BCS502 COMPUTER NETWORKS

Module-1

Chapter 1: Introduction (Pg. 1 to 19): Data Communications, Networks, Network Types
Chapter 2: Networks Models (Pg. 1 to 19): Protocol Layering, TCP/IP Protocol suite, The OSI model
Chapter 7 (Pg. 1 to 19): Introduction to Physical Layer: Transmission media, Guided Media, Unguided Media: Wireless.
Chapter 8: Switching(Pg. 1 to 19): Packet Switching and its types.
Textbook: Ch. 1.1 - 1.3, 2.1 - 2.3, 7.1 – 7.3, 8.3.

Chapter 1: Introduction: Data Communications, Networks, Network Types

---

Data Communications - *Components - Data Representation - Data Flow*

- Data communications are the exchange of data between two devices via some form of transmission medium such as a wire cable.
- For data communications to occur, the communicating devices must be part of a communication system made up of a combination of hardware (physical equipment) and software (programs).
- The effectiveness of a data communications system depends on **four fundamental characteristics**:
    1. Delivery
    2. Accuracy
    3. Timeliness, and
    4. Jitter.

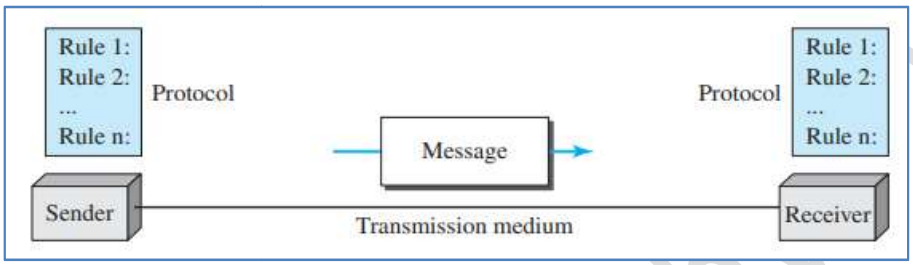
1. Delivery: The system must deliver data to the correct destination. Data must be received by the intended device or user and only by that device or user.
2. Accuracy: The system must deliver the data accurately. Data that have been altered in transmission and left uncorrected are unusable.
3. Timeliness: The system must deliver data in a timely manner. Data delivered late are useless. In the case of video and audio, timely delivery means delivering data as they are produced, in the same order that they are produced, and without significant delay. This kind of delivery is called real-time transmission.
4. Jitter: Jitter refers to the variation in the packet arrival time. It is the uneven delay in the delivery of audio or video packets. For example, let us assume that video packets are sent every 30 ms. If some of the packets arrive with 30-ms delay and others with 40-ms delay, an uneven quality in the video is the result.

Components

- A data communications system has **five components.**
    1. Message
    2. Sender
    3. Receiver
    4. Transmission medium
    5. Protocol

1. **Message.** The message is the information (data) to be communicated. Popular forms of information include text, numbers, pictures, audio, and video.
2. **Sender.** The sender is the device that sends the data message. It can be a computer, workstation, telephone handset, video camera, and so on.

3. **Receiver.** The receiver is the device that receives the message. It can be a computer, workstation, telephone handset, television, and so on.
4. **Transmission medium**. The transmission medium is the physical path by which a message travels from sender to receiver. Some examples of transmission media include twisted-pair wire, coaxial cable, fiber-optic cable, and radio waves.
5. **Protocol.** A protocol is a set of rules that govern data communications. It represents an agreement between the communicating devices. Without a protocol, two devices may be connected but not communicating, just as a person speaking French cannot be understood by a person who speaks only Japanese.



***

Data Representation

- Information today comes in different forms such as text, numbers, images, audio, and video.

Text

- In data communications, text is represented as a bit pattern, a sequence of bits (0s or 1s). Different sets of bit patterns have been designed to represent text symbols.
- Each set is called a code, and the process of representing symbols is called coding.
- Today, the prevalent coding system is called Unicode, which uses 32 bits to represent a symbol or character used in any language in the world.
- The American Standard Code for Information Interchange (ASCII), developed some decades ago in the United States, now constitutes the first 127 characters in Unicode and is also referred to as Basic Latin.

Numbers

- Numbers are also represented by bit patterns. However, a code such as ASCII is not used to represent numbers; the number is directly converted to a binary number to simplify mathematical operations.

Images

- Images are also represented by bit patterns. In its simplest form, an image is composed of a matrix of pixels (picture elements), where each pixel is a small dot. The size of the pixel depends on the ***resolution***. For example, an image can be divided into 1000 pixels or 10,000 pixels. In the second case, there is a better representation of the image (better resolution), but more memory is needed to store the image.
- After an image is divided into pixels, each pixel is assigned a bit pattern. The size and the value of the pattern depend on the image. For an image made of only blackand-white dots (e.g., a chessboard), a 1-bit pattern is enough to represent a pixel.
- If an image is not made of pure white and pure black pixels, we can increase the size of the bit pattern to include gray scale. For example, to show four levels of gray scale, we can use 2-bit patterns. A black pixel can be represented by 00, a dark gray pixel by 01, a light gray pixel by 10, and a white pixel by 11.

- There are several methods to represent color images. One method is called RGB, so called because each color is made of a combination of three primary colors: red, green, and blue. The intensity of each color is measured, and a bit pattern is assigned to it. Another method is called YCM, in which a color is made of a combination of three other primary colors: yellow, cyan, and magenta.

Audio

- Audio refers to the recording or broadcasting of sound or music. Audio is by nature different from text, numbers, or images. It is continuous, not discrete. Even when we use a microphone to change voice or music to an electric signal, we create a continuous signal.

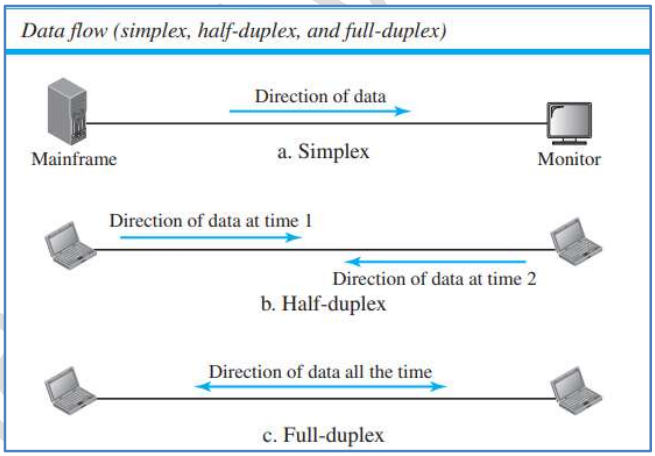
Video

- Video refers to the recording or broadcasting of a picture or movie. Video can either be produced as a continuous entity (e.g., by a TV camera), or it can be a combination of images, each a discrete entity, arranged to convey the idea of motion.

***

Data Flow

- Communication between two devices can be simplex, half-duplex, or full-duplex.



Simplex

- In ***simplex mode, the communication is unidirectional***, as on a one-way street. Only one of the two devices on a link can transmit; the other can only receive.
- Keyboards and traditional monitors are examples of simplex devices.
- The keyboard can only introduce input; the monitor can only accept output. The simplex mode can use the entire capacity of the channel to send data in one direction.

Half-Duplex

- In ***half-duplex mode, each station can both transmit and receive, but not at the same time***. When one device is sending, the other can only receive, and vice versa. The half-duplex mode is like a one-lane road with traffic allowed in both directions.
- In a half-duplex transmission, the entire capacity of a channel is taken over by whichever of the two devices is transmitting at the time. ***Walkie-talkies and CB (citizens band) radios are both half-duplex systems.*** The half-duplex mode is used in cases where there is no need for communication in both directions at the same time; the entire capacity of the channel can be utilized for each direction.

Full-Duplex

- In ***full-duplex mode (also called duplex), both stations can transmit and receive simultaneously***. The full-duplex mode is like a two-way street with traffic flowing in both directions at the same time.
- In full-duplex mode, signals going in one direction share the capacity of the link with signals going in the other direction. This ***sharing can occur in two ways***: ***Either the link must contain two physically separate transmission paths, one for sending and the other for receiving; or the capacity of the channel is divided between signals traveling in both directions***. One common example of full-duplex communication is the telephone network.

- When two people are communicating by a telephone line, both can talk and listen at the same time. The full-duplex mode is used when communication in both directions is required all the time. The capacity of the channel, however, must be divided between the two directions.

Networks: *Network Criteria - Physical Structure*

- A ***network*** is the ***interconnection of a set of devices capable of communication***. In this definition, ***a device can be a host*** (or an end system as it is sometimes called) ***such as a large computer, desktop, laptop, workstation, cellular phone, or security system.***
- A device in this definition can also be a ***connecting device such as a router***, which connects the network to other networks, a switch, which connects devices together, a modem (modulator-demodulator), which changes the form of data, and so on.
- These devices in a network are connected using wired or wireless transmission media such as cable or air. When we connect two computers at home using a plug-and-play router, we have created a network, although very small.

Network Criteria

- A network must be able to meet a certain number of criteria. The most important of these are ***performance***, ***reliability***, and ***security***.

Performance

- Performance can be measured in many ways, including ***transit time*** and ***response time***.
  - ***Transit time*** is the amount of time required for a message to travel from one device to another.
  - ***Response time*** is the elapsed time between an inquiry and a response.
- The performance of a network depends on a ***number of factors***, including
  - the number of users
  - the type of transmission medium
  - the capabilities of the connected hardware, and
  - The efficiency of the software.
- Performance is often evaluated by ***two networking metrics***: ***throughput*** and ***delay***. We often need more throughput and less delay. However, these two criteria are often contradictory. If we try to send more data to the network, we may increase throughput but we increase the delay because of traffic congestion in the network.

Reliability

- In addition to accuracy of delivery, network reliability is measured by the frequency of failure, the time it takes a link to recover from a failure, and the network's robustness in a catastrophe.

Security

- Network security issues include protecting data from unauthorized access, protecting data from damage and development, and implementing policies and procedures for recovery from breaches and data losses.

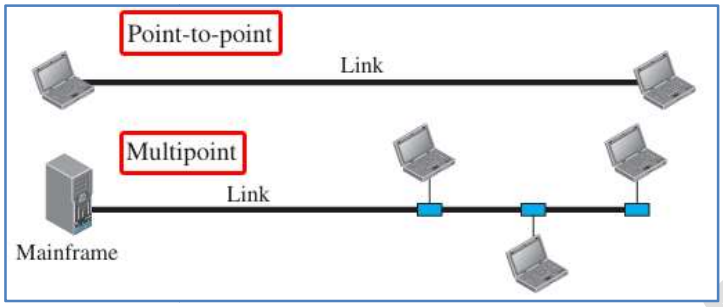
****

Physical Structures - Type of Connection - Physical Topology

Type of Connection

- A network is two or more devices connected through links.
- A ***link*** is a communications pathway that transfers data from one device to another. For visualization purposes, it is simplest to imagine any link as a line drawn between two points.

- For communication to occur, ***two devices must be connected*** in some way to the same link at the same time. There are ***two possible types of connections:***
  - ***point-to-point*** and
  - ***multipoint***



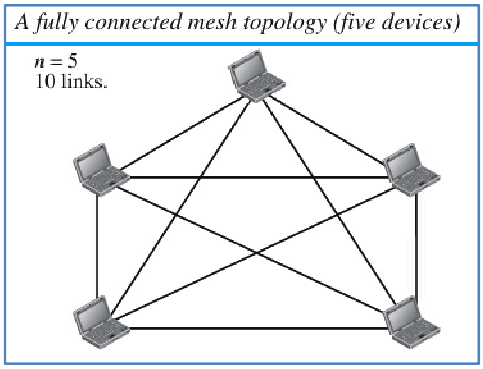
Point-to-Point

- A point-to-point connection provides a dedicated link between two devices. The entire capacity of the link is reserved for transmission between those two devices. Most point-to-point connections use an actual length of wire or cable to connect the two ends, but other options, such as microwave or satellite links, are also possible. When we change television channels by infrared remote control, we are establishing a point-to-point connection between the remote control and the television's control system.

Multipoint

- A multipoint (also called multidrop) connection is one in which more than two specific devices share a single link.
- In a multipoint environment, the capacity of the channel is shared, either spatially or temporally.
- If several devices can use the link simultaneously, it is a spatially shared connection. If users must take turns, it is a timeshared connection.
- The term physical topology refers to the way in which a network is laid out physically. Two or more devices connect to a link; two or more links form a topology. The topology of a network is the geometric representation of the relationship of all the links and linking devices (usually called nodes) to one another.
- There are ***four basic topologies*** possible: ***mesh***, ***star***, ***bus***, and ***ring***.

1. Mesh Topology



- In a mesh topology, every device has a dedicated point-to-point link to every other device.
- The term ***dedicated*** means that the link carries traffic only between the two devices it connects. To find the number of physical links in a fully connected mesh net work with n nodes, we first consider that each node must be connected to every other node.
- Node 1 must be connected to n – 1 nodes, node 2 must be connected to n – 1 nodes, and finally node n must be connected to n – 1 nodes. We need n (n – 1) physical links.
- If each physical link allows communication in both directions (duplex mode), we can divide the number of links by 2 [we need n (n – 1) / 2 duplex-mode links].
- To accommodate that many links, every device on the network must have n – 1 input/output (I/O) ports (see Figure 1.4) to be connected to the other n – 1 stations.

- ***One practical example*** of a mesh topology is the connection of telephone regional offices in which each regional office needs to be connected to every other regional office.

Advantages

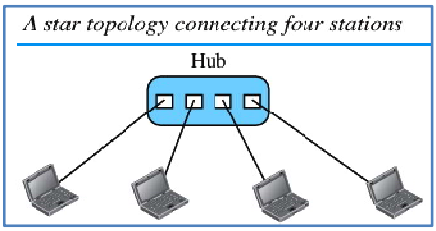
1. The use of dedicated links guarantees that each connection can carry its own data load, thus eliminating the traffic problems that can occur when links must be shared by multiple devices.
2. A mesh topology is robust. If one link becomes unusable, it does not incapacitate the entire system.
3. There is the advantage of privacy or security. When every message travels along a dedicated line, only the intended recipient sees it. Physical boundaries prevent other users from gaining access to messages.
4. Point-to-point links make fault identification and fault isolation easy. Traffic can be routed to avoid links with suspected problems. This facility enables the network manager to discover the precise location of the fault and aids in finding its cause and solution.

Disadvantages

The main disadvantages of a mesh are related to the amount of cabling and the number of I/O ports required.

1. Because every device must be connected to every other device, installation and reconnection are difficult.
2. The sheer bulk of the wiring can be greater than the available space (in walls, ceilings, or floors) can accommodate.
3. The hardware required to connect each link (I/O ports and cable) can be prohibitively expensive. For these reasons a mesh topology is usually implemented in a limited fashion.

2. Star Topology



- In a star topology, each device has a dedicated point-to-point link only to a central controller, usually called a hub. The devices are not directly linked to one another.
- Unlike a mesh topology, a star topology does not allow direct traffic between devices. The controller acts as an exchange: If one device wants to send data to another, it sends the data to the controller, which then relays the data to the other connected device.
- The star topology is **used in local-area networks (LANs).**
- High-speed LANs often use a star topology with a central hub.

Advantages

- A **star topology is less expensive than a mesh topology**. In a star, each device needs only one link and one I/O port to connect it to any number of others. This factor also makes it easy to install and reconfigure. Far less cabling needs to be housed, and additions, moves, and deletions involve only one connection: between that device and the hub.
- **Robustness**. If one link fails, only that link is affected. All other links remain active. This factor also lends itself to easy fault identification and fault isolation. As long as the hub is working, it can be used to monitor link problems and bypass defective links.

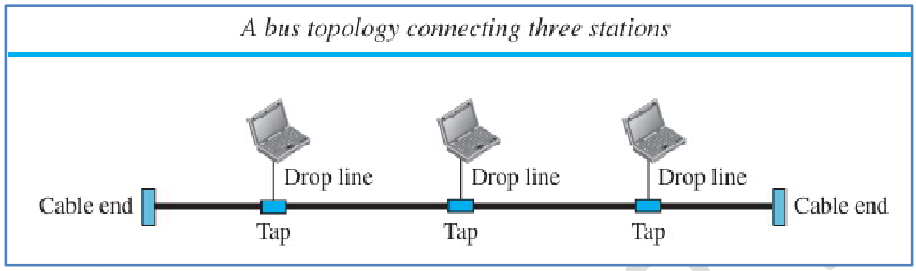
Disadvantages

- The **dependency of the whole topology on one single point, the hub**. **If the hub goes down, the whole system is dead**.
- Although a star requires far less cable than a mesh, each node must be linked to a central hub. For this reason, **often more cabling is required in a star** than in some other topologies (such as ring or bus).

---

3. Bus Topology

- A bus topology is multipoint. One long cable acts as a backbone to link all the devices in a network.
- Nodes are connected to the bus cable by drop lines and taps. A **drop line** is a connection running between the **device and the main cable**.
- A **tap** is a connector that either splices into the main cable or punctures the sheathing of a cable to create a contact with the metallic core. As a signal travels along the backbone, some of its energy is transformed into heat. Therefore, it becomes weaker and weaker as it travels farther and farther. For this reason there is a limit on the number of taps a bus can support and on the distance between those taps.



Advantages

- **Ease of installation** - Backbone cable can be laid along the most efficient path, and then connected to the nodes by drop lines of various lengths. In this way, a bus uses less cabling than mesh or star topologies.
- In a star, for example, four network devices in the same room require four lengths of cable reaching all the way to the hub. **In a bus, this redundancy is eliminated**. Only the backbone cable stretches through the entire facility. Each drop line has to reach only as far as the nearest point on the backbone.

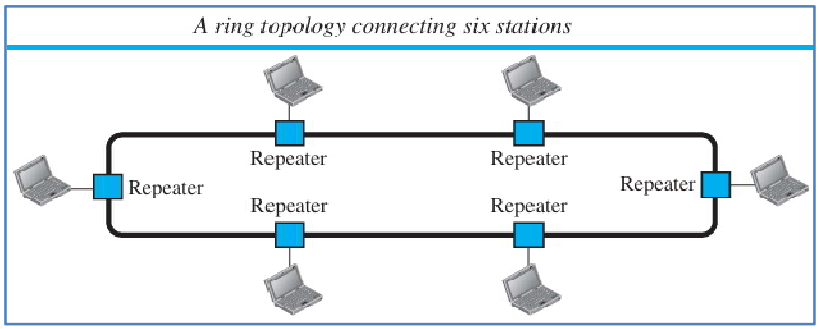
Disadvantages

- **Difficult in reconnection and fault isolation.** A bus is usually designed to be optimally efficient at installation. It can therefore be difficult to add new devices. Signal reflection at the taps can cause degradation in quality. This degradation can be controlled by limiting the number and spacing of devices connected to a given length of cable.
- Adding new devices may therefore require modification or replacement of the backbone.
- In addition, a fault or break in the bus cable stops all transmission, even between devices on the same side of the problem. The damaged area reflects signals back in the direction of origin, creating noise in both directions. Bus topology was the one of the first topologies used in the design of early local area networks. Traditional Ethernet LANs can use a bus topology.

---

4. Ring Topology

- In a ring topology, each device has a dedicated point-to-point connection with only the two devices on either side of it.
- A signal is passed along the ring in one direction, from device to device, until it reaches its destination.
- Each device in the ring incorporates a repeater. When a device receives a signal intended for another device, its repeater regenerates the bits and passes them along.



Advantages

- A ring is relatively easy to install and reconfigure.
- Each device is linked to only its immediate neighbors (either physically or logically).
- To add or delete a device requires changing only two connections. The only constraints are media and traffic considerations (maximum ring length and number of devices).
- Fault isolation is simplified. Generally, in a ring a signal is circulating at all times. If one device does not receive a signal within a specified period, it can issue an alarm. The alarm alerts the network operator to the problem and its location.

Disadvantages

- Unidirectional traffic can be a disadvantage. In a simple ring, a break in the ring (such as a disabled station) can disable the entire network. This weakness can be solved by using a dual ring or a switch capable of closing off the break.

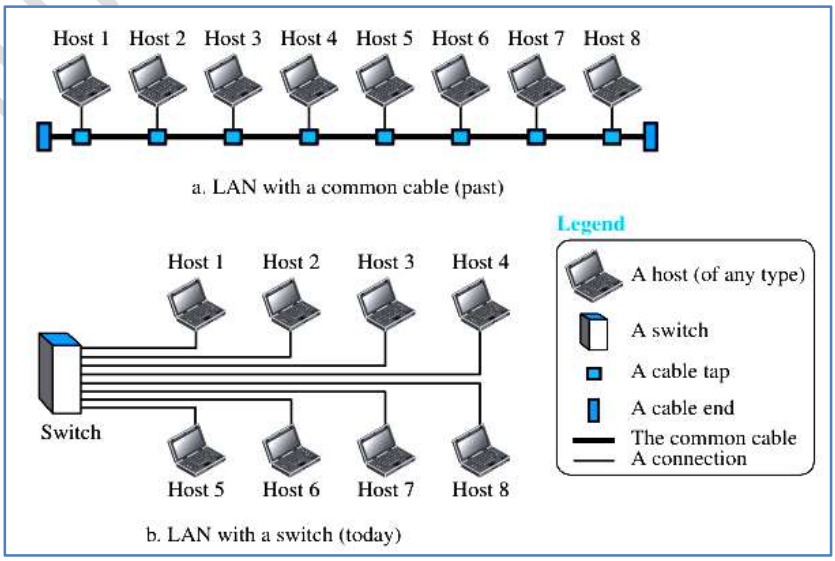
Network Types (Geographical coverage)

1. **Local Area Network**
2. **Wide Area Network**
3. **Switching**

---

1. Local Area Network

- A local area network (LAN) is usually privately owned and connects some hosts in a single office, building, or campus.
- Depending on the needs of an organization, a LAN can be as simple as two PCs and a printer in someone's home office, or it can extend throughout a company and include audio and video devices.
- Each host in a LAN has an identifier, an address that uniquely defines the host in the LAN.
- A packet sent by a host to another host carries both the source host's and the destination host's addresses.
- In the past, all hosts in a network were connected through a common cable, which meant that a packet sent from one host to another was received by all hosts. The intended recipient kept the packet; the others dropped the packet.
- Today, most LANs use a **smart connecting switch**, which is able to recognize the destination address of the packet and guide the packet to its destination without sending it to all other hosts.



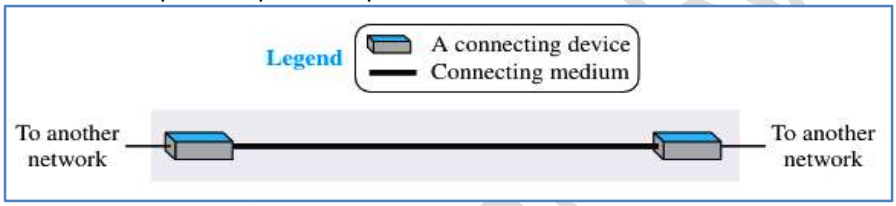
- The switch improve the traffic in the LAN and allows more than one pair to communicate with each other at the same time if there is no common source and destination among them.
- Note that the above definition of a LAN does not define the minimum or maximum number of hosts in a LAN. Figure shows a LAN using either a common cable or a switch.

2. Wide Area Network

- A wide area network (WAN) is also an interconnection of devices capable of communication.
- However, there are some differences between a LAN and a WAN. A LAN is normally limited in size, spanning an office, a building, or a campus; a WAN has a wider geographical span, spanning a town, a state, a country, or even the world.
- A **LAN interconnects hosts**; a **WAN interconnects connecting devices such as switches, routers, or modems**.
- A LAN is normally privately owned by the organization that uses it; a WAN is normally created and run by communication companies and leased by an organization that uses it.
- Two distinct examples of WANs today:
    1. Point-to-point WANs
    2. Switched WANs.

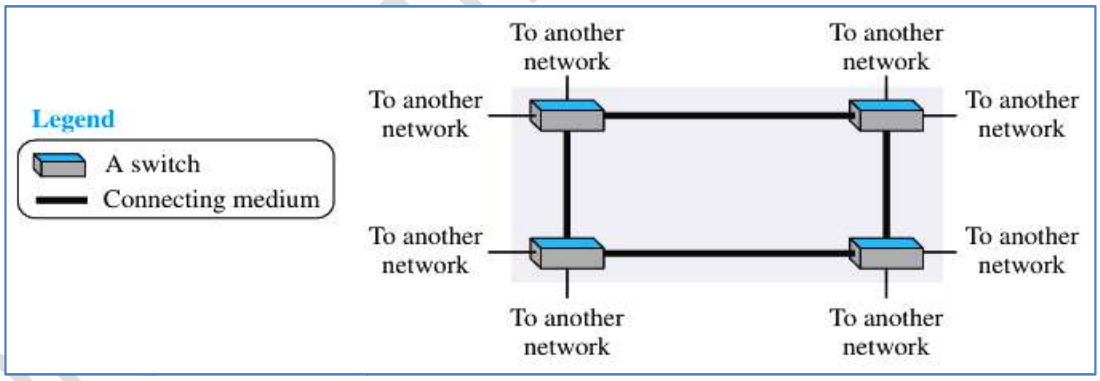
Point-to-Point WAN

- A point-to-point WAN is a network that **connects two communicating devices through a transmission media (cable or air)**.
- Figure shows an example of a point-to-point WAN.



Switched WANs

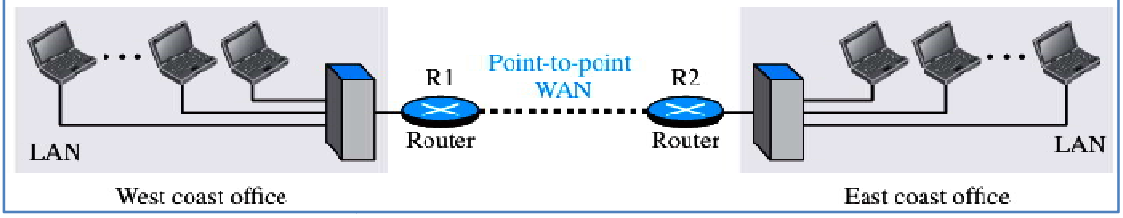
- A switched WAN is a network with more than two ends. A switched WAN is used in the backbone of global communication today. We can say that a switched WAN is a combination of several point-to-point WANs that are connected by switches. Figure shows an example of a switched WAN.



Internetwork

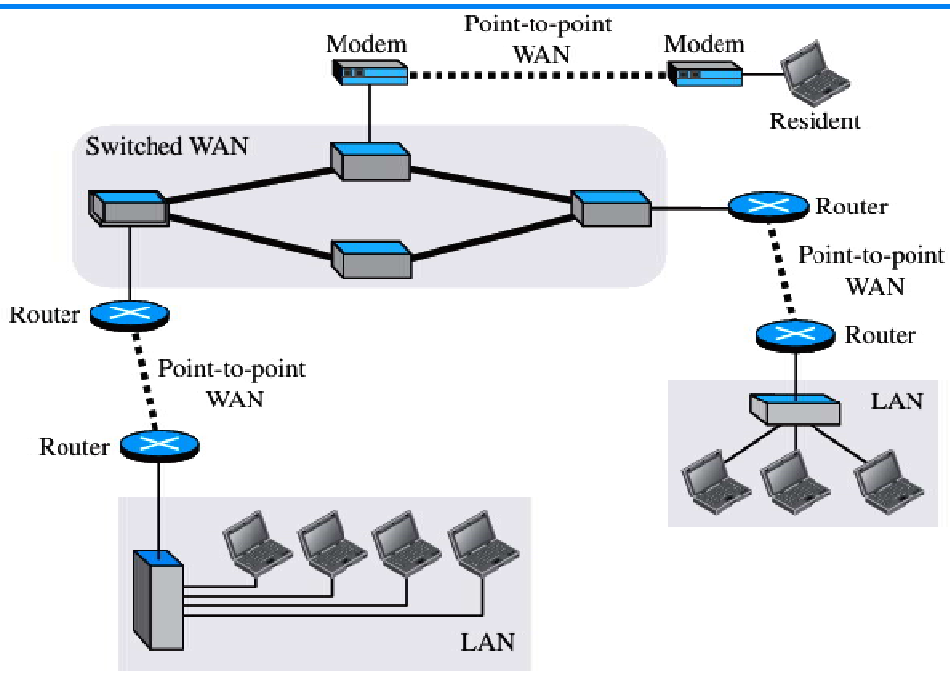
- When two or more networks (a LAN or a WAN) are connected, they make an internetwork, or internet.
- As an example, assume that an organization has two offices, one on the east coast and the other on the west coast. Each office has a LAN that allows all employees in the office to communicate with each other. To make the communication between employ ees at different offices possible, the management leases a point-to-point dedicated WAN from a service provider, such as a telephone company, and connects the two LANs.
- Now the company has an internetwork, or a private internet. Communication between offices is now possible. Figure shows this internet.

Figure *An internetwork made of two LANs and one point-to-point WAN*



- When a host in the west coast office sends a message to another host in the same office, the **router blocks the message, but the switch directs the message to the destination**. On the other hand, when a host on the west coast sends a message to a host on the east coast, router R1 routes the packet to router R2, and the packet reaches the destination. The following figure shows another internet with several LANs and WANs connected. One of the WANs is a switched WAN with four switches.

Figure *A heterogeneous network made of four WANs and three LANs*

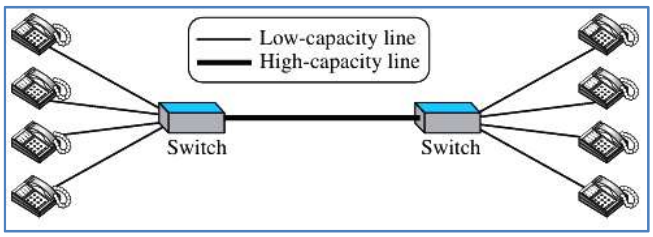


3. Switching

- An **internet is a switched network in which a switch connects at least two links together**.
- A **switch needs to forward data from a network to another network when required**.
- The **two most common types of switched networks** are
  1. circuit-switched networks
  2. packet-switched networks

Circuit-switched networks

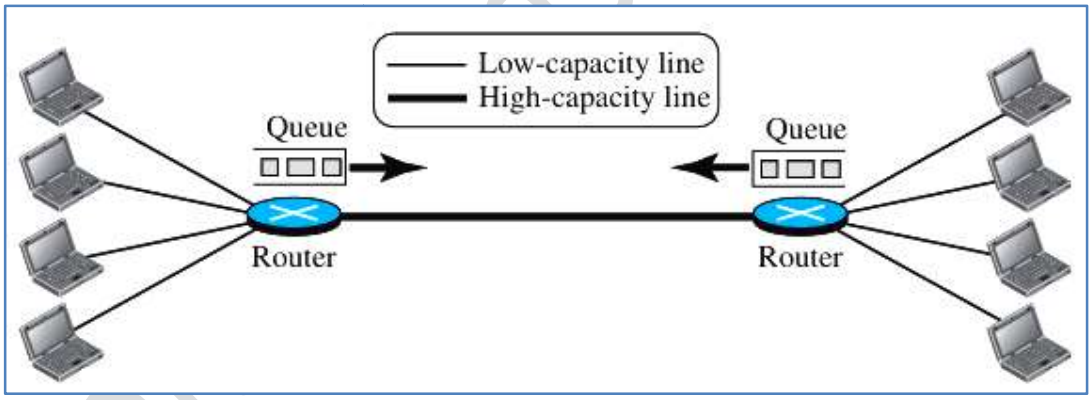
- In a circuit-switched network, a dedicated connection, called a circuit, is always available between the two end systems; the switch can only make it active or inactive. The following figure shows a very simple switched network that connects four telephones to each end.
- We have used telephone sets instead of computers as an end system because circuit switching was very common in telephone networks in the past.



- In Figure, the four telephones at each side are connected to a switch. The switch connects a telephone set at one side to a telephone set at the other side.
- The thick line connecting two switches is a high-capacity communication line that can handle four voice communications at the same time; the capacity can be shared between all pairs of telephone sets. The switches used in this example have forwarding tasks but no storing capability.
- Let us look at two cases.
  - In the first case, all telephone sets are busy; four people at one site are talking with four people at the other site; the capacity of the thick line is fully used.
  - In the second case, only one telephone set at one side is connected to a tele phone set at the other side; only one-fourth of the capacity of the thick line is used.
- This means that a circuit-switched network is efficient only when it is working at its full capacity; most of the time, it is inefficient because it is working at partial capacity.
- The reason that we need to make the capacity of the thick line four times the capacity of each voice line is that we do not want communication to fail when all telephone sets at one side want to be connected with all telephone sets at the other side.

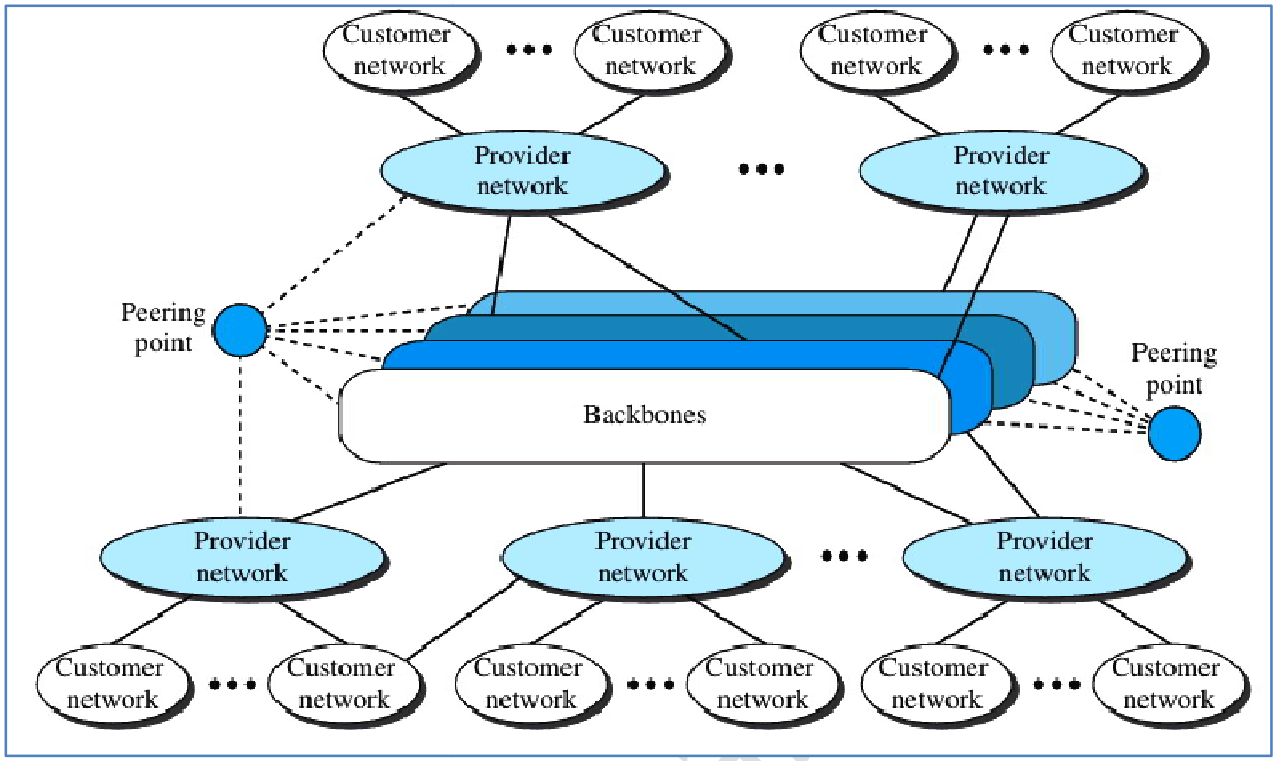
Packet-switched networks

- In a computer network, the communication between the two ends is done in blocks of data called packets. In other words, instead of the continuous communication we see between two telephone sets when they are being used, we see the exchange of individual data packets between the two computers. This allows us to make the switches function for both storing and forwarding because a packet is an independent entity that can be stored and sent later.
- The following figure shows a small packet-switched network that con nects four computers at one site to four computers at the other site.



- A router in a packet-switched network has a queue that can store and forward the packet.
- Now assume that the capacity of the thick line is only twice the capacity of the data line connecting the computers to the routers. If only two computers (one at each site) need to communicate with each other, there is no waiting for the packets.
- However, if packets arrive at one router when the thick line is already working at its full capacity, the packets should be stored and forwarded in the order they arrived.
- The two simple examples show that a packet-switched network is more efficient than a circuit switched network, but the packets may encounter some delays.

The Internet



- Backbones and provider networks are also called **Internet Service Providers (ISPs).**
- The backbones are often referred to as international ISPs; the **provider networks are often referred to as national or regional ISPs.**

Accessing the Internet

- The Internet today is an internetwork that allows any user to become part of it. The user, however, needs to be physically connected to an ISP. The physical connection is normally done through a point-to-point WAN. They are
  1. *Using Telephone Networks*
  2. *Using Cable Networks*
  3. *Using Wireless Networks*
  4. *Direct Connection to the Internet*

Using Telephone Networks

- Today most residences and small businesses have telephone service, which means they are connected to a telephone network.
- Since most telephone networks have already connected themselves to the Internet, one option for residences and small businesses to connect to the Internet is to change the voice line between the residence or business and the telephone center to a point-to-point WAN. This can be done in two ways.
  1. Dial-up service
  2. DSL Service

Using Cable Networks

- More and more residents over the last two decades have begun using cable TV services instead of antennas to receive TV broadcasting. The cable companies have been upgrading their cable networks and connecting to the Internet. A residence or a small business can be connected to

the Internet by using this service. It provides a higher speed connection, but the speed varies depending on the number of neighbors that use the same cable.

Using Wireless Networks

- Wireless connectivity has recently become increasingly popular. A household or a small business can use a combination of wireless and wired connections to access the Internet. With the growing wireless WAN access, a household or a small business can be connected to the Internet through a wireless WAN.

Direct Connection to the Internet

- A large organization or a large corporation can itself become a local ISP and be con nected to the Internet. This can be done if the organization or the corporation leases a high-speed WAN from a carrier provider and connects itself to a regional ISP. For example, a large university with several campuses can create an internetwork and then connect the internetwork to the Internet.
