NETWORKS

A network is a set of devices (often referred to as *nodes)* connected by communication links. A node can be a computer, printer, or any other device capable of sending and/or receiving data generated by other nodes on the network.

"Computer network'' to mean a collection of autonomous computers interconnected by a single technology. Two computers are said to be interconnected if they are able to exchange information.
The connection need not be via a copper wire; fiber optics, microwaves, infrared, and communication satellites can also be used.

Networks come in many sizes, shapes and forms, as we will see later.They are usually connected together to make larger networks, with the **Internet** being the most well-known example of a network of networks.

There is considerable confusion in the literature between a **computer network** and a **distributed system**. The key distinction is that in a distributed system, a collection of independent computers appears to its users as a single coherent system. Usually, it has a single model or paradigm that it presents to the users. Often a layer of software on top of the operating system, called **middleware**, is responsible for implementing this model. A well-known example of a distributed system is the **World Wide Web**. It runs on top of the Internet and presents a model in which everything looks like a document (Web page).

USES OF COMPUTER NETWORKS
1. Business Applications
- to distribute information throughout the company (**resource sharing).**sharing physical resources such as printers, and tape backup systems, issharing information
- **client-server model**. It is widely used and forms the basis of much network usage.
- **communication medium** among employees.**email (electronic mail)**,which employees generally use for a great deal of daily communication.
- Telephone calls between employees may be carried by the computer network instead of by the phone company. This technology is called **IP telephony** or **Voice over IP (VoIP)** when Internet technology is used.
- **Desktop sharing** lets remote workers see and interact with a graphicalcomputer screen
- doing business electronically, especially with customers and suppliers. This new model is called **e-commerce (electronic commerce)** and it has grownrapidly in recent years.

2 Home Applications
- **peer-to-peer** communication
- person-to-person communication

- electronic commerce
- entertainment.(game playing,)

3 Mobile Users
- Text messaging or texting
- Smart phones,
- GPS (Global Positioning System)
- m-commerce
- NFC (Near Field Communication)

4 Social Issues

With the good comes the bad, as this new-found freedom brings with it manyunsolved social, political, and ethical issues.

Social networks, message boards, content sharing sites, and a host of other applications allow people to share their views with like-mindedindividuals. As long as the subjects are restricted to technical topics or hobbies like gardening, not too many problems will arise.

The trouble comes with topics that people actually care about, like politics,religion, or sex. Views that are publicly posted may be deeply offensive to some people. Worse yet, they may not be politically correct. Furthermore, opinions need not be limited to text; high-resolution color photographs and video clipsare easily shared over computer networks. Some people take a live-and-let-live view, but others feel that posting certain material (e.g., verbal attacks on particular countries or religions, pornography, etc.) is simply unacceptable and that such content must be censored. Different countries have different and conflicting laws in this area. Thus, the debate rages.

Computer networks make it very easy to communicate. They also make it easy for the people who run the network to snoop on the traffic. This sets up conflicts over issues such as **employee rights versus employer rights**. Many people read and write email at work. Many employers have claimed the right to read and possibly censor employee messages, including messages sent from a home computer outside working hours. Not all employees agree withthis, especially the latter part.
Another conflict is centered around government versus citizen's rights.
A new twist with mobile devices is location privacy. As part of the process of providing service to your mobile device the network operators learn where you are at different times of day. This allows them to track your movements. They may know which nightclub you frequent and which medical center you visit.

Phishing ATTACK: *Phishing* is a type of social engineering *attack* often used to steal user data, including login credentials and credit card numbers. It occurs when an attacker, masquerading as a trusted entity, dupes a victim into opening an email, instant message, or text message.

BOTNET ATTACK: Botnets can be used to perform <u>distributed denial-of-service</u> <u>attack</u> (DDoS attack), steal data, send spam, and allows the attacker to access the device and its connection.

The effectiveness of a data communications system depends on four fundamental characteristics: delivery, accuracy, timeliness, and jitter.

I. **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 beenaltered 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 unevendelay 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.

A data communications system has five components

I. **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 acomputer, workstation, telephone handset, video camera, and so on.

3. **Receiver.** The receiver is the device that receives the message. It can be acomputer, 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 aperson speaking French cannot be understood by a person who speaks only Japanese.
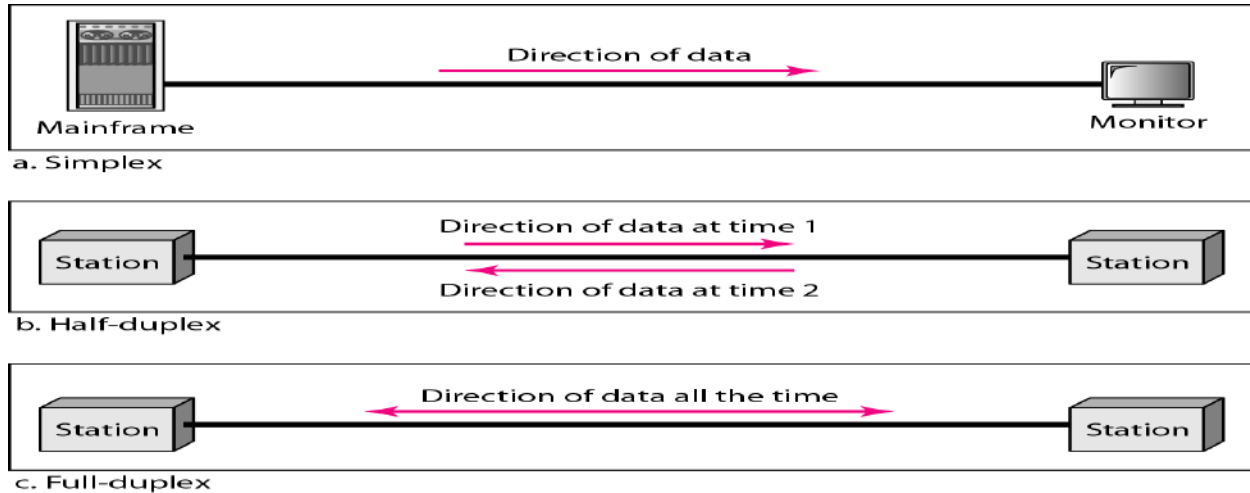

Data Representation

Text Numbers
Images Audio
Video
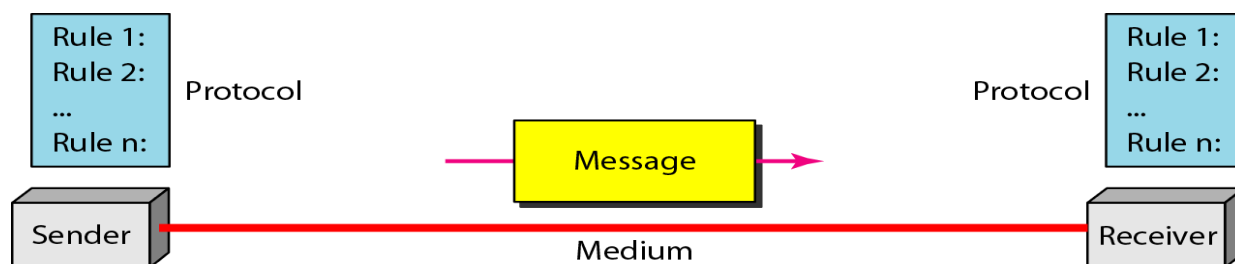
Data Flow

Communication between two devices can be simplex, half-duplex, or full-duplexas shown in Figure.

a. Simplex

b. Half-duplex

c. 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 canonly receive (Figure a). Keyboards and traditional monitors are examples of simplex devices.

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 (Figure b). Walkie-talkies and CB (citizens band) radios are both half- duplex systems.

Full-Duplex

In full-duplex, both stations can transmit and receive simultaneously (Figure c). One common example of full-duplex communication is the telephone network.When two people are communicating by a telephone line, both can talk andlisten at the same time. The full-duplex mode is used when communication inboth directions is required all the time.

Network Criteria

A network must be able to meet a certain number of criteria. The mostimportant 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, andthe 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

Before discussing networks, we need to define some network attributes.

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.

There are two possible types of connections: point-to-point and multipoint. **Point-to-Point** A point-to-point connection provides a dedicated link betweentwo devices. The entire capacity of the link is reserved for transmissionbetween 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 asmicrowave or satellite links, are also possible

When you change television channels by infrared remote control, you are establishing a point-to-point connection between the remote control and the television's control system.

Multipoint A multipoint (also called multi-drop) 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, eitherspatially 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.
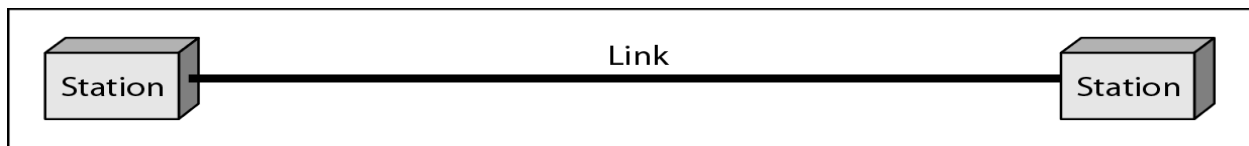
a. Point-to-point
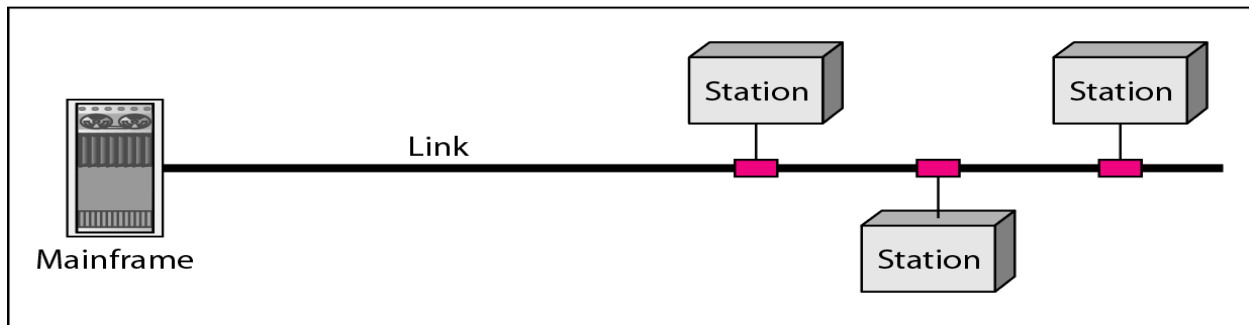
b. Multipoint

Physical Topology

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
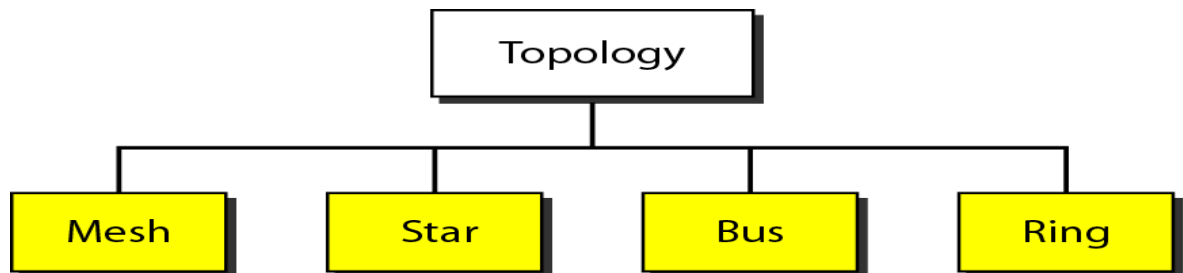
MESH:

A mesh topology is the one where every node is connected to every other nodein the network.
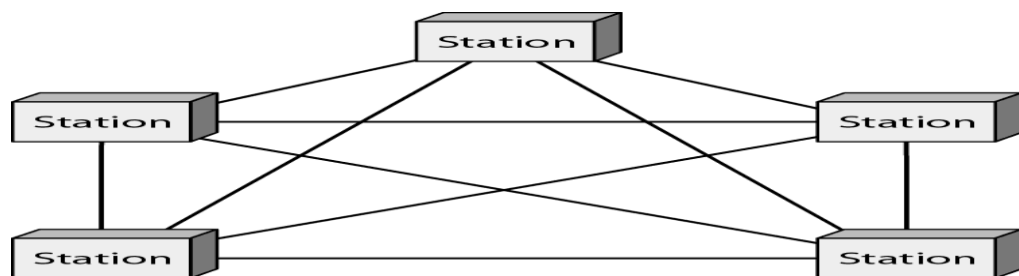
A mesh topology can be a **full mesh topology** or a **partially connected mesh topology**. In a *full mesh topology*, every computer in the network has a connection to each of the other computers in that network. The number of connections in this

network can be calculated using the following formula (**n** is the number ofcomputers in the network): **n(n-1)/2**

In a *partially connected mesh topology*, at least two of the computers in the network have connections to multiple other computers in that network. It is an inexpensive way to implement redundancy in a network. In the event that oneof the primary computers or connections in the network fails, the rest of the network continues to operate normally.

Advantages of a mesh topology

- Can handle high amounts of traffic, because multiple devices can transmitdata simultaneously.
- A failure of one device does not cause a break in the network or transmissionof data.
- Adding additional devices does not disrupt data transmission between otherdevices.

Disadvantages of a mesh topology

- The cost to implement is higher than other network topologies, making it aless desirable option.
- Building and maintaining the topology is difficult and time consuming.
- The chance of redundant connections is high, which adds to the high costsand potential for reduced efficiency.

STAR:

Hub
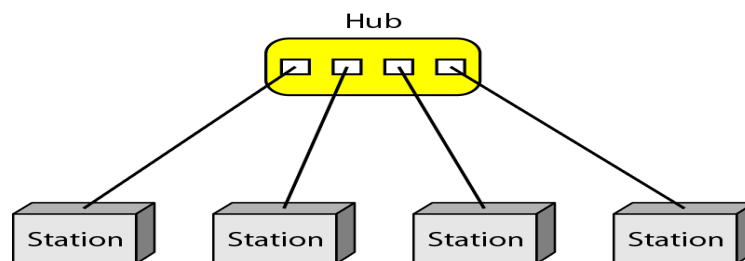
A star network, **star topology** is one of the most common network setups. In this configuration, every node connects to a central network device, likea hub, switch, or computer. The central network device acts as a server and the peripheral devices act as clients. Depending on the type of network card usedin each computer of the star topology, a coaxial cable or a RJ-45 network cableis used to connect computers together.
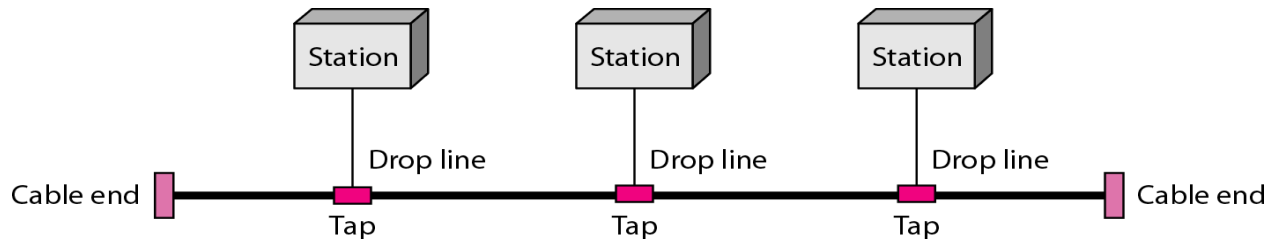
Advantages of star topology

- Centralized management of the network, through the use of the centralcomputer, hub, or switch.
- Easy to add another computer to the network.
- If one computer on the network fails, the rest of the network continues tofunction normally.
- The star topology is used in local-area networks (LANs), High-speed LANsoften use a star topology with a central hub.

Disadvantages of star topology

- Can have a higher cost to implement, especially when using a switch orrouter as the central network device.
- The central network device determines the performance and number ofnodes the network can handle.
- If the central computer, hub, or switch fails, the entire network goes downand all computers are disconnected from the network

BUS:

a **line topology**, a **bus topology** is a network setup in which each computerand network device are connected to a single cable or [backbone](#).

Advantages of bus topology

- It works well when you have a small network.
- It's the easiest network topology for connecting computers or peripheralsin a linear fashion.
- It requires less cable length than a star topology.

Disadvantages of bus topology

- It can be difficult to identify the problems if the whole network goes down.
- It can be hard to troubleshoot individual device issues.
- Bus topology is not great for large networks.
- Terminators are required for both ends of the main cable.
- Additional devices slow the network down.
- If a main cable is damaged, the network fails or splits into two.

RING:
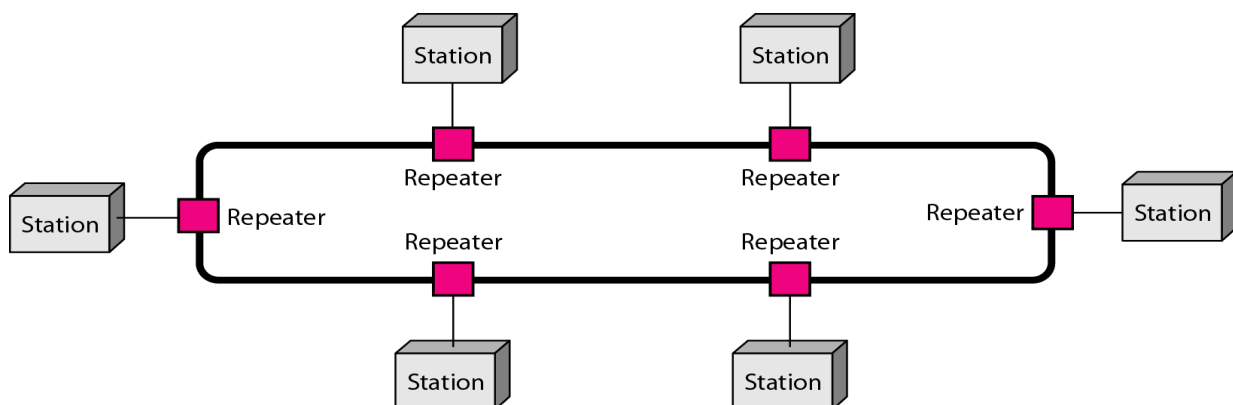
A **ring topology** is a network configuration in which device connections create a circular data path. In a ring network, packets of data travel from one device to the next until they reach their destination. Most ring topologies allow packets to travel only in one direction, called a **unidirectional** ring network. Others permit data to move in either direction, called **bidirectional**.

The major disadvantage of a ring topology is that if any individual connection in the ring is broken, the entire network is affected.

Ring topologies may be used in either local area networks (LANs) or wide area networks (WANs).

Advantages of ring topology

- All data flows in one direction, reducing the chance of packet collisions.
- A network server is not needed to control network connectivity between each workstation.
- Data can transfer between workstations at high speeds.
- Additional workstations can be added without impacting performance of the network.

Disadvantages of ring topology

- All data being transferred over the network must pass through each workstation on the network, which can make it slower than a star topology.
- The entire network will be impacted if one workstation shuts down.
- The hardware needed to connect each workstation to the network is more expensive than Ethernet cards and hubs/switches.

Hybrid Topology A network can be hybrid. For example, we can have a main star topology with each branch connecting several stations in a bus topology as shown in Figure
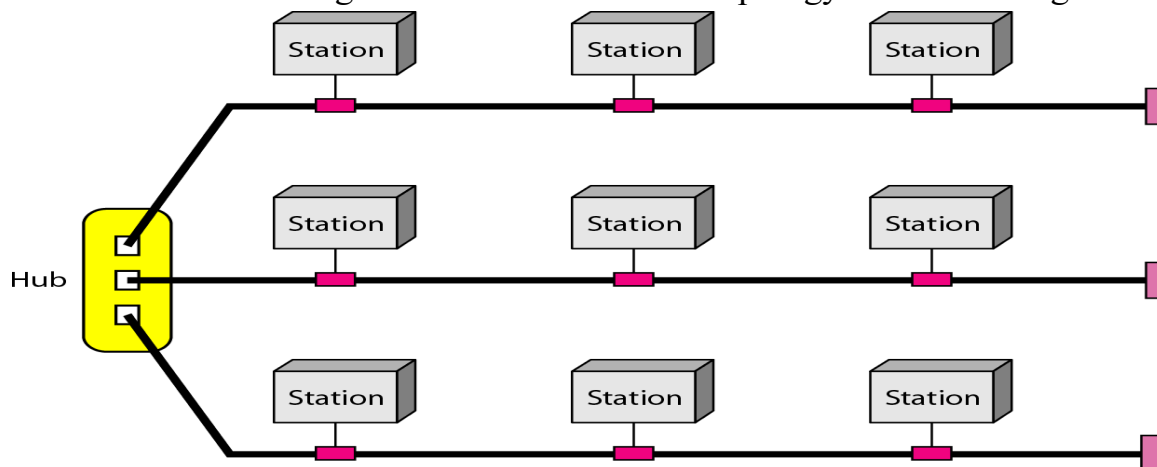
Types of Network based on size

The types of network are classified based upon the size, the area it covers and its physical architecture. The three primary network categories are LAN, WAN and MAN. Each network differs in their characteristics such as distance, transmission speed, cables and cost.

Basic types

LAN (Local Area Network)

Group of interconnected computers within a small area. (room, building, campus)

Two or more pc's can from a LAN to share files, folders, printers, applicationsand other devices.

Coaxial or CAT 5 cables are normally used for connections.Due to short

distances, errors and noise are minimum.

Data transfer rate is 10 to 100 mbps.Example: A

computer lab in a school. **MAN (Metropolitan**

Area Network) Design to extend over a large

area.

Connecting number of LAN's to form larger network, so that resources can beshared.

Networks can be up to 5 to 50 km. Owned by

organization or individual. Data transfer rate is low

compare to LAN.

Example: Organization with different branches located in the city.

WAN (Wide Area Network)

Are country and worldwide network.Contains

multiple LAN's and MAN's.

Distinguished in terms of geographical range.Uses satellites

and microwave relays.

Data transfer rate depends upon the ISP provider and varies over the location.Best example is the internet.

Other types

WLAN (Wireless LAN)

A LAN that uses high frequency radio waves for communication. Provides short range

connectivity with high speed data transmission.**PAN (Personal Area Network)**

Network organized by the individual user for its personal use.
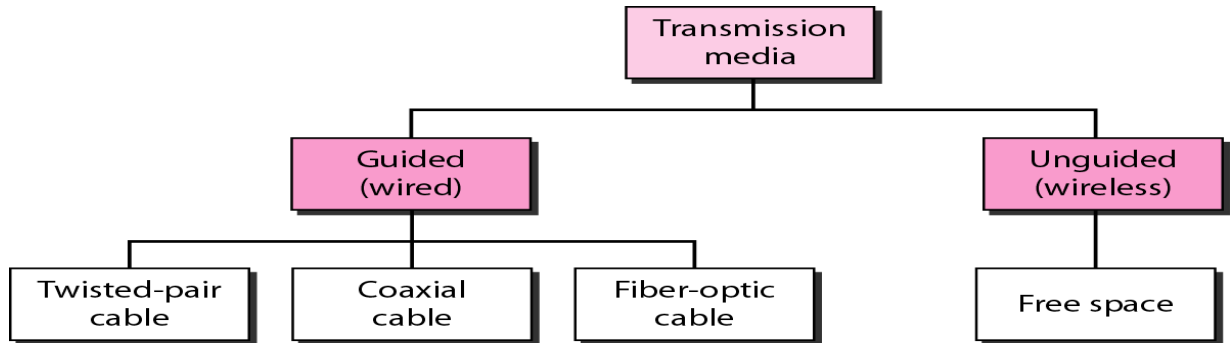
SAN (Storage Area Network)

Connects servers to data storage devices via fiber-optic cables.E.g.: Used for daily

backup of organization or a mirror copy

A **transmission medium** can be broadly defined as anything that can carryinformation from a source to a destination.
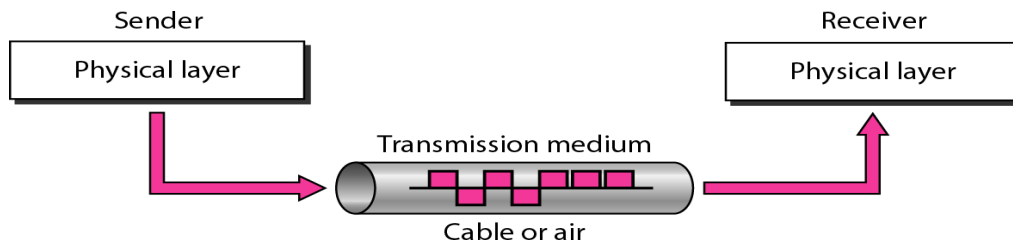
Classes of transmission media

Guided Media: Guided media, which are those that provide a medium from one device to another, include twisted-pair cable, coaxial cable, and fiber-optic cable.

Twisted-Pair Cable: A twisted pair consists of two conductors (normally copper), each with its own plastic insulation, twisted together. One of the wires is used to carry signals to the receiver, and the other is used only as a ground reference.
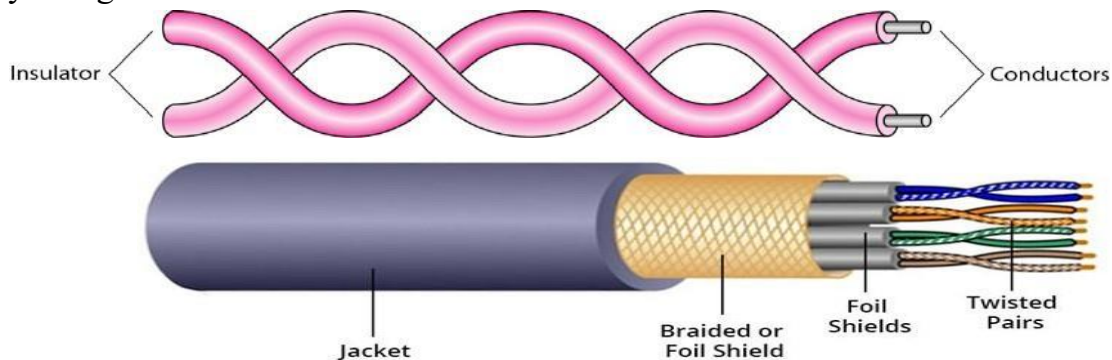
Unshielded Versus Shielded Twisted-Pair Cable

The most common twisted-pair cable used in communications is referred to as unshielded twisted-pair (UTP). STP cable has a metal foil or braided mesh covering that encases each pair of insulated conductors. Although metal casing improves the quality of cable by preventing the penetration of noise or crosstalk, it is bulkier and more expensive.
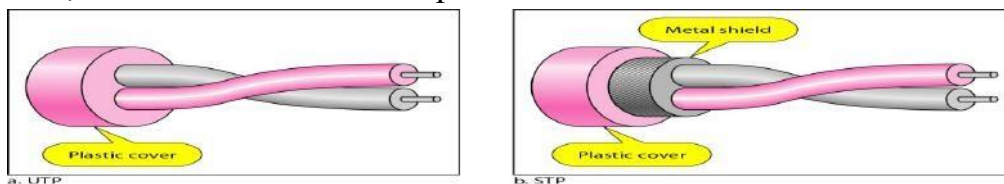

The most common UTP connector is RJ45 (RJ stands for registered jack)

Twisted-pair cables are used in telephone lines to provide voice and datachannels.
Local-area networks, such as l0Base-T and l00Base-T, also use twisted-paircables.

Coaxial Cable

Coaxial cable (or *coax*) carries signals of higher frequency ranges than those in twisted pair cable. coax has a central core conductor of solid or stranded wire (usuallycopper) enclosed in an insulating sheath, which is, in turn, encased inan outer conductor of metal foil, braid, or a combination of the two. The outer metallic wrapping serves both as a shield against noise and as the secondconductor, which completes the circuit.This outer conductor is also enclosed in an insulating sheath, and the whole cable is protected by a plastic cover.
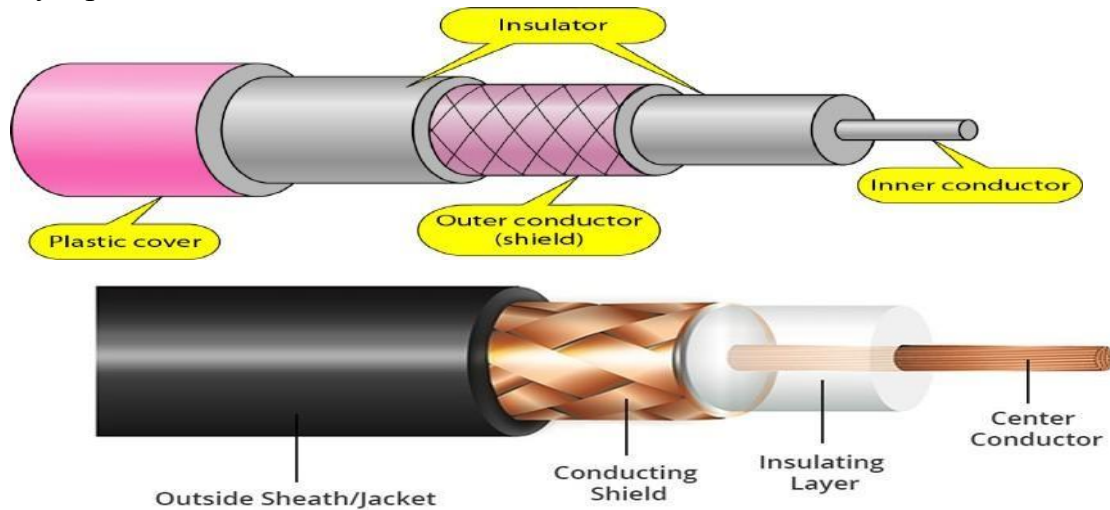
The most common type of connector used today is the Bayone-Neill-Concelman(BNe), connector.

Applications
Coaxial cable was widely used in analog telephone networks,digital telephonenetworks
Cable TV networks also use coaxial cables.
Another common application of coaxial cable is in traditional Ethernet LANs

Fiber-Optic Cable

A fiber-optic cable is made of glass or plastic and transmits signals in the formof light. Light travels in a straight line as long as it is moving through a single uniform substance.
If a ray of light traveling through one substance suddenly enters another substance(of a different density), the ray changes direction.
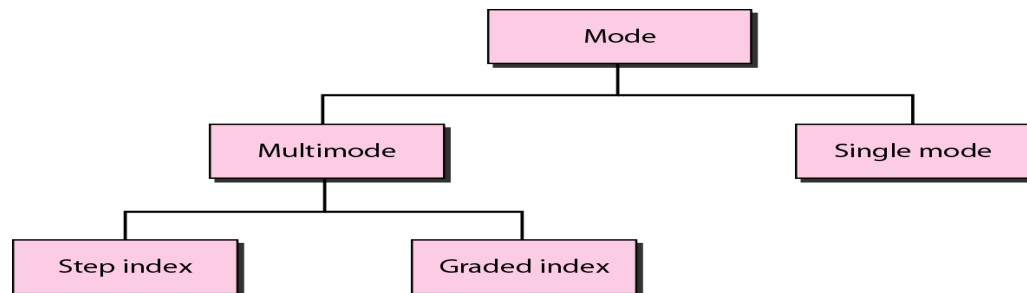*Bending of light ray*

| Less dense		Less dense		Less dense	
More dense		More dense		More dense	
I < critical angle, refraction		I = critical angle, refraction		I > critical angle, reflection	
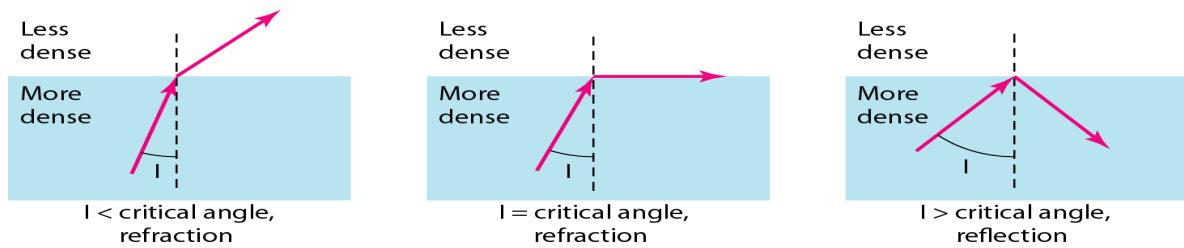
Optical fibers use reflection to guide light through a channel. A glass or plasticcore is surrounded by a cladding of less dense glass or plastic.
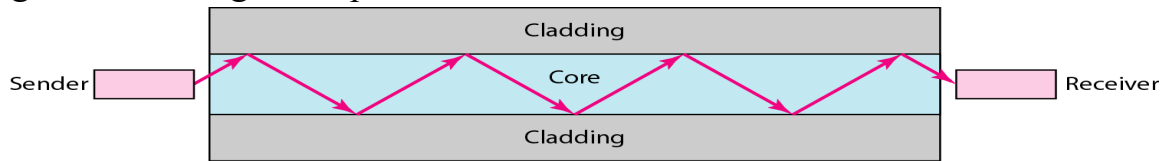
Propagation Modes

Multimode is so named because multiple beams from a light source move through the core in different paths. How these beams move within the cable depends on the structure of the core, as shown in Figure.

a. Multimode, step index

b. Multimode, graded index

c. Single mode
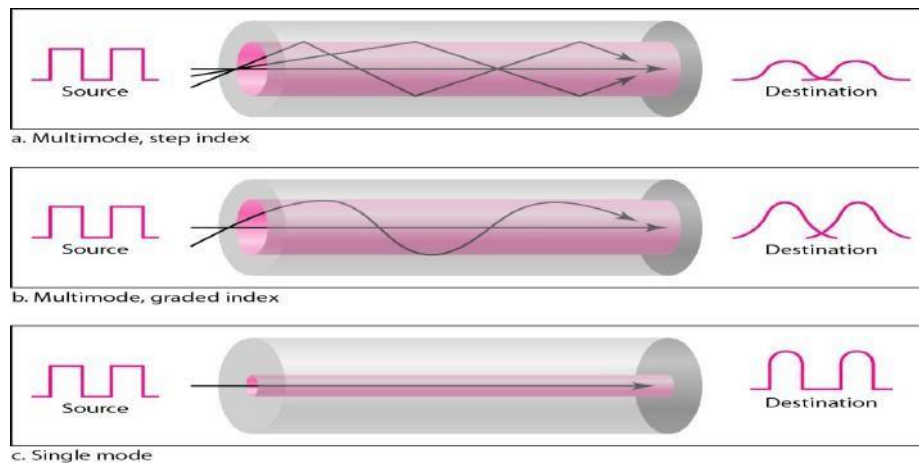
In **multimode step-index fiber**, the density of the core remains constant from the center to the edges. A beam of light moves through this constant density ina straight line until it reaches the interface of the core and the cladding. The term *step index* refers to the suddenness of this change, which contributes to the distortion of the signal as it passes through the fiber.

A second type of fiber, called **multimode graded-index fiber**, decreases this distortion of the signal through the cable. The word *index* here refers to the index of refraction.

Single-Mode: Single-mode uses step-index fiber and a highly focused sourceof light that limits beams to a small range of angles, all close to the horizontal.

<u>Fiber Construction</u>
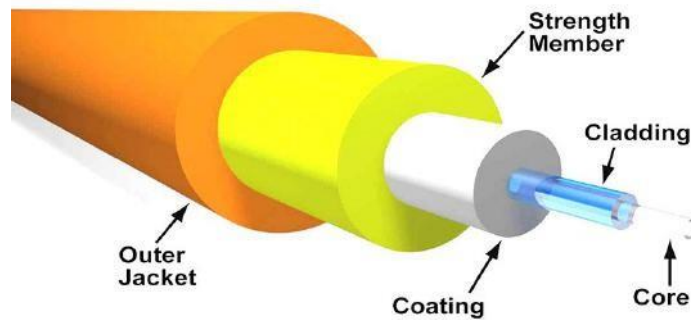
The **subscriber channel** (SC) **connector,** The **straight-tip** (ST) **connector,MT-RJ(mechanical transfer registered jack)** is a connector

Applications

Fiber-optic cable is often found in backbone networks because its wide bandwidth is cost-effective..

Some cable TV companies use a combination of optical fiber and coaxialcable,thus creating a hybrid network.

Local-area networks such as 100Base-FX network (Fast Ethernet) and 1000Base-X also use fiber-optic cable

Advantages and Disadvantages of Optical Fiber

Advantages Fiber-optic cable has several advantages over metallic cable(twisted pair or coaxial).

1 Higher bandwidth.

2 Less signal attenuation. Fiber-optic transmission distance is significantly greaterthan that of other guided media. A signal can run for 50 km without requiring regeneration. We need repeaters every 5 km for coaxial or twisted-pair cable.

3 Immunity to electromagnetic interference. Electromagnetic noise cannot affect fiber-optic cables.

4 Resistance to corrosive materials. Glass is more resistant to corrosive materials than copper.

5 Light weight. Fiber-optic cables are much lighter than copper cables.

6 Greater immunity to tapping. Fiber-optic cables are more immune to tapping than copper cables. Copper cables create antenna effects that can easily be tapped.

Disadvantages There are some disadvantages in the use of optical fiber.1Installation and maintenance

2 Unidirectional light propagation. Propagation of light is unidirectional. If weneed bidirectional communication, two fibers are needed.

3 Cost. The cable and the interfaces are relatively more expensive than those of other guided media. If the demand for bandwidth is not high, often the use of optical fiber cannot be justified.
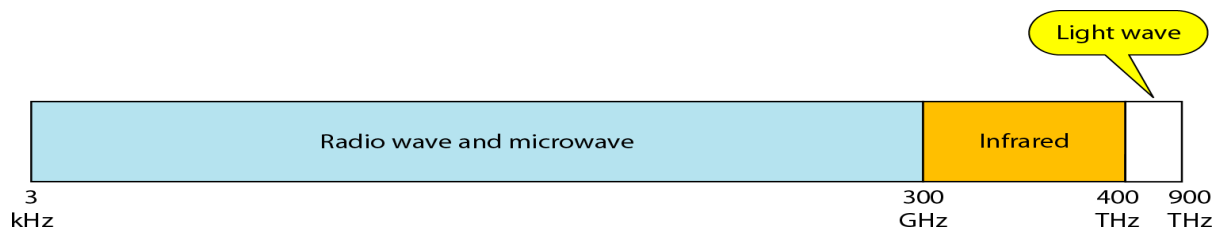

UNGUIDED MEDIA: WIRELESS

Unguided media transport electromagnetic waves without using a physical conductor. This type of communication is often referred to as wireless communication.
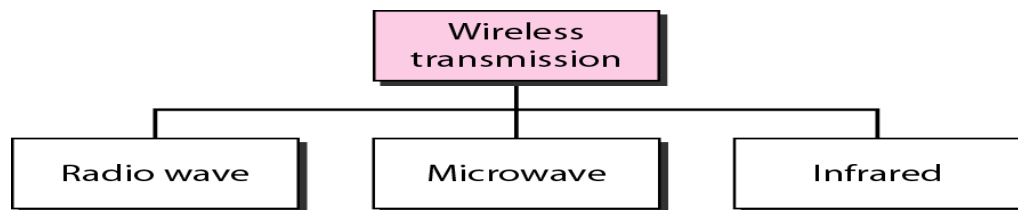
Radio Waves

Microwaves

Infrared

Unguided signals can travel from the source to destination in several ways: ground propagation, sky propagation, and line-of-sight propagation, as shown in Figure

Ground propagation (below 2 MHz)

Sky propagation (2–30 MHz)

Line-of-sight propagation (above 30 MHz)
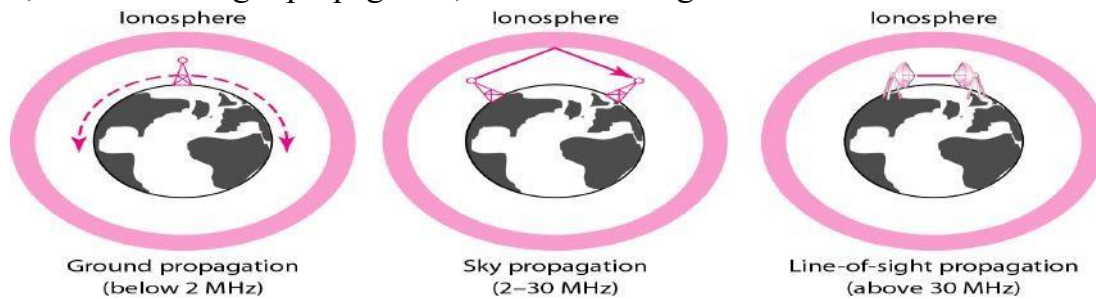
Radio Waves

Electromagnetic waves ranging in frequencies between 3 kHz and 1 GHz are normally called radio waves. Radio waves are omni directional. When an antenna transmits radio waves, they are propagated in all directions. This means that the sending and receiving antennas do not have to be aligned. A sending antenna sends waves that can be received by any receiving antenna.The omni directional property has a disadvantage, too. The radio waves transmitted by one antenna are susceptible to interference by another antenna that may send signals using the same frequency or band.

Omni directional Antenna

Radio waves use omnidirectional antennas that send out signals in all directions. Based on the wavelength, strength, and the purpose of transmission, we can have several types of antennas. Figure shows an omnidirectional antenna.
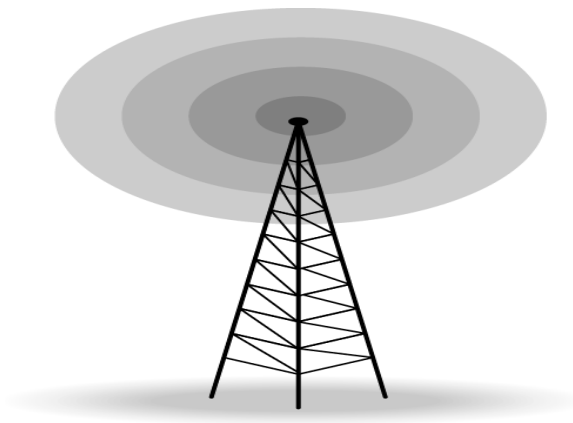
Applications

The Omni directional characteristics of radio waves make them useful for multicasting, in which there is one sender but many receivers. AM and FM radio, television, maritime radio, cordless phones, and paging are examples of multicasting.

Microwaves

Electromagnetic waves having frequencies between 1 and 300 GHz are called microwaves. Microwaves are unidirectional. The sending and receiving antennas need to be aligned. The unidirectional property has an obvious advantage. A pair of antennas can be aligned without interfering with another pair of aligned antennas

Unidirectional Antenna

Microwaves need unidirectional antennas that send out signals in one direction. Two types of antennas are used for microwave communications: the parabolic dish and the horn
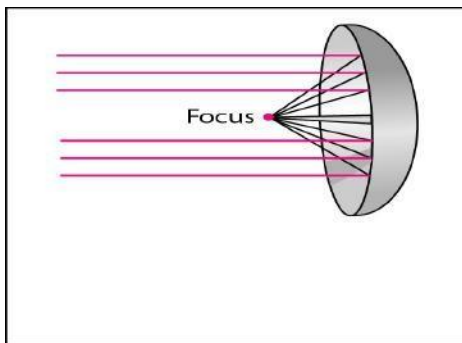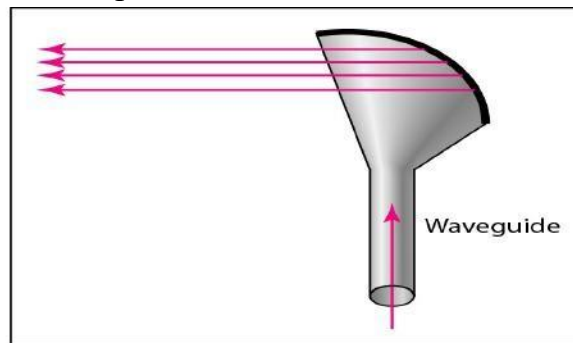
a. Dish antenna   b. Horn antenna

Applications:

Microwaves are used for unicast communication such as cellular telephones, satellite networks, and wireless LANs

Infrared

Infrared waves, with frequencies from 300 GHz to 400 THz (wavelengths from 1 mm to 770 nm), can be used for short-range communication. Infrared waves, having high frequencies, cannot penetrate walls. This advantageous

characteristic prevents interference between one system and another; a short- range communication system in one room cannot be affected by another system in the next room.

When we use our infrared remote control, we do not interfere with the use ofthe remote by our neighbors. Infrared signals useless for long-range communication. In addition, we cannot use infrared waves outside a building because the sun's rays contain infrared waves that can interfere with the communication.

Applications:

Infrared signals can be used for short-range communication in a closedarea using line-of-sight propagation.

Switching

A network is a set of connected devices. Whenever we have multiple devices, we have the problem of how to connect them to make one-to-one communication possible. One solution is to make a point-to-point connection between each pair of devices (a mesh topology) or between a central deviceand every other device (a star topology). These methods, however, are impractical and wasteful when applied to very large networks.

The number and length of the links require too much infrastructure to be cost-efficient, and the majority of those links would be idle most of the time.

A better solution is switching. A switched network consists of a series of interlinked nodes, called switches. Switches are devices capable of creating temporary connections between two or more devices linked to the switch. In a switched network, some of these nodes are connected to the end systems (computers or telephones, for example). Others are used only for routing. Figure shows a switched network.
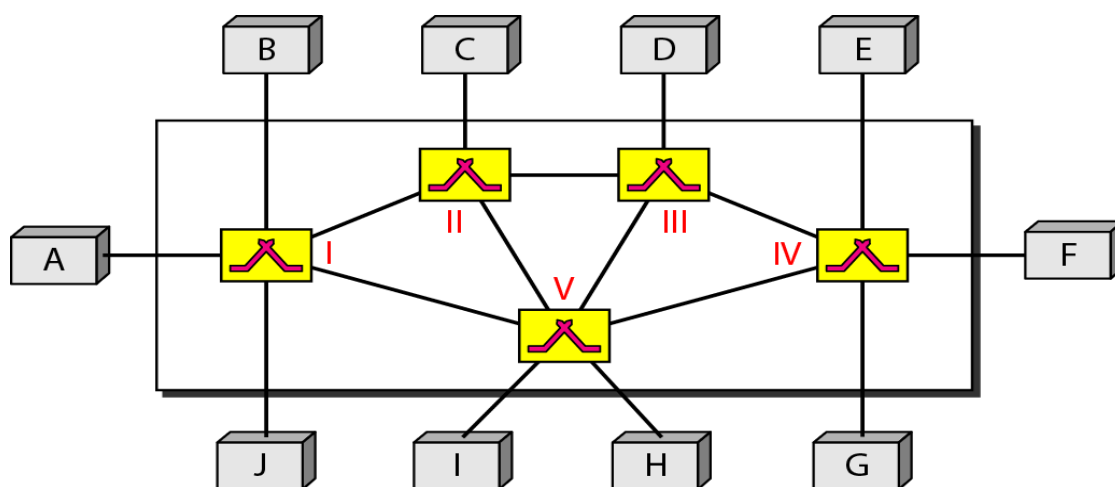
We can then divide today's networks into three broad categories: circuit- switched networks, packet-switched networks, and message-switched. Packet- switched networks can further be divided into two subcategories-virtual-circuit networks and datagram networks as shown in Figure.
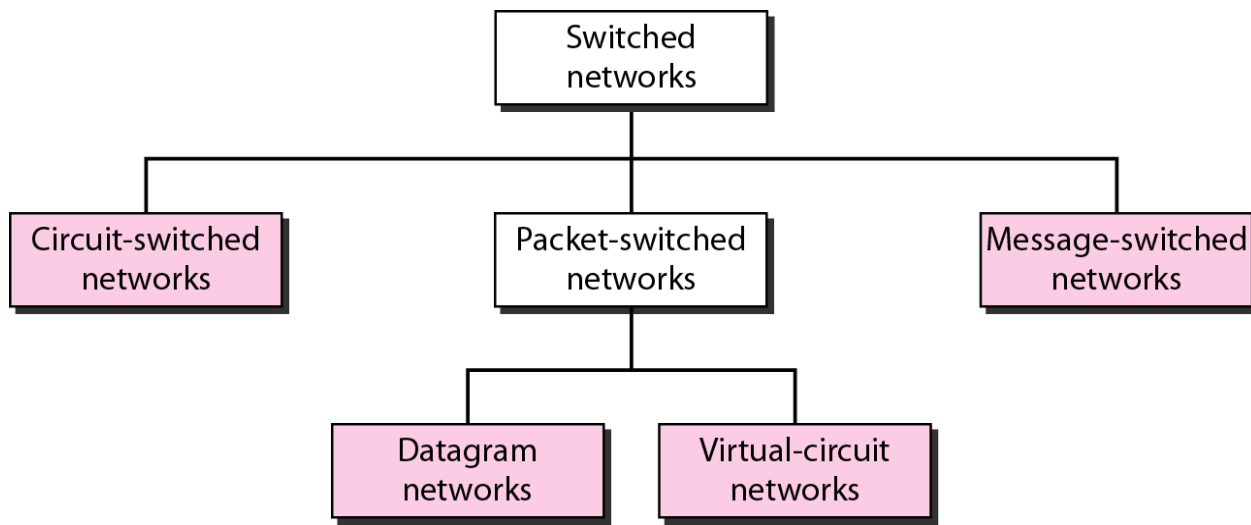
CIRCUIT-SWITCHED NETWORKS

A circuit-switched network consists of a set of switches connected byphysical links. A connection between two stations is a dedicated path made ofone or more links. However, each connection uses only one dedicated channelon each link. Each link is normally divided into n channels by using FDM or TDM.

In circuit switching, the resources need to be reserved during the setup phase; the resources remain dedicated for the entire duration of data transfer until theteardown phase
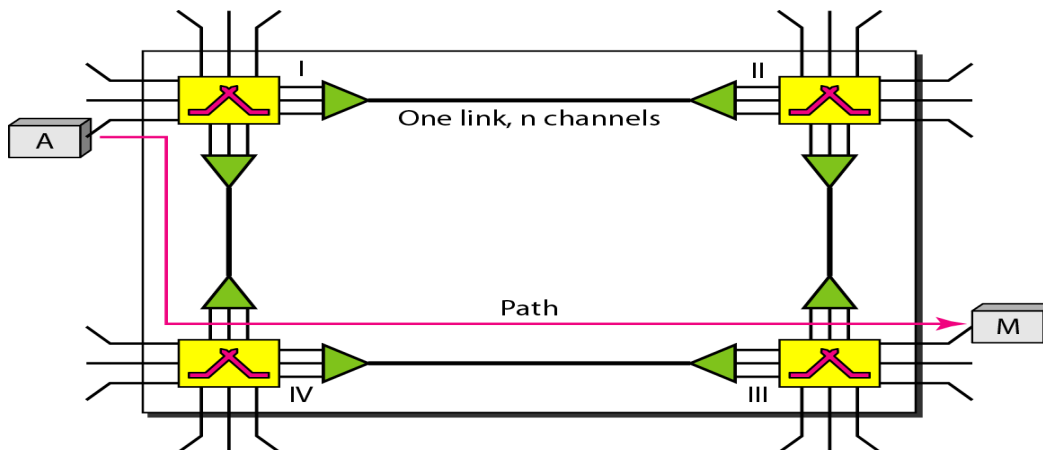
Three Phases

The actual communication in a circuit-switched network requires three phases:connection setup, data transfer, and connection teardown.

Setup Phase

Before the two parties (or multiple parties in a conference call) cancommunicate, a dedicated circuit (combination of channels in links) needs to be established. Connection setup means creating dedicated channels between the switches. For example, in Figure, when system A needs to connect to system M,it sends a setup request that includes the address of system M, to switch I.Switch I finds a channel between itself and switch IV that can be dedicated for this purpose. Switch I then sends the request to switch IV, which finds a

dedicated channel between itself and switch III. Switch III informs system M of system A's intention at this time.

In the next step to making a connection, an acknowledgment from systemM needs to be sent in the opposite direction to system A. Only after system A receives this acknowledgment is the connection established.

Data Transfer Phase

After the establishment of the dedicated circuit (channels), the two parties cantransfer data.

Teardown Phase

When one of the parties needs to disconnect, a signal is sent to each switch torelease the resources.

Efficiency

It can be argued that circuit-switched networks are not as efficient as the other two types of networks because resources are allocated during the entire duration of the connection. These resources are unavailable to otherconnections.

Delay

Although a circuit-switched network normally has low efficiency, the delay inthis type of network is minimal. During data transfer the data are not delayedat each switch; the resources are allocated for the duration of the connection.

The total delay is due to the time needed to create the connection, transfer data, and disconnect the circuit.

Switching at the physical layer **in the traditional telephone network** uses **the circuit-switching approach.**

DATAGRAM NETWORKS

In a packet-switched network, there is no resource reservation; resources are allocated on demand. The allocation is done on a first come, first-served basis. When a switch receives a packet, no matter what is the source or destination, the packet must wait if there are other packets being processed. This lack of reservation may create delay. For example, if we do not have a reservation at a restaurant, we might have to wait.

In a datagram network, each packet is treated independently of all others. Packets in this approach are referred to as datagrams. Datagram switching is normally done at the network layer.

Figure shows how the datagram approach is used to deliver four packets from station A to station X. The switches in a datagram network are traditionallyreferred to as routers.

The datagram networks are sometimes referred to as connectionless networks. The term *connectionless* here means that the switch (packet switch) does not keep information about the connection state. There are no setup or teardown phases. Each packet is treated the same by a switch regardless of its source or destination.

A switch in a datagram network uses a routing table that is based on the destination address. The destination address in the header of a packet in a datagram network remains the same during the entire journey of the packet.
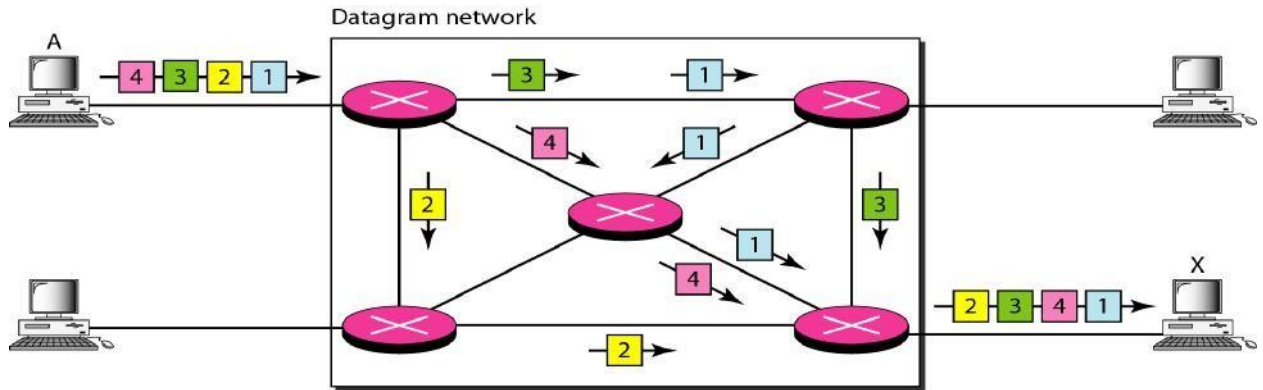
Datagram network

Efficiency

The efficiency of a datagram network is better than that of a circuit-switchednetwork; resources are allocated only when there are packets to be transferred. **Delay**

There may be greater delay in a datagram network than in a virtual-circuit network. Although there are no setup and teardown phases, each packet may experience a wait at a switch before it is forwarded. In addition, since not all packets in a message necessarily travel through the same switches, the delay is not uniform for the packets of a message.

Switching in the Internet is done by using the datagram approach topacket switching at the network layer.

VIRTUAL-CIRCUIT NETWORKS

A virtual-circuit network is a cross between a circuit-switched network and a datagram network. It has some characteristics of both.
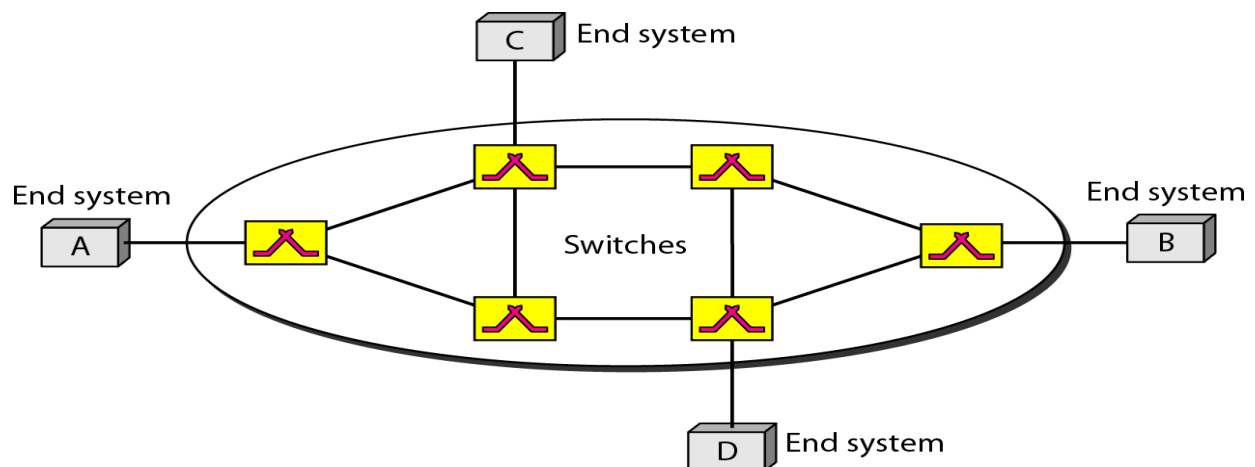
1.   As in a circuit-switched network, there are setup and teardown phases in addition to the data transfer phase.

2.   Resources can be allocated during the setup phase, as in a circuit-switched network, or on demand, as in a datagram network.

3.   As in a datagram network, data are packetized and each packet carries an address in the header. However, the address in the header has local jurisdiction (it defines what should be the next switch and the channel on which the packetis being carried), not end-to-end jurisdiction.

4.   As in a circuit-switched network, all packets follow the same path established during the connection.

5.   A virtual-circuit network is normally implemented in the data link layer, whilea circuit-switched network is implemented in the physical layer and a datagram network in the network layer.

Addressing

In a virtual-circuit network, two types of addressing are involved: global andlocal (virtual-circuit identifier).

Global Addressing

A source or a destination needs to have a global address-an address that can beunique in the scope of the network.

Virtual-Circuit Identifier

The identifier that is actually used for data transfer is called the virtual-circuit identifier (VCI). A VCI, unlike a global address, is a small number that has only switch scope; it is used by a frame between two switches. When a frame arrives at a switch, it has a VCI; when it leaves, it has a different VCl.

Figure shows how the VCI in a data frame changes from one switch to another. Note that a VCI does not need to be a large number since each switch can useits own unique set of VCls.
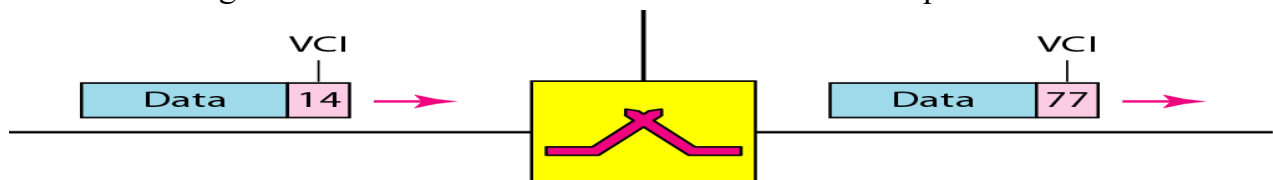
Three Phases

Three phases in a virtual-circuit network: setup, data transfer, and teardown. We first discuss the data transfer phase, which is more straightforward; we thentalk about the setup and teardown phases.

Data Transfer Phase

Incoming		Outgoing	
Port	VCI	Port	VCI
1	14	3	22
1	77	2	41
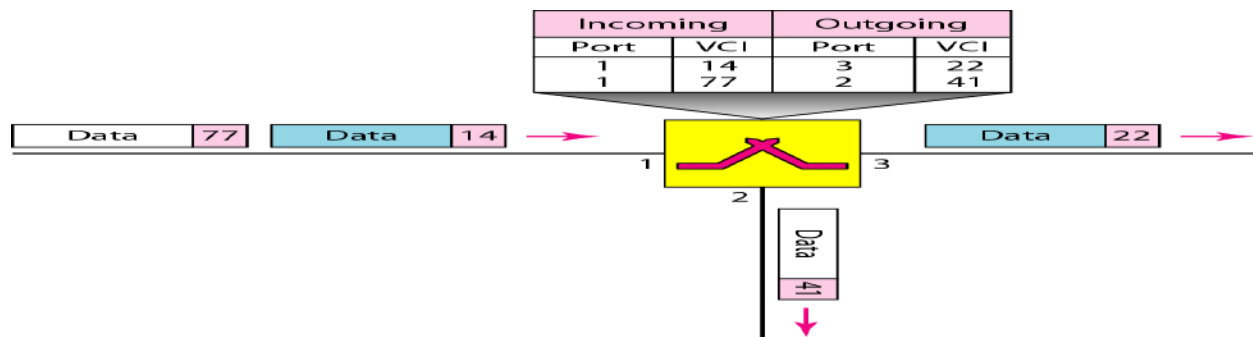
To transfer a frame from a source to its destination, all switches need to have a table entry for this virtual circuit. The table, in its simplest form, has fourcolumns.

We show later how the switches make their table entries, but for the moment we assume that each switch has a table with entries for all active virtual circuits. Figure shows such a switch and its corresponding table.

Figure shows a frame arriving at port 1 with a VCI of 14. When the frame arrives, the switch looks in its table to find port 1 and a VCI of 14. When it is found, the switch knows to change the VCI to 22 and send out the frame from port 3.

Figure shows how a frame from source A reaches destination B and how its VCI changes during the trip.

Incoming		Outgoing	
Port	VCI	Port	VCI
1	14	3	66

Incoming		Outgoing	
Port	VCI	Port	VCI
2	22	3	77

Incoming		Outgoing	
Port	VCI	Port	VCI
1	66	2	22
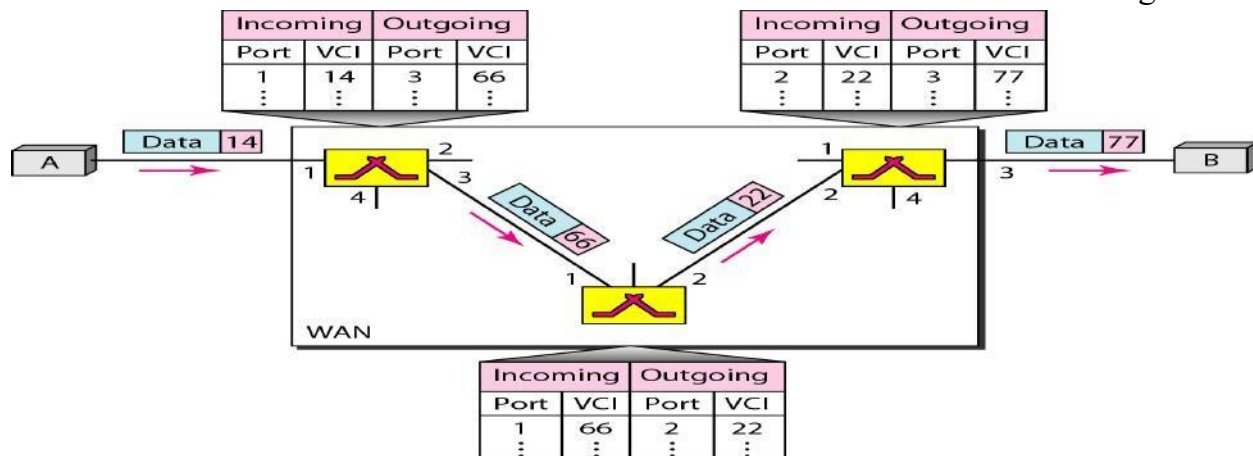
Each switch changes the VCI and routes the frame.

The data transfer phase is active until the source sends all its frames tothe destination. The procedure at the switch is the same for each frame of a message. The process creates a virtual circuit, not a real circuit, between the source and destination.

Setup Phase

In the setup phase, a switch creates an entry for a virtual circuit. For example, suppose source A needs to create a virtual circuit to B. Two steps are required: the setup request and the acknowledgment.

Setup Request A setup request frame is sent from the source to the destination. Figure shows the process.

Switch 1 (setup)

Incoming		Outgoing	
Port	VCI	Port	VCI
1	14	3	

Switch 3 (setup)

Incoming		Outgoing	
Port	VCI	Port	VCI
2	22	3	

VCI = 77

A → Switch 1 (port 1, port 3) → Switch 2 (port 1, port 2) → Switch 3 (port 2, port 3) → B

Switch 2 (setup)

Incoming		Outgoing	
Port	VCI	Port	VCI
1	66	2	
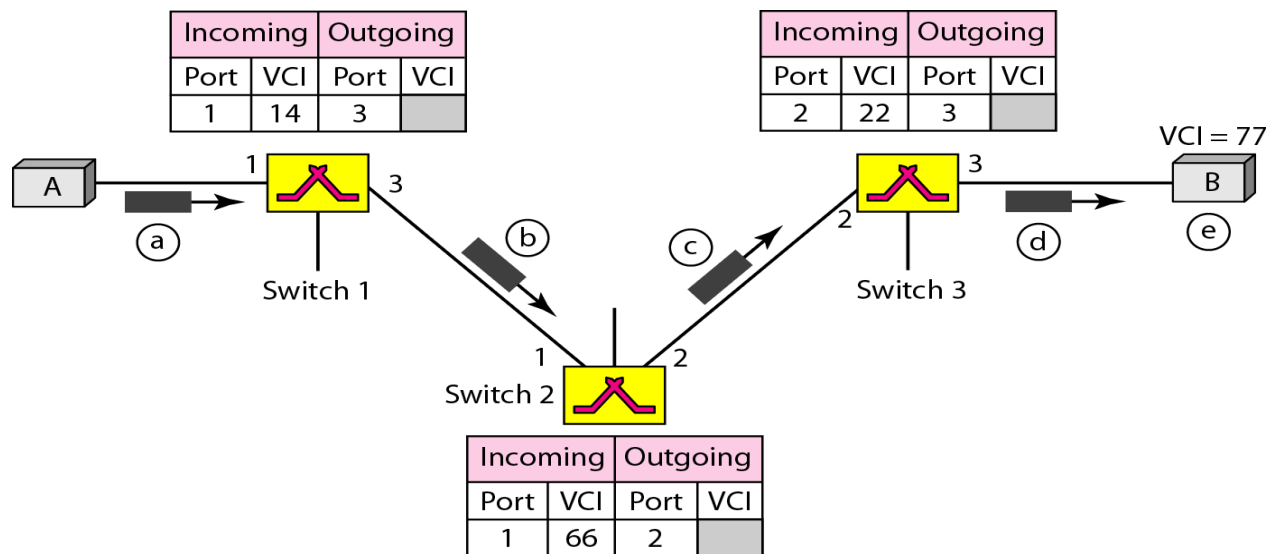
a. Source A sends a setup frame to switch 1.

b.   Switch 1 receives the setup request frame. It knows that a frame going fromA to B goes out through port 3. For the moment, assume that it knows the output port. The switch creates an entry in its table for this virtual circuit, but itis only able to fill three of the four columns. The switch assigns the incoming port (1) and chooses an available incoming VCI (14) and the outgoing port (3). Itdoes not yet know the outgoing VCI, which will be found during the acknowledgment step. The switch then forwards the frame through port 3 to switch 2.
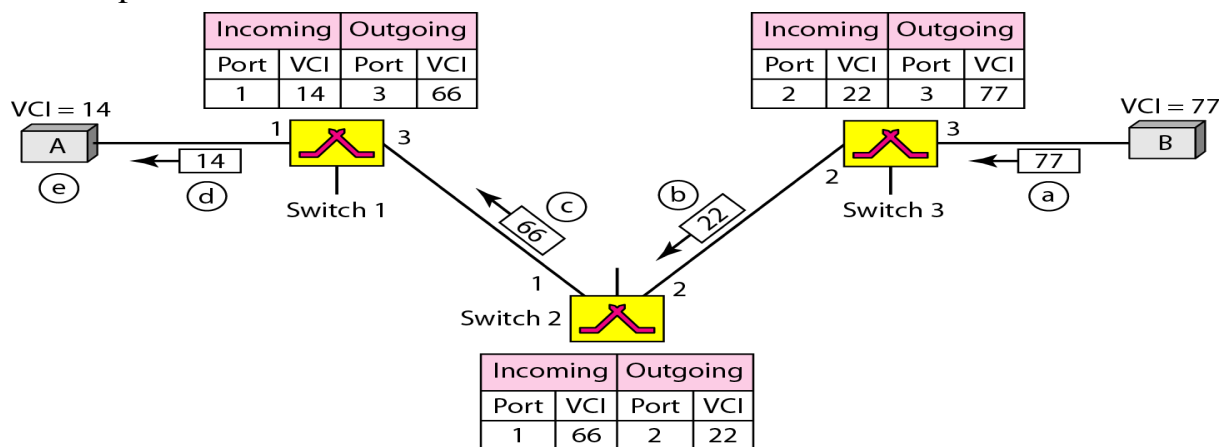
c.   Switch 2 receives the setup request frame. The same events happen here asat switch 1; three columns of the table are completed: in this case, incoming port (l), incoming VCI (66), and outgoing port (2).

d.   Switch 3 receives the setup request frame. Again, three columns are completed: incoming port (2), incoming VCI (22), and outgoing port (3).

e.   Destination B receives the setup frame, and if it is ready to receive frames from A, it assigns a VCI to the incoming frames that come from A, in this case

77. This VCI lets the destination know that the frames come from A, and not other sources.

<u>Acknowledgment</u> A special frame, called the acknowledgment frame, completes the entries in the switching tables.

Figure shows the process.

Switch 1 (acknowledgment)

Incoming		Outgoing	
Port	VCI	Port	VCI
1	14	3	66

VCI = 14

Switch 3 (acknowledgment)

Incoming		Outgoing	
Port	VCI	Port	VCI
2	22	3	77

VCI = 77

Switch 2 (acknowledgment)

Incoming		Outgoing	
Port	VCI	Port	VCI
1	66	2	22

a.   The destination sends an acknowledgment to switch 3. The acknowledgmentcarries the global source and destination addresses so the switch knows whichentry in the table is to be completed. The frame also carries VCI 77, chosen bythe destination as the incoming VCI for frames from A. Switch 3 uses this VCI tocomplete the outgoing VCI column for this entry. Note that 77 is the incomingVCI for destination B, but the outgoing VCI for switch 3.

b.   Switch 3 sends an acknowledgment to switch 2 that contains its incoming VCIin the table, chosen in the previous step. Switch 2 uses this as the outgoing VCIin the table.

c.   Switch 2 sends an acknowledgment to switch 1 that contains its incoming VCIin the table, chosen in the previous step. Switch 1 uses this as the outgoing VCIin the table.

d.   Finally switch 1 sends an acknowledgment to source A that contains its incoming VCI in the table, chosen in the previous step.

e.   The source uses this as the outgoing VCI for the data frames to be sent to destination B.

Teardown Phase

In this phase, source A, after sending all frames to B, sends a special frame called a *teardown request.* Destination B responds with a teardown confirmation frame. All switches delete the corresponding entry from their tables.

Efficiency

In virtual-circuit switching, all packets belonging to the same source and destination travel the same path; but the packets may arrive at the destination with different delays if resource allocation is on demand.

Delay

In a virtual-circuit network, there is a one-time delay for setup and a one-time delay for teardown. If resources are allocated during the setup phase, there isno wait time for individual packets. Figure shows the delay for a packet traveling through two switches in a virtual-circuit network
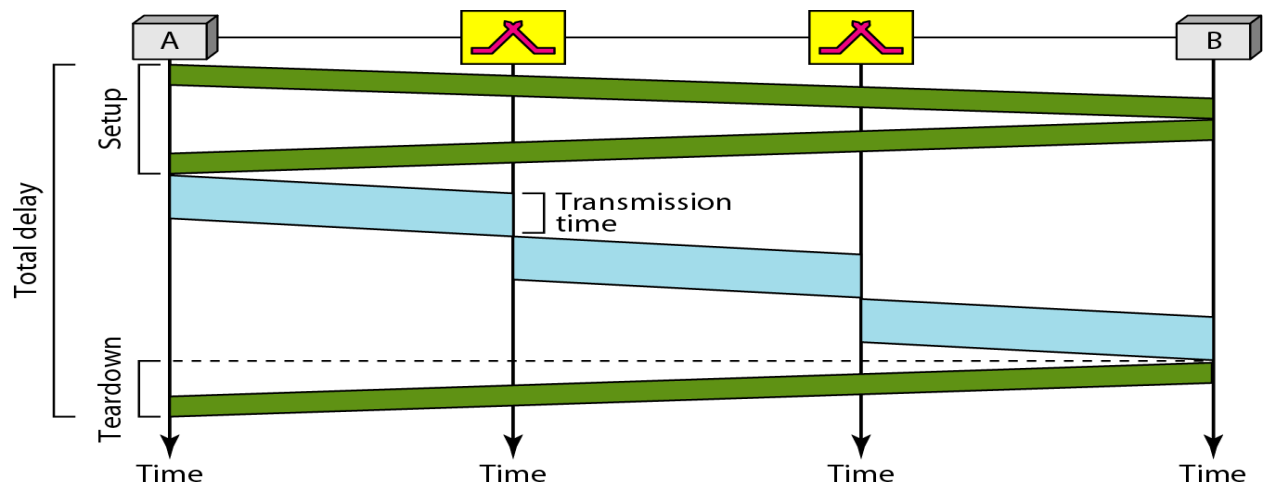
Switching at the data link layer in a switched WAN is normally implemented byusing virtual-circuit techniques.

Comparison

Issue	Datagram network	Virtual-circuit network
Circuit setup	Not needed	Required
Addressing	Each packet contains the full source and destination address	Each packet contains a short VC number
State information	Routers do not hold state information about connections	Each VC requires router table space per connection
Routing	Each packet is routed independently	Route chosen when VC is set up; all packets follow it
Effect of router failures	None, except for packets lost during the crash	All VCs that passed through the failed router are terminated
Quality of service	Difficult	Easy if enough resources can be allocated in advance for each VC
Congestion control	Difficult	Easy if enough resources can be allocated in advance for each VC

Diagrams from Tanenbaum Textbook
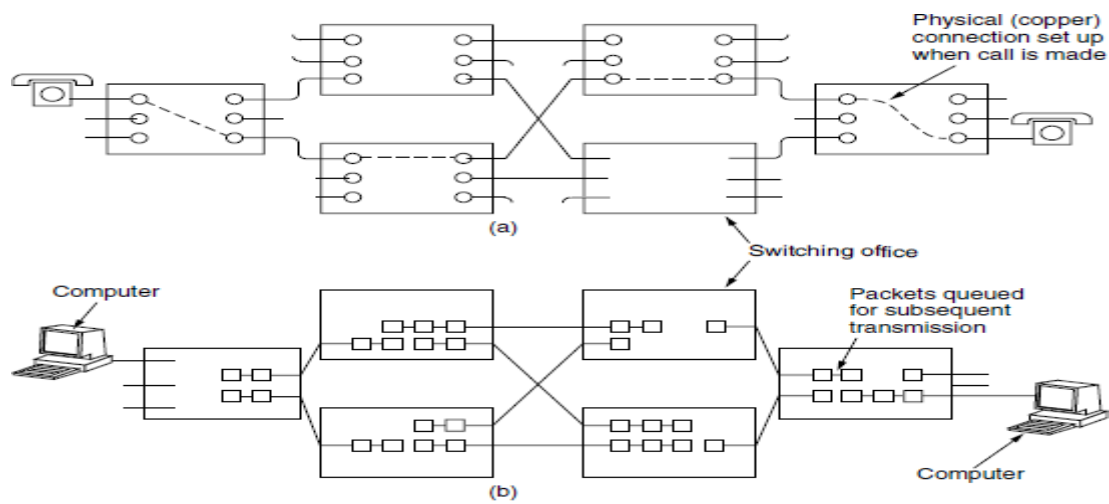
Figure 2-42. (a) Circuit switching. (b) Packet switching.
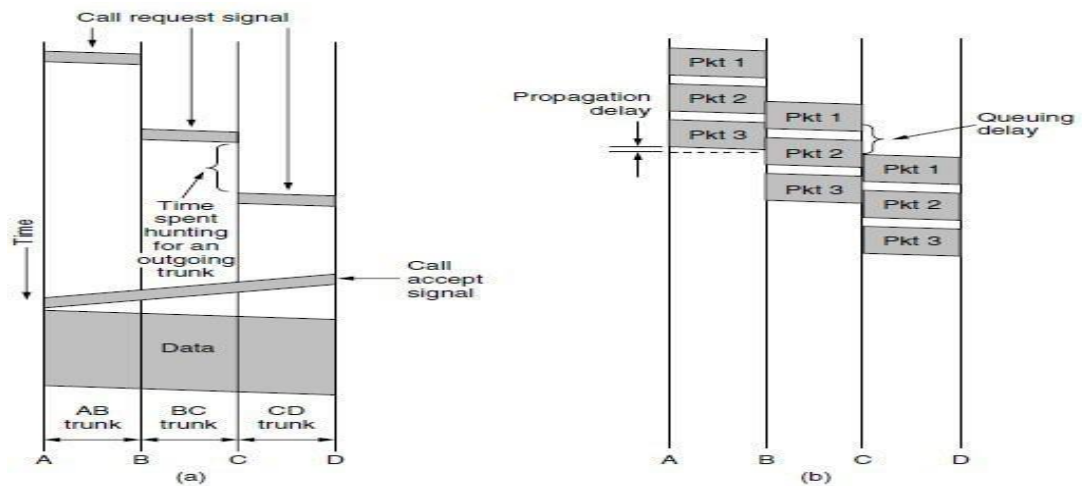
Figure 2-43. Timing of events in (a) circuit switching, (b) packet switching.

OSI

- OSI stands for Open Systems Interconnection
- Created by International Standards Organization (ISO)
- Was created as a framework and reference model to explain how differentnetworking technologies work together and interact
- It is not a standard that networking protocols must follow
- Each layer has specific functions it is responsible for
- All layers work together in the correct order to move data around a network

7	Application
6	Presentation
5	Session
4	Transport
3	Network
2	Data link
1	Physical
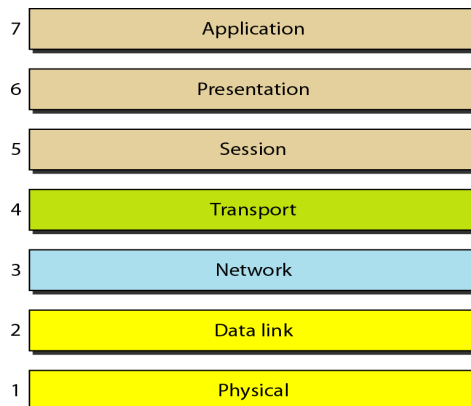
Top to bottom
–All People Seem To Need Data ProcessingBottom to top
–Please Do Not Throw Sausage Pizza Away
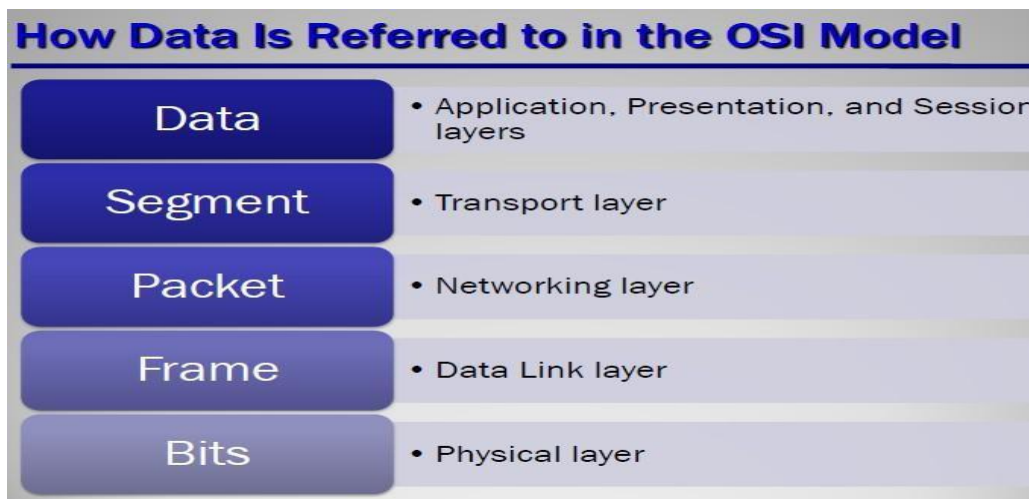
Physical Layer

- Deals with all aspects of physically moving data from one computer to the next
- Converts data from the upper layers into 1s and 0s for transmission over media
- Defines how data is encoded onto the media to transmit the data
- Defined on this layer: Cable standards, wireless standards, and fiber opticstandards. Copper wiring, fiber optic cable, radio frequencies, anything that can be used totransmit data is defined on the Physical layer of the OSI Model
- Device example: Hub
- Used to transmit data

Data Link Layer

- Is responsible for moving frames from node to node or computer to computer
- Can move frames from one adjacent computer to another, cannot move framesacross routers
- Encapsulation = frame
- Requires MAC address or *physical address*
- Protocols defined include Ethernet Protocol and Point-to-Point Protocol (PPP)
- Device example: Switch
- Two sublayers: Logical Link Control (LLC) and the Media Access Control (MAC)
o Logical Link Control (LLC)
▪ –Data Link layer addressing, flow control, address notification, error control
o Media Access Control (MAC)
▪ –Determines which computer has access to the network media at any giventime
▪ –Determines where one frame ends and the next one starts, called frame synchronization

Network Layer

- Responsible for moving packets (data) from one end of the network to the other, called *end-to-end communications*
- Requires *logical addresses* such as IP addresses
- Device example: Router
- –Routing is the ability of various network devices and their related software to move data packets from source to destination
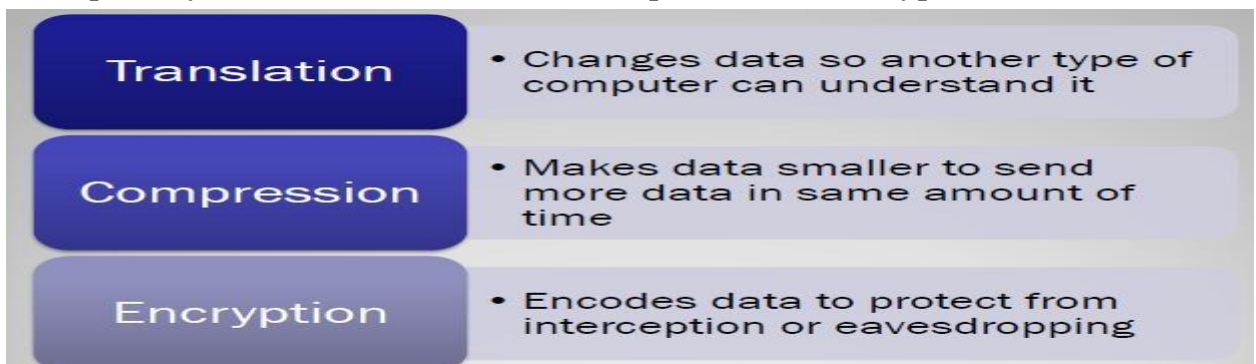
Transport Layer
- Takes data from higher levels of OSI Model and breaks it into segments that can be sent to lower-level layers for data transmission
- Conversely, reassembles data segments into data that higher-level protocols and applications can use
- Also puts segments in correct order (called sequencing) so they can be reassembled in correct order at destination
- Concerned with the reliability of the transport of sent data
- May use a *connection-oriented protocol* such as TCP to ensure destination received segments
- May use a *connectionless protocol* such as UDP to send segments without assurance of delivery
- Uses port addressing

Session Layer
- Responsible for managing the dialog between networked devices
- Establishes, manages, and terminates connections
- Provides duplex, half-duplex, or simplex communications between devices
- Provides procedures for establishing checkpoints, adjournment, termination, and restart or recovery procedures

Presentation Layer
- Concerned with how data is presented to the network
- Handles three primary tasks: –Translation , –Compression , –Encryption

Translation	Changes data so another type of computer can understand it
Compression	Makes data smaller to send more data in same amount of time
Encryption	Encodes data to protect from interception or eavesdropping

Application Layer
- Contains all services or protocols needed by application software or operating system to communicate on the network
- Examples
- –Firefox web browser uses HTTP (Hyper-Text Transport Protocol)
- –E-mail program may use POP3 (Post Office Protocol version 3) to read e-mails and SMTP (Simple Mail Transport Protocol) to send e-mails

The interaction between layers in the OSI model
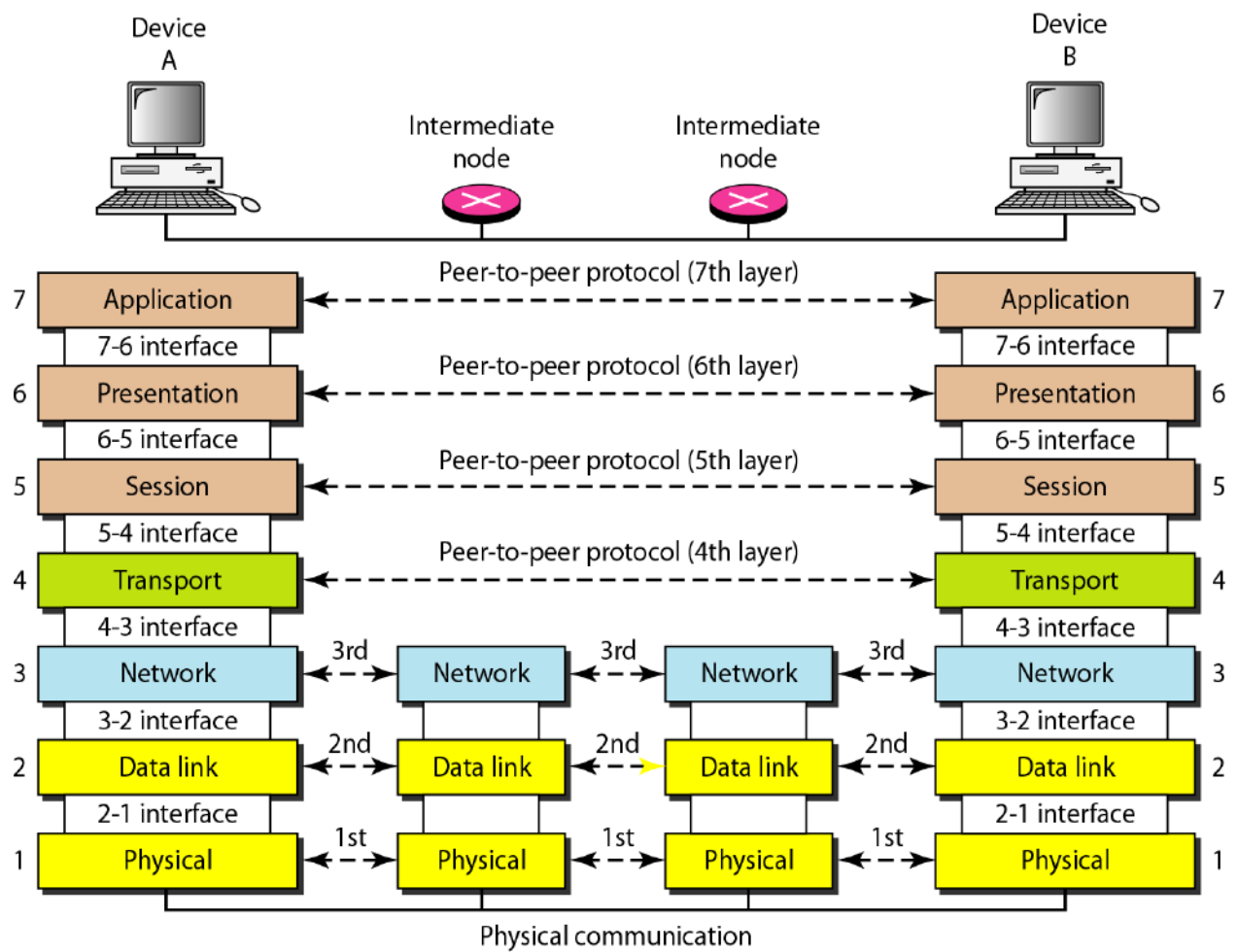
An exchange using the OSI model

SUMMAR

Application — To allow access to network resources

Presentation — To translate, encrypt, and compress data

Session — To establish, manage, and terminate sessions

Transport — To provide reliable process-to-process message delivery and error recovery

Network — To move packets from source to destination; to provide internetworking

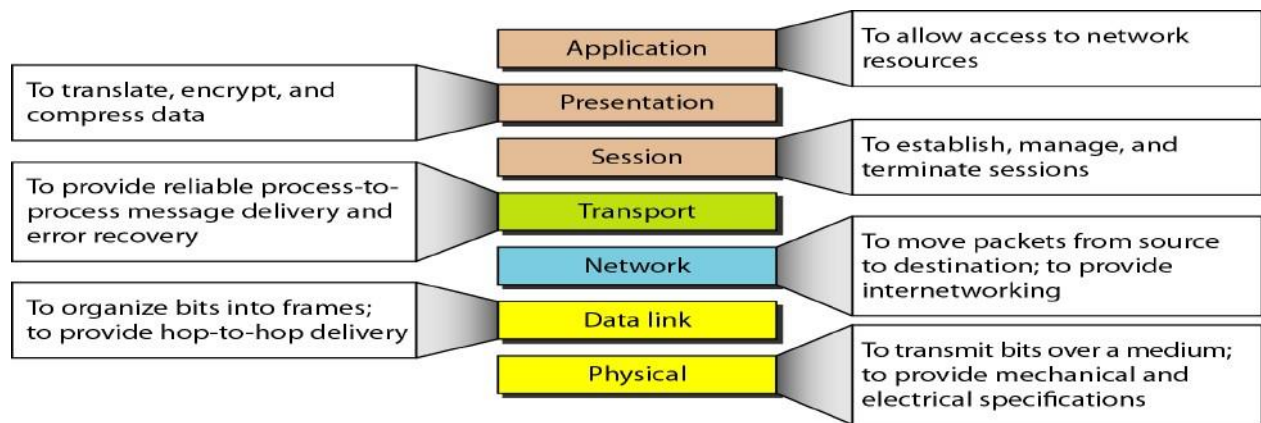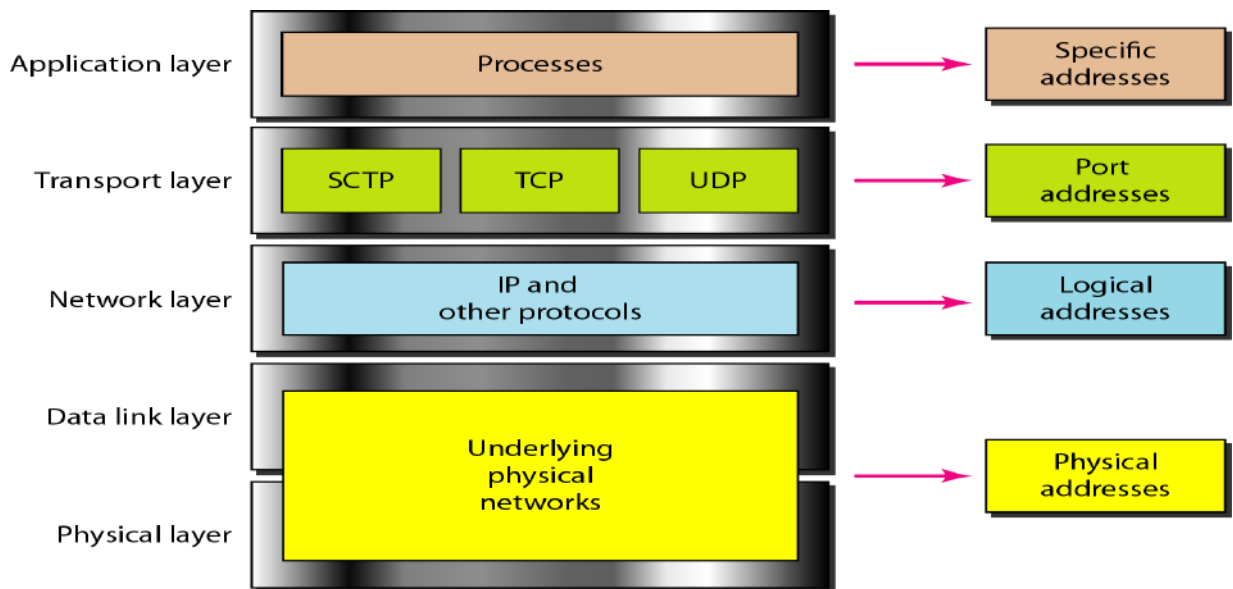**Data link** — To organize bits into frames; to provide hop-to-hop delivery

Physical — To transmit bits over a medium; to provide mechanical and electrical specifications

TCP/IP Model (Transmission Control Protocol/Internet Protocol)

–A *protocol suite* is a large number of related protocols that work together toallow networked computers to communicate

Application layer	Processes	→ Specific addresses
Transport layer	SCTP TCP UDP	→ Port addresses
Network layer	IP and other protocols	→ Logical addresses
Data link layer	Underlying physical networks	→ Physical addresses
Physical layer		

Relationship of layers and addresses in TCP/IP

Application Layer

- Application layer protocols define the rules when implementing specific networkapplications
- Rely on the underlying layers to provide accurate and efficient data delivery
- Typical protocols:
- FTP – File Transfer Protocol
  - For file transfer
- Telnet – Remote terminal protocol
  - For remote login on any other computer on the network
- SMTP – Simple Mail Transfer Protocol
  - For mail transfer
- HTTP – Hypertext Transfer Protocol
  - For Web browsing
- Encompasses   same   functions   as   these   OSI   Model   layers   Application Presentation Session
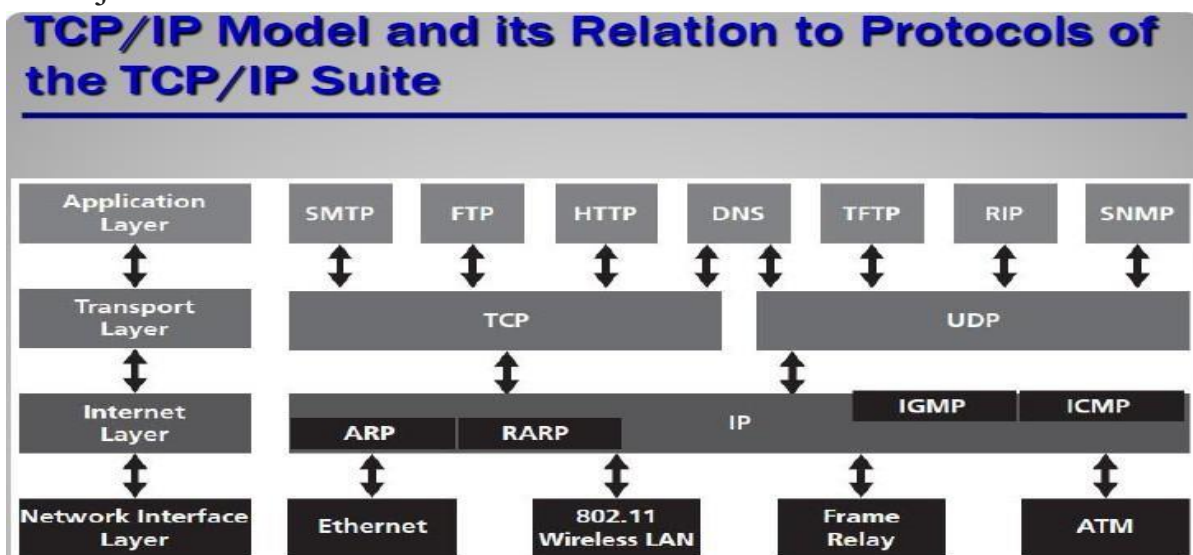
Transport Layer

TCP

- TCP is a connection-oriented protocol
  o Does not mean it has a physical connection between sender and receiver
  o TCP provides the function to allow a connection virtually exists – also calledvirtual circuit
- UDP provides the functions:
  o Dividing a chunk of data into segments
  o Reassembly segments into the original chunk
  o Provide further the functions such as reordering and data resend
- Offering a reliable byte-stream delivery service
- Functions the same as the Transport layer in OSI
- Synchronize source and destination computers to set up the session betweenthe respective computers

Internet Layer
- The network layer, also called the internet layer, deals with packets and connects independent networks to transport the packets across network boundaries. The network layer protocols are the IP and the Internet Control Message Protocol (ICMP), which is used for error reporting.

Host-to-network layer
The **Host-to-network layer** is the lowest **layer** of the **TCP/IP** reference model. It combines the link **layer** and the physical **layer** of the ISO/OSI model. At this **layer**, data is transferred between adjacent **network** nodes in a WAN or between nodes on the same LAN.

TCP/IP Model and its Relation to Protocols of the TCP/IP Suite

Application Layer	SMTP	FTP	HTTP	DNS	TFTP	RIP	SNMP
Transport Layer	TCP				UDP		
Internet Layer	ARP	RARP		IP	IGMP	ICMP	
Network Interface Layer	Ethernet		802.11 Wireless LAN		Frame Relay		ATM

OSI MODEL	TCP/IP MODEL
Contains 7 Layers	Contains 4 Layers
Uses Strict Layering resulting in vertical layers.	Uses Loose Layering resulting in horizontal layers.
Supports both connectionless & connection-oriented communication in the Network layer, but only connection-oriented communication in Transport Layer	Supports only connectionless communication in the Network layer, but both connectionless & connection-oriented communication in Transport Layer
It distinguishes between Service, Interface and Protocol.	Does not clearly distinguish between Service, Interface and Protocol.
Protocols are better hidden and can be replaced relatively easily as technology changes (No transparency)	Protocols are not hidden and thus cannot be replaced easily. (Transparency) Replacing IP by a substantially different protocol would be virtually impossible
OSI reference model was devised before the corresponding protocols were designed.	The protocols came first and the model was a description of the existing protocols

THE INTERNET

The Internet has revolutionized many aspects of our daily lives. It has affected the way we do business as well as the way we spend our leisure time. Countthe ways you've used the Internet recently. Perhaps you've sent electronic mail (e-mail) to a business associate, paid a utility bill, read a newspaper from a distant city, or looked up a local movie schedule-all by using the Internet. Ormaybe you researched a medical topic, booked a hotel reservation, chattedwith a fellow Trekkie, or comparison-shopped for a car. The Internet is a communication system that has brought a wealth of information to our fingertips and organized it for our use.

A Brief History

A network is a group of connected communicating devices such as computers and printers. An internet (note the lowercase letter i) is two ormore networks that can communicate with each other. The most notable internet is called the Internet (uppercase letter I), a collaboration of more than hundreds of thousands of interconnected networks. Private individuals as well as various organizations such as government agencies, schools, research facilities, corporations, and libraries in more than 100 countries use the Internet. Millions of people are users. Yet this extraordinary communication system only came into being in 1969.

In the mid-1960s, mainframe computers in research organizations were standalone devices. Computers from different manufacturers were unable to communicate with one another. The Advanced Research Projects Agency

(ARPA) in the Department of Defense (DoD) was interested in finding a way to connect computers so that the researchers they funded could share theirfindings, thereby reducing costs and eliminating duplication of effort.

In 1967, at an Association for Computing Machinery (ACM) meeting, ARPA presented its ideas for ARPANET, a small network of connected computers. The idea was that each host computer (not necessarily from the same manufacturer) would be attached to a specialized computer, called an *inteiface message processor* (IMP). The IMPs, in tum, would be connected to one another. Each IMP had to be able to communicate with other IMPs as well as with its own attached host. By 1969, ARPANET was a reality. Four nodes, at the University of California at Los Angeles (UCLA), the University of California at Santa Barbara (UCSB), Stanford Research Institute (SRI), and the Universityof Utah, were connected via the IMPs to form a network. Software called the *Network Control Protocol* (NCP) provided communication between the hosts.

In 1972, Vint Cerf and Bob Kahn, both of whom were part of the core ARPANET group, collaborated on what they called the *Internetting Projec1*. Cerf and Kahn's landmark 1973 paper outlined the protocols to achieve end- to-end delivery of packets. This paper on Transmission Control Protocol (TCP) included concepts such as encapsulation, the datagram, and the functions ofa gateway. Shortly thereafter, authorities made a decision to split TCP into twoprotocols: Transmission Control Protocol (TCP) and Internetworking Protocol (lP). IP would handle datagram routing while TCP would be responsible for higher-level functions such as segmentation, reassembly, and error detection. The internetworking protocol became known as TCPIIP.

The Internet Today

The Internet has come a long way since the 1960s. The Internet today is not a simple hierarchical structure. It is made up of many wide- and local-area networks joined by connecting devices and switching stations. It is difficult to give an accurate representation of the Internet because it is continually changing-new networks are being added, existing networks are adding addresses, and networks of defunct companies are being removed. Todaymost end users who want Internet connection use the services of Internet service providers (lSPs). There are international service providers, national service providers, regional service providers, and local service providers. The Internet today is run by private companies, not the government. Figure 1.13 shows a conceptual (not geographic) view of the Internet.
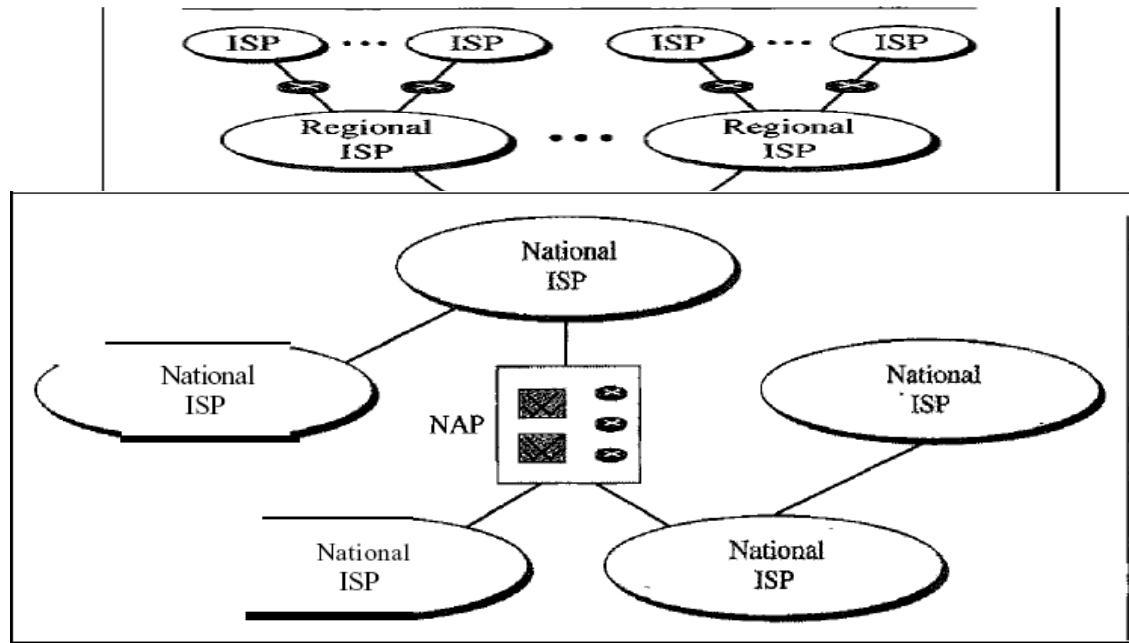
b. Interconnection of national ISPs

International Internet Service Providers:

At the top of the hierarchy are the international service providers that connect nations together.

National Internet Service Providers:

The national Internet service providers are backbone networks created and maintained by specialized companies. There are many national ISPs operating in North America; some of the most well known are SprintLink, PSINet, UUNet Technology, AGIS, and internet Mel. To provide connectivity between the end users, these backbone networks are connected by complex switching stations (normally run by a third party) called network access points (NAPs). Some national ISP networks are also connected to one another by private switching stations called *peering points.* These normally operate at a high data rate (up to 600 Mbps).

Regional Internet Service Providers:

Regional internet service providers or regional ISPs are smaller ISPs that are connected to one or more national ISPs. They are at the third level of the hierarchy with a smaller data rate. *Local Internet Service Providers:*

Local Internet service providers provide direct service to the end users. The local ISPs can be connected to regional ISPs or directly to national ISPs. Most end users are connected to the local ISPs. Note that in this sense, a local ISP can be a company that just provides Internet services, a corporation witha network that supplies services to its own employees, or a nonprofit organization, such as a college or a university, that runs its own network. Each of these local ISPs can be connected to a regional or national service provider.