how files such as text, graphics, sounds, and video are exchanged on the Internet or World Wide Web (WWW).

Telnet – Telnet enables terminal access to local or remote systems. The telnet application is used to access remote devices for configuration, control, and troubleshooting.

File Transfer Protocol (FTP) – FTP is an application that provides services for file transfer and manipulation. FTP uses the session layer to allow multiple simultaneous connections to remote file systems.

Transport Protocols

The transport layer is the third layer in the TCP/IP model. It provides an end-to-end management of the communications session.

Transmission Control Protocol (TCP) – TCP is the primary Internet protocol for the reliable delivery of data.

Network Protocols

The Internet layer is the second layer in TCP/IP model. It provides internetworking for the communications session.

Internet Protocol (IP) – IP provides source and destination addressing. In conjunction with routing protocols, IP provides packet forwarding from one network to another toward a destination.

Address Resolution Protocol (ARP) – ARP is used to discover the local address, the MAC address, of a station on the network when its IP address is known. End stations as well as routers use ARP to discover local addresses.

TCP/IP Utilities

TCP/IP is a complex collection of protocols. Most vendors implement the suite to include a variety of utilities for viewing configuration information and troubleshooting problems.

Ping - Ping is a simple but highly useful command line utility that is included in most implementations of TCP/IP. Ping can be used with either the hostname or the IP address to test IP connectivity.

TCP/IP Configuration - TCP/IP configuration information can be displayed using different utilities. Depending on the operating system used, the following utilities are used:

ipconfig – Windows NT and Windows 2000 (command line).

winipcfg – Windows 95, 98, and ME (graphical interface).

The configuration utilities can provide a wealth of information including the currently used IP address, MAC address, subnet mask, and default gateway. The utilities can show the addresses of DNS and WINS servers, DHCP information, and services enabled. There are a variety of switches available, depending on the vendor and specific utility.

tracert - Tracing the route a packet takes on its journey from source computer to destination host is often useful. TCP/IP stacks include a route tracing utility that enables users to identify the routers through which the message passes.

Connecting to the Internet.

Modems.

The modem is an electronic device that is used for computer communications through telephone lines. It allows data transfer between one computer and another.

Expansion cards – These modems, as shown in Figure , are the most common type. They plug into the motherboard expansion slots, either the ISA or PCI. They are called internal modems.

Personal Computer Memory Card International Association (PCMCIA) – These modems, as shown in Figure , are a variation of modems that are designed for easy installation in notebook computers. Also known as PC cards, they look like credit cards and are small and very portable.

External modems – These can be used with any computer. The connection type depends on the type of modem used. External modems for dial-up plug into a serial port, either COM1 or COM2, as shown in Figure . External modems for DSL or Cable, shown in Figure , are generally connected by a USB or through the network card on the back of the computer.

Built-in modems – These are used in some notebook or laptop computers.

Digital subscriber line (DSL)

Digital subscriber line (DSL) is an always-on technology. This means there is no need to dial up each time to connect to the Internet. It is a relatively new technology currently being offered by phone companies as an add-on service over existing copper wire or phone lines.

Cable modems and DSL Modems are available as internal and external units. Most internal cable modems are in the form of PCI cards. An external cable modem is a small box with a coaxial CATV cable connection. Usually, a splitter is used to divide the signal between the TV and the cable modem. The box is connected to an Ethernet card in the computer through UTP Ethernet. External USB devices may also be available to connect the modem to the computer USB port without requiring an Ethernet card.

Satellite Internet

Users in rural areas or with no other access to high speed Internet service may want to consider Satellite. Figure shows a Satellite dish. Satellite Internet does not require a phone line or cable. Two-way communication, for upload and download, is achieved with the use of a satellite dish. Download speed is up to 500 kbps while the upload speed is one-tenth of that. A two-way satellite Internet consists of the following:

- Approximately a two-foot by three-foot dish
- Two modems for uplink and downlink
- Coaxial cables between the dish and modem

Satellites require a clear view to the south since orbiting satellites are over the equator. Just like satellite TV, heavy rains and high winds affect the Internet signals.