MODULE 1

Introduction – Uses of computer networks, Network hardware, Network software. Reference models – The OSI reference model, The TCP/IP reference model, Comparison of OSI and TCP/IP reference models.

Physical Layer – Modes of communication, Physical topologies, Signal encoding, Repeaters and hub, Transmission media overview. Performance indicators – Bandwidth, Throughput, Latency, Queuing time, Bandwidth–Delay product.

NETWORK

- Computer network is 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.
- The Internet is not a single network but a network of networks and the Web is a distributed system that runs on top of the Internet.

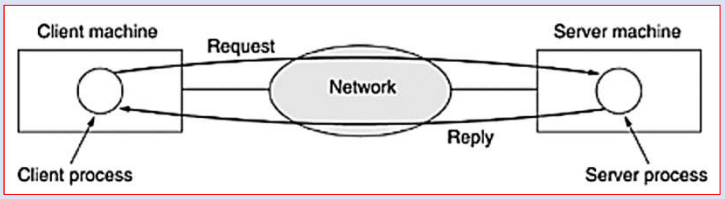
2

❖Uses of Computer Networks

1. Business Applications

- resource sharing - a group of office workers share a common printer
- client-server model - two processes are involved, one on the client machine and one on the server machine. Communication takes the form of the client process sending a message over the network to the server process. The client process then waits for a reply message. When the server process gets the request, it performs the requested work or looks up the requested data and sends back a reply.

3



- e-mail
- Videoconferencing
- e-commerce (electronic commerce)

2. Home Applications

- ➢Access to remote information
- ➢Person-to-person communication
- ➢Interactive entertainment (Online Games)
- ➢Electronic commerce

3. Mobile Users

- Mobile computers, such as notebook computers and personal digital assistants (PDAs)
- wireless networks
- mobile computing

4. Social Issues

- new social, ethical, and political problems
- anonymous messages

❖Data Flow

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

❖Simplex

- ✓Communication is unidirectional
- ✓Only one of the two devices on a link can transmit; the other can only receive
- ✓**Eg :** Keyboards and traditional monitors
- ✓The simplex mode can use the entire capacity of the channel to send data in one direction.

6

❖**Half-Duplex**

✓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

✓**Eg:** Walkie-talkies and CB (citizens band) radios

❖**Full-Duplex**

✓Both stations can transmit and receive simultaneously

✓signals going in one direction share the capacity of the link

7

✓This sharing can occur in two ways:

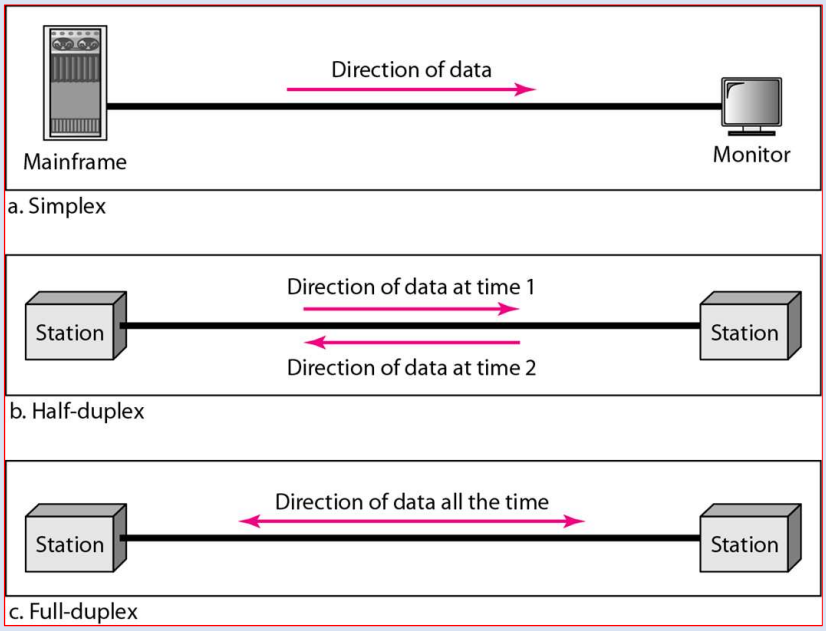
- Either the link must contain two physically separate transmission paths, one for sending and the other for receiving
- Or the capacity of the channel is divided between signals traveling in both directions.

✓**Eg:** telephone network.

✓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.

8



9

NETWORK HARDWARE

❖**Two criterion for classifying networks are**

1. **Transmission technology**
2. **Scale**

➢ There are two types of transmission technology

A. Broadcast links

- Broadcast networks have a single communication channel that is shared by all the machines on the network.
- Short messages, called packets, sent by any machine are received by all the others.

10

- An address field within the packet specifies the intended recipient. Upon receiving a packet, a machine checks the address field.
- If the packet is intended for the receiving machine, that machine processes the packet; if the packet is intended for some other machine, it is just ignored.
- Broadcast systems generally also allow the possibility of addressing a packet to all destinations by using a special code in the address field.
- When a packet with this code is transmitted, it is received and processed by every machine on the network. This mode of operation is called **broadcasting**.

11

- Some broadcast systems also support transmission to a subset of the machines, something known as **multicasting**.
- One possible scheme is to reserve one bit to indicate multicasting. The remaining n - 1 address bits can hold a group number.. When a packet is sent to a certain group, it is delivered to all machines subscribing to that group

B. Point-to-point links

- 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.
- When you change television channels by infrared remote control, you are establishing a point-to-point connection

12

- Smaller, geographically localized networks tend to use broadcasting, whereas larger networks usually are point-to-point.
- Point-to-point transmission with one sender and one receiver is sometimes called **unicasting.**

❖**SCALE -** By physical size of network

Interprocessor distance	Processors located in same	Example
1 m	Square meter	Personal area network
10 m	Room	Local area network
100 m	Building	
1 km	Campus	
10 km	City	Metropolitan area network
100 km	Country	Wide area network
1000 km	Continent	
10,000 km	Planet	The Internet

1. Local Area Networks (LAN)

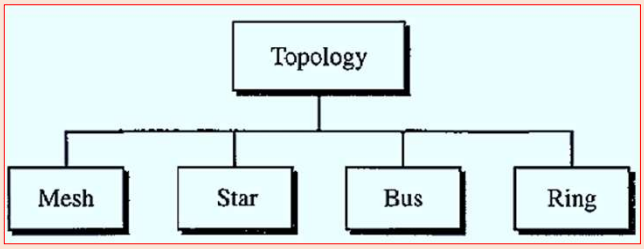
- Privately-owned networks within a single building or campus of up to a few kilometers in size.
- They are widely used to connect personal computers and workstations in company offices and factories to share resources (e.g., printers) and exchange information.
- LANs are distinguished from other kinds of networks by three characteristics:

A. size

B. Their transmission technology

C. Their topology.

- LANs are restricted in size
- LANs may use a transmission technology consisting of a cable to which all the machines are attached, like the telephone lines used in rural areas

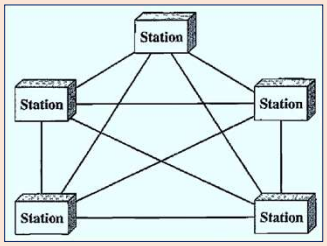


- **MESH TOPOLOGY** - every device has a dedicated point-to-point link to every other device. The term dedicated means that the link carries traffic only between the two devices it connects.

15

- To find the number of physical links in a fully connected mesh network with **n** nodes

n(n -1) /2



❖**ADVANTAGE**

- **Eliminating the traffic problems** - the use of dedicated links guarantees that each connection can carry its own data load
- **Mesh topology is robust** - If one link becomes unusable, it does not incapacitate the entire system
- **Privacy or security** - When every message travels along a dedicated line, only the intended recipient sees it.

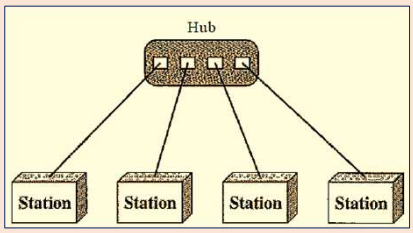
❖**DISADVANTAGE**

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

❖**EXAMPLE -** connection of telephone regional offices

- **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
- The controller (hub) 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

❖**ADVANTAGE**



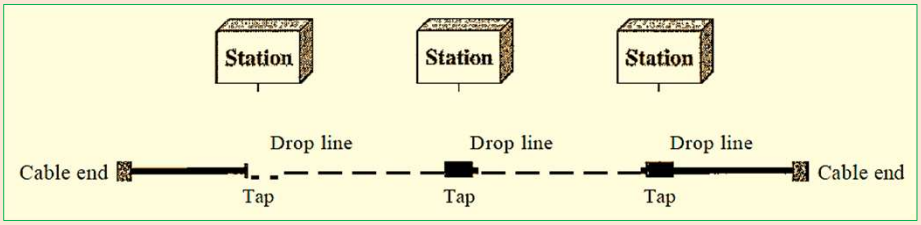
- Less expensive than a mesh topology.
- Easy to install and reconfigure.
- Less cabling needs to be housed,
- Robustness - If one link fails, only that link is affected. All other links remain active
- Easy fault identification

❖**DISADVANTAGE**

- If the hub goes down, the whole system is dead

❖**EXAMPLE -** High-speed LANs often use a star topology with a central hub

- **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.

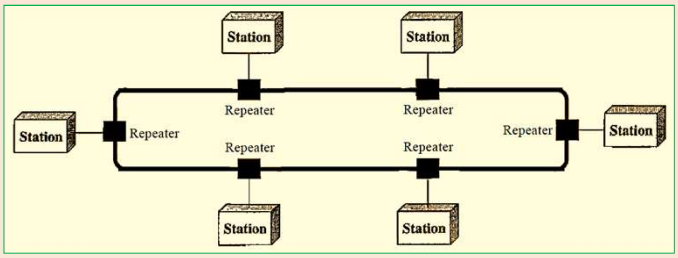


❖**ADVANTAGE**

- Ease of installation.
- Bus uses less cabling than mesh or star topologies

❖**DISADVANTAGE**

- Difficult reconnection and fault isolation.
- Difficult to add new devices
- A fault or break in the bus cable stops all transmission
- **Eg :** Ethernet LANs can use a bus topology
- **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**. Repeater regenerates the bits and passes them .



❖**ADVANTAGE**

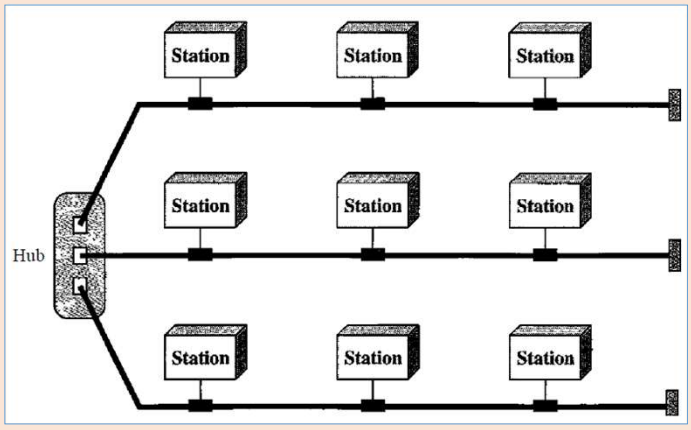
- Easy to install and reconfigure
- To add or delete a device requires changing only two connections

❖**DISADVANTAGE**

- Unidirectional traffic
- A break in the ring can disable the entire network

21

- **Hybrid Topology -** we can have a main star topology with each branch connecting several stations in a bus topology



22

2. Metropolitan Area Networks (MAN)

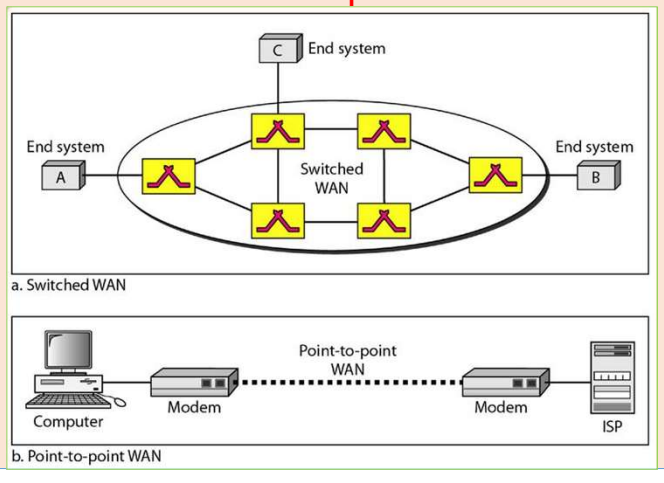
- A metropolitan area network, or MAN, covers a city.
- Example of a MAN is the cable television network available in many cities
- Another example of a MAN is the part of the telephone company network that can provide a high-speed DSL line to the customer

3. wide area network (WAN)

- A wide area network, or WAN, spans a large geographical area, often a country or continent
- The switched WAN connects the end systems, which usually comprise a router that connects to another LAN or WAN

23

- The point-to-point WAN is normally a line leased from a telephone or cable TV provider that connects a home computer or a small LAN to an Internet service provider (ISP).
- This type of WAN is often used to provide Internet access.



24

NETWORK SOFTWARE

❖Protocol Hierarchies

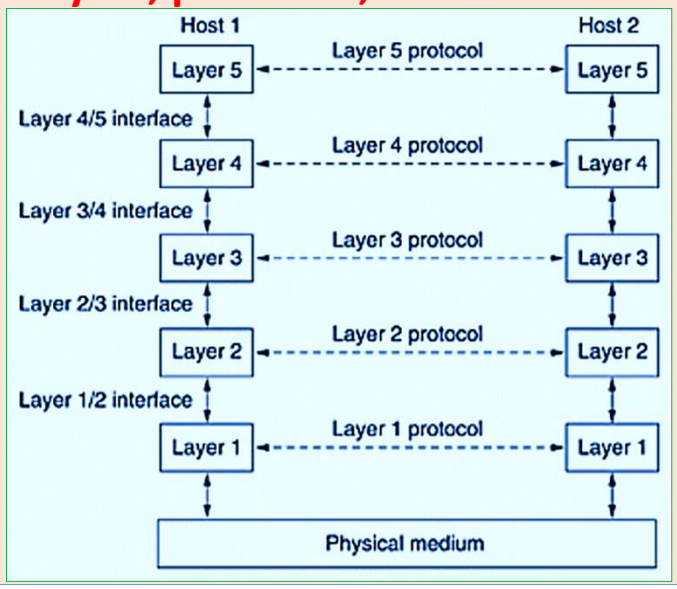
- To reduce the design complexity, most networks are organized as a stack of layers or levels, each one built upon the one below it.
- The number of layers, the name of each layer, the contents of each layer, and the function of each layer differ from network to network.
- The purpose of each layer is to offer certain services to the higher layers, shielding those layers from the details of how the offered services are actually implemented.
- Each layer is a kind of virtual machine, offering certain services to the layer above it

25

- Layer **N** on one machine carries on a conversation with layer **N** on another machine. The rules and conventions used in this conversation are collectively known as the **layer N protocol**.
- Basically, a protocol is an agreement between the communicating parties on how communication is to proceed.
- In reality, no data are directly transferred from layer N on one machine to layer N on another machine.
- Instead, each layer passes data and control information to the layer immediately below it, until the lowest layer is reached.
- Below layer 1 is the physical medium through which actual communication occurs.

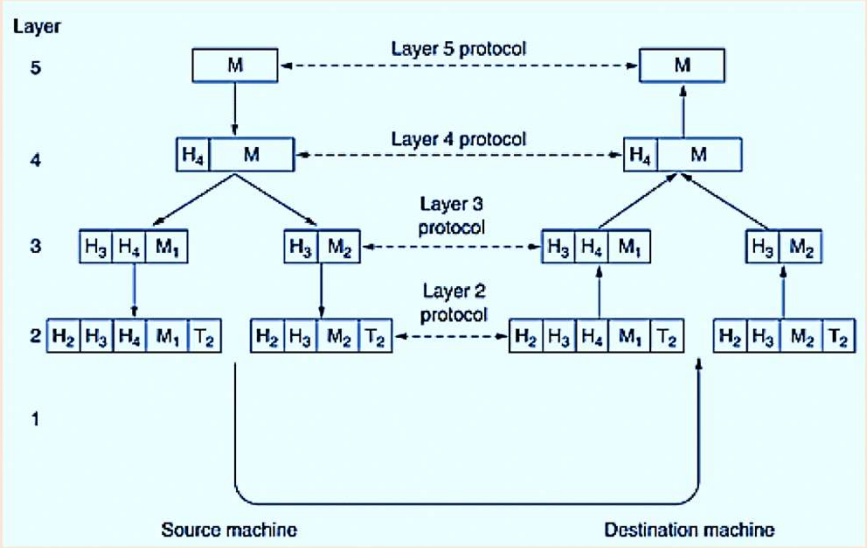
26

Layers, protocols, and interfaces



27

Example information flow supporting virtual communication in layer 5.



28

- A message, M, is produced by an application process running in layer 5 and given to layer 4 for transmission.
- Layer 4 puts a header in front of the message to identify the message and passes the result to layer 3. The header includes control information(sequence numbers) to allow layer 4 on the destination machine to deliver messages in the right order if the lower layers do not maintain sequence.
- In some layers, headers can also contain sizes, times, and other control fields.
- Layer 3 must break up the incoming messages into smaller units, packets, prepending a layer 3 header to each packet

29

- Layer 2 adds not only a header to each piece, but also a trailer, and gives the resulting unit to layer 1 for physical transmission.
- At the receiving machine the message moves upward, from layer to layer, with headers being stripped off as it progresses.

30

❖Design Issues for the Layers

- Every layer needs a mechanism for identifying senders and receivers. some form of addressing is needed in order to specify a specific destination
- **The rules for data transfer-** In some systems, data only travel in one direction; in others, data can go both ways.
- **Error control** is an important issue because physical communication circuits are not perfect. Many error-detecting and error-correcting codes are known, but both ends of the connection must agree on which one is being used. In addition, the receiver must have some way of telling the sender which messages have been correctly received and which have not.

31

- Not all communication channels preserve the **order of messages** sent on them. To deal with a possible loss of sequencing, the protocol must make explicit provision for the receiver to allow the pieces to be reassembled properly
- An issue that occurs at every level is how to keep a fast sender from swamping a slow receiver with data.
- Another problem that must be solved at several levels is the inability of all processes to accept arbitrarily long messages. This property leads to mechanisms for disassembling, transmitting, and then reassembling messages.
- When there are multiple paths between source and destination, a route must be chosen. Sometimes this decision must be split over two or more layers (Routing)

32

❖Connection-Oriented Service

- To use a connection-oriented network service, the service user first establishes a connection, uses the connection, and then releases the connection (Eg: telephone system)
- In most cases the order is preserved so that the bits arrive in the order they were sent.
- The source first makes a connection with the destination before sending a packet. When the connection is established, a sequence of packets from the same source to the same destination can be sent one after another.
- In this case, there is a relationship between packets. They are sent on the same path in sequential order.

33

- A packet is logically connected to the packet traveling before it and to the packet traveling after it.
- When all packets of a message have been delivered, the connection is terminated.

❖Connectionless Service

- In connectionless service, the network layer protocol treats each packet independently, with each packet having no relationship to any other packet.
- The packets in a message may or may not travel the same path to their destination.
- The Internet has chosen this type of service at the network layer.

34

❖Protocols

- A protocol is a set of rules that govern data communications. A protocol defines what is communicated, how it is communicated, and when it is communicated. The key elements of a protocol are syntax, semantics, and timing.

➢**Syntax** - The term syntax refers to the structure or format of the data, meaning the order in which they are presented

➢**Semantics** - The word semantics refers to the meaning of each section of bits

➢**Timing** - The term timing refers to two characteristics: when data should be sent and how fast they can be sent

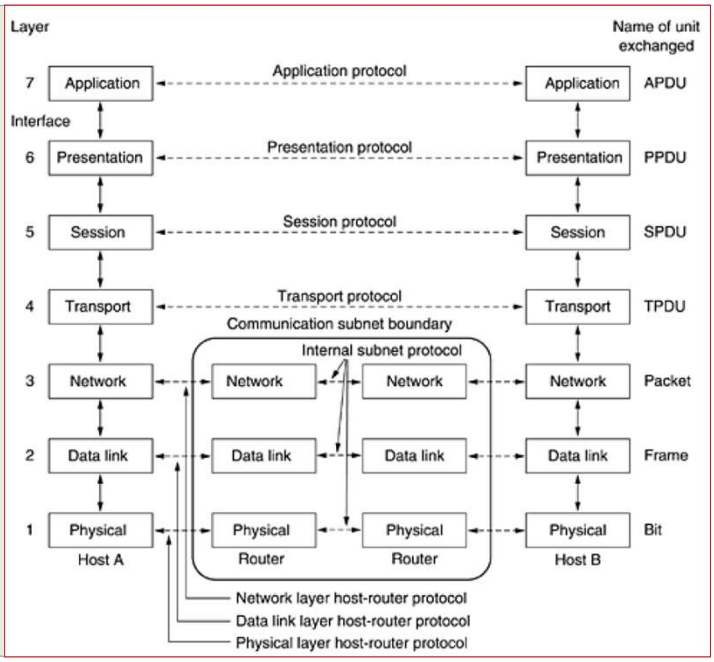
35

OSI REFERENCE MODEL

- A network is a combination of hardware and software that sends data from one location to another.
- The hardware consists of the physical equipment that carries signals from one point of the network to another. The software consists of instruction sets that make possible the services that we expect from a network
- The OSI model is a layered framework for the design of network systems that allows communication between all types of computer systems
- It consists of seven separate but related layers

36

The OSI reference model



37

❖PHYSICAL LAYER

- The physical layer is concerned with transmitting raw bits over a communication channel
- The physical layer is responsible for movements of individual bits from one hop (node) to the next.

➢**Other Responsibilities :**

1. Physical characteristics of interfaces and medium – defines the characteristics of the interface between the devices and the transmission medium. It also defines the type of transmission medium.

38

2. Representation of bits - To be transmitted, bits must be encoded into signals (electrical or optical). The physical layer defines the type of encoding (how 0s and 1s are changed to signals).
3. Data rate (The transmission rate) - the number of bits sent each second is also defined by the physical layer
4. Synchronization of bits - the sender and the receiver clocks must be synchronized.
5. Line configuration - The physical layer is concerned with the connection of devices to the media. In a point-to-point configuration, two devices are connected through a dedicated link. In a multipoint configuration, a link is shared among several devices.

39

6. Physical topology - The physical topology defines how devices are connected to make a network. Devices can be connected by using a mesh topology ,a star topology ,a ring topology ,a bus topology or a hybrid topology
7. Transmission mode - The physical layer also defines the direction of transmission between two devices: simplex, half-duplex, or full-duplex.

- In simplex mode, only one device can send; the other can only receive. The simplex mode is a one-way communication.
- In the half-duplex mode, two devices can send and receive, but not at the same time.
- In a full-duplex (or simply duplex) mode, two devices can send and receive at the same time.

40

❖DATA LINK LAYER

- The data link layer is responsible for moving frames from one hop (node) to the next

➢Other responsibilities :

1. Framing - The data link layer divides the stream of bits received from the network layer into manageable data units called frames
2. Physical addressing - If frames are to be distributed to different systems on the network, the data link layer adds a header to the frame to define the sender and/or receiver of the frame. If the frame is intended for a system outside the sender's network, the receiver address is the address of the device that connects the network to the next one.

41

3. Flow control - If the rate at which the data are absorbed by the receiver is less than the rate at which data are produced in the sender, the data link layer imposes a flow control mechanism to avoid overwhelming the receiver.
4. Error control - The data link layer adds reliability to the physical layer by adding mechanisms to detect and retransmit damaged or lost frames. It also uses a mechanism to recognize duplicate frames. Error control is normally achieved through a trailer added to the end of the frame
5. Access control - When two or more devices are connected to the same link, data link layer protocols are necessary to determine which device has control over the link at any given time.

42

❖NETWORK LAYER

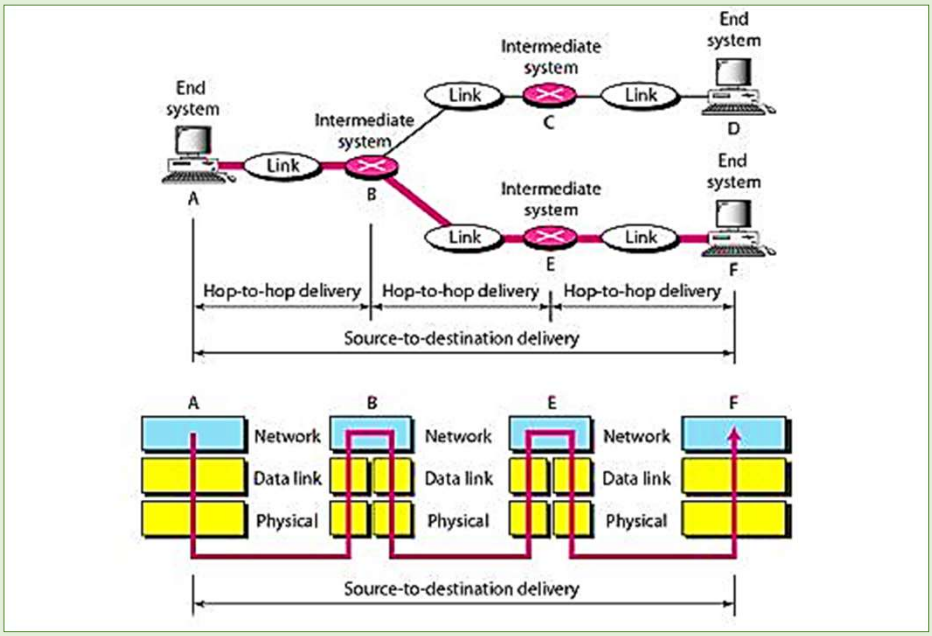
- The network layer is responsible for the delivery of individual packets from the source host to the destination host
- If two systems are connected to the same link, there is usually no need for a network layer.
- If the two systems are attached to different networks (links) with connecting devices between the networks (links), there is often a need for the network layer to accomplish source-to-destination delivery

➢**Other Responsibilities :**

43

1. Logical addressing - The physical addressing implemented by the data link layer handles the addressing problem locally. If a packet passes the network boundary, we need another addressing system to help distinguish the source and destination systems. The network layer adds a header to the packet coming from the upper layer that, among other things, includes the logical addresses of the sender and receiver
2. Routing - When independent networks or links are connected to create internetworks (network of networks) or a large network, the connecting devices (called routers or switches) route or switch the packets to their final destination

44



45

❖TRANSPORT LAYER

- The transport layer is responsible for process-to-process delivery of the entire message
- The transport layer is responsible for the delivery of a message from one process to another . A process is an application program running on a host.

➢Other responsibilities

1. Service-point addressing - delivery of message not only from one computer to the next but also from a specific process (running program) on one computer to a specific process (running program) on the other. The transport layer header must therefore include a type of address called a service-point address (or port address).

46

- The network layer gets each packet to the correct computer; the transport layer gets the entire message to the correct process on that computer.

2. Segmentation and reassembly - A message is divided into transmittable segments, with each segment containing a sequence number. These numbers enable the transport layer to reassemble the message correctly upon arriving at the destination.
3. Connection control - The transport layer can be either connectionless or connection oriented.
4. Flow control - The transport layer is responsible for flow control. However, flow control at this layer is performed end to end rather than across a single link

47

5. Error control - Like the data link layer, the transport layer is responsible for error control. However, error control at this layer is performed process-to process rather than across a single link.

- The sending transport layer makes sure that the entire message arrives at the receiving transport layer without error (damage, loss, or duplication).
- Error correction is usually achieved through retransmission.

48

❖SESSION LAYER

- The session layer is responsible for dialog control and synchronization.

➢**Specific responsibilities :**

1. Dialog control - The session layer allows two systems to enter into a dialog. It allows the communication between two processes to take place in either half duplex (one way at a time) or full-duplex (two ways at a time) mode.
2. Synchronization - The session layer allows a process to add checkpoints, or synchronization points, to a stream of data

49

❖PRESENTATION LAYER

- The presentation layer is concerned with the syntax and semantics of the information exchanged between two systems

➢**Specific responsibilities :**

1. Translation - Because different computers use different encoding systems, the presentation layer is responsible for interoperability between these different encoding methods. The presentation layer at the sender changes the information from its sender-dependent format into a common format. The presentation layer at the receiving machine changes the common format into its receiver-dependent format

50

2. Encryption - To carry sensitive information, a system must be able to ensure privacy. Encryption means that the sender transforms the original information to another form and sends the resulting message out over the network. Decryption reverses the original process to transform the message back to its original form
3. Compression - Data compression reduces the number of bits contained in the information. Data compression becomes particularly important in the transmission of multimedia such as text, audio, and video

51

❖APPLICATION LAYER

- The application layer is responsible for providing services to the user.
- It provides user interfaces and support for services such as electronic mail, remote file access and transfer, shared database management, and other types of distributed information services

➢**Other Responsibilities:**

1. Network Virtual Terminal (NVT) - A network virtual terminal is a software version of a physical terminal, and it allows a user to log on to a remote host. The remote host believes it is communicating with one of its own terminals and allows the user to log on.

52

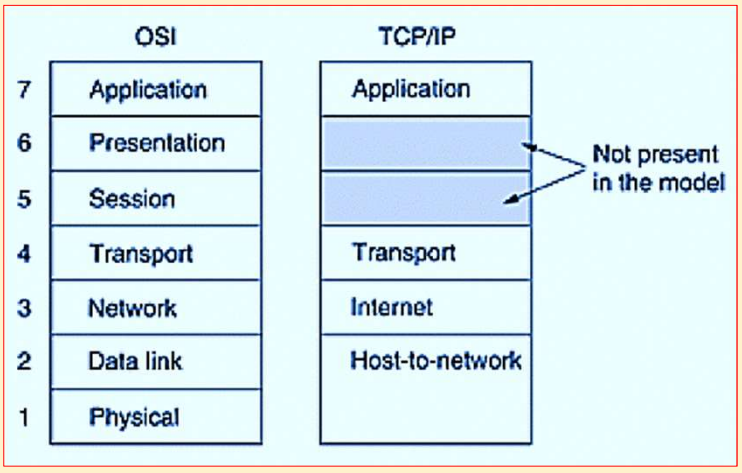
2. File transfer, access, and management - This application allows a user to access files in a remote host (to make changes or read data), to retrieve files from a remote computer for use in the local computer, and to manage or control files in a remote computer locally
3. Mail services - This application provides the basis for e-mail forwarding and storage.
4. Directory services - This application provides distributed database sources and access for global information about various objects and services.

53

TCP/IP PROTOCOL SUITE

➢The original TCP/IP protocol suite was defined as having four layers:

- **Host-to-network**
- **Internet**
- **Transport**
- **Application**



54

TCP/IP Protocol Suite

- It is the Internet Protocol Suite
- The set of communication protocols used for the internet and other similar networks
- Viewed as a set of layers
- Each layer solves a set of problems involving the transmission of data and provides well defined services to the upper layers

TCP/IP Protocol Suite

Consists of 4 layers

1. **Link layer**
2. **Internet layer**
3. **Transport layer**
4. **Application layer**

Application layer

- This is the place where high level protocols reside and those protocols include FTP, SMTP, DNS, SNMP and HTTP.
- **File Transfer Protocol(FTP)** : To permit reliable transfer of files between different platforms. It uses TCP at the transport layer.
- **Hyper Text Transfer Protocol(HTTP)**: Permits applications such as browsers to upload and download web pages. To check reliability, it makes use of TCP at the transport layer. HTTP delivers HTML documents
- **Simple Mail Transfer Protocol (SMTP)** : Helps to send email to other computers that support TCP/IP protocol suite.

Application layer

- **Domain Name System(DNS) Protocol**: Allows the network determine the IP address from name and vice versa
- **Simple Network Management Protocol (SNMP)** : For the transport of network management information
- **Telnet Protocol**: This is the virtual terminal protocol which allows the user in one machine to log into another machine and work

Transport Layer

- The transport layer is responsible for the transport of data
- Transport layer communicates data between two applications running on computers, making use of port numbers
- It also incorporates error detection
- **TCP(Transmission Control Protocol)**: It is a reliable connection oriented protocol that permits a byte stream originating on machine to be transported without error to any machine in the internet.
- **UDP(User Datagram Protocol)** : It is an unreliable connectionless protocol for applications that do not want TCP's sequencing on flow control.

Internet Layer

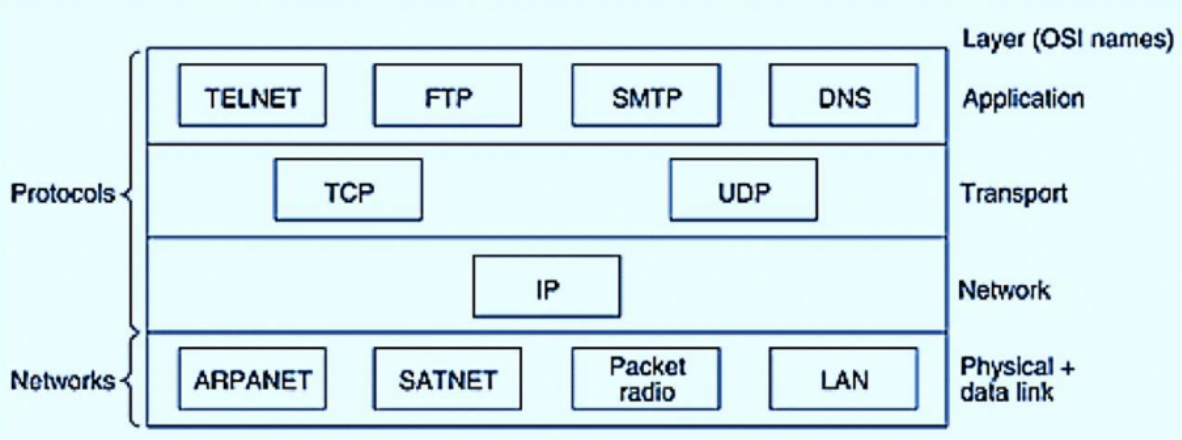
- This layer is responsible for sending packets through different networks
- The internet layer encapsulates the segments from the Transport Layer into envelopes called packets and then determines the path the information is to take across the network
- **IP(Internet Protocol):** Responsible for delivering packets from source to destination by looking at the IP addresses
- **ARP(address Resolution Protocol):** Used to find Ethernet(hardware) address from a specific IP address

Link Layer or Network Access Layer

- The link layer offers the ability to access the physical network to transmit data
- Breaks down the packets from the Internet layer into frames and then eventually into bits for transmission across the physical network medium
- Contains all specifications relating to the transmission of data over a physical network
- Routing and synchronizing data over a network, checking data formats, converting signals and error detection in the transmitted data

Link Layer or Network Access Layer

- Signaling and network medium standards such as Ethernet, Token ring, FDDI, X.25,Frame Relay, Point-to-Point Protocol(PPP), RS 232 etc. are defined in this layer
- Network Interface Cards, hubs, repeaters, switches etc. operate at this layer



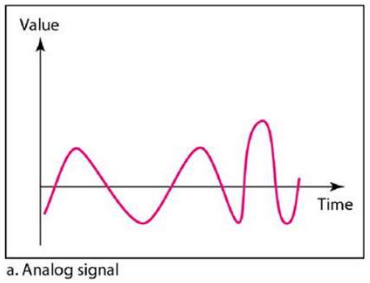
PHYSICAL LAYER

- One major task of Physical Layer is to provide services for the data link layer.
- The data in the data link layer consists of 0s and 1s organized into frames that are ready to be sent across the transmission medium.
- This stream of 0s and 1s must first be converted into signals.
- One of the services provided by the physical layer is to create a signal that represents this stream of bits.
- The transmission medium must be controlled by the physical layer.

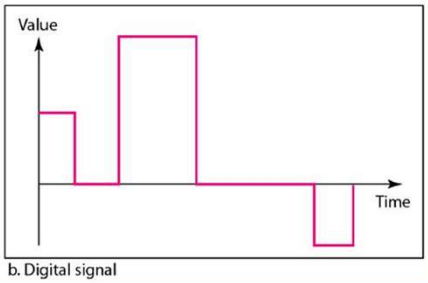
❖Analog and Digital Data

- To be transmitted, data must be transformed to electromagnetic signals
- Both data and the signals that represent them can be either analog or digital in form.
- The term analog data refers to information that is continuous.
- For example, an analog clock that has hour, minute, and second hands gives information in a continuous form; the movements of the hands are continuous
- digital data refers to information that has discrete states. a digital clock that reports the hours and the minutes will change suddenly from 8:05 to 8:06.

- Digital data take on discrete values.
- For example, data are stored in computer memory in the form of 0s and 1s. They can be converted to a digital signal or modulated into an analog signal for transmission across a medium.
- Signals can be analog or digital. Analog signals can have an infinite number of values in a range; digital signals can have only a limited number of values.



a. Analog signal



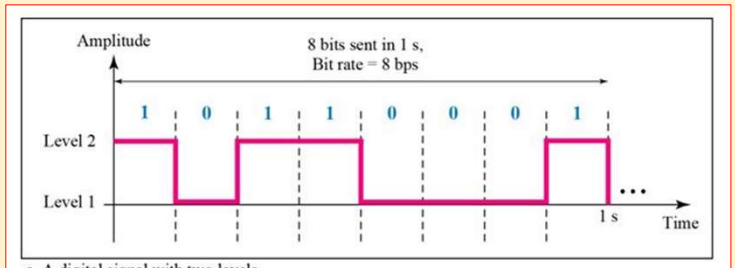
b. Digital signal

❖Periodic and Non-periodic Signals

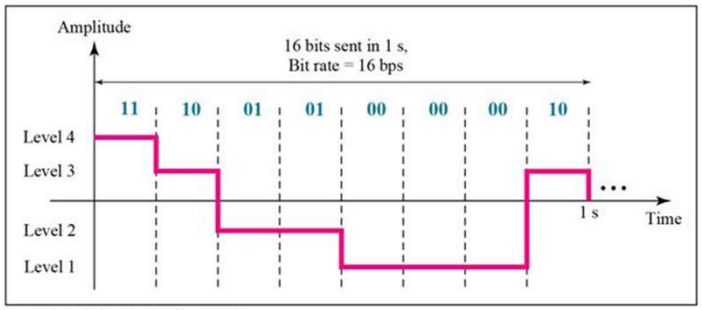
- Both analog and digital signals can take one of two forms: periodic or non-periodic.
- A periodic signal completes a pattern within a measurable time frame, called a period, and repeats that pattern over subsequent identical periods. The completion of one full pattern is called a cycle.
- A non-periodic signal changes without exhibiting a pattern or cycle that repeats over time.
- In data communications, we commonly use periodic analog signals and non-periodic digital signals.

❖DIGITAL SIGNALS

- A 1 can be encoded as a positive voltage and a 0 as zero voltage.
- A digital signal can have more than two levels. In this case, we can send more than 1 bit for each level .
- We send 1 bit per level in part a of the figure and 2 bits per level in part b of the figure.
- In general, if a signal has L levels, each level needs **log2L bits**



a. A digital signal with two levels



b. A digital signal with four levels

- **Bit Rate** - The bit rate is the number of bits sent in 1second, expressed in bits per second (bps).
- **Bit Length** - The bit length is the distance one bit occupies on the transmission medium.

Bit length = propagation speed x bit duration

NETWORK PERFORMANCE

1. Bandwidth

- Bandwidth is the data carrying capacity of the network/transmission medium. Bandwidth is usually measured in bits transferred per second (bps) through a path or link.

➢ **bandwidth in hertz**

- It is the range of frequencies in a composite signal or the range of frequencies that a channel can pass.

➢ **bandwidth in bits per second**

- It is the speed of bit transmission in a channel or link.

2. Throughput

- The throughput is a measure of how fast we can actually send data through a network.
- Practical measure of the amount of data actually transmitted through a channel.
- It depends on the latency.

3. Latency (Delay)

- The latency or delay defines how long it takes for an entire message to completely arrive at the destination from the time the first bit is sent out from the source.
- **Latency = propagation time + transmission time + queuing time + processing delay**

➢Propagation Time

- Propagation time measures the time required for a bit to travel from the source to the destination.

  Propagation time = Distance/Propagation speed

➢Transmission Time

- There is a time between the first bit leaving the sender and the last bit arriving at the receiver.

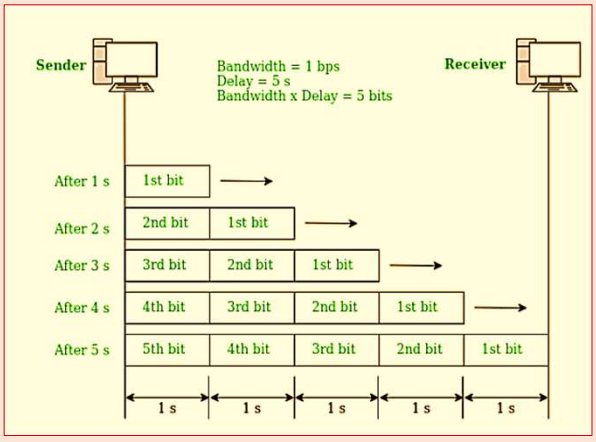
  Transmission time =Message size /Bandwidth

➢Queuing Time

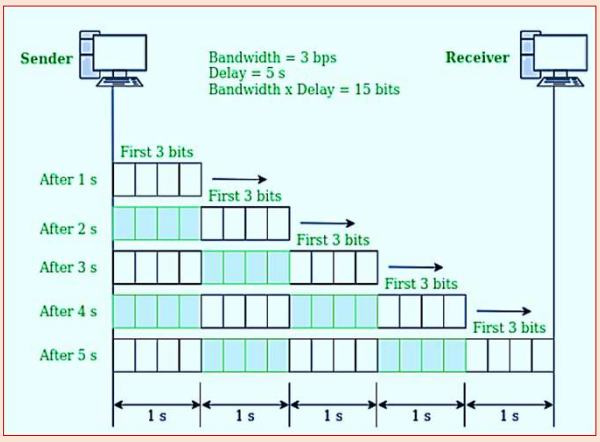
- The time needed for each intermediate or end device to hold the message before it can be processed.

4. Bandwidth-Delay Product

- The bandwidth-delay product defines the number of bits that can fill the link.



Case 1



Case 2

Case 1: Assume a link is of bandwidth 1bps and the delay of the link is 5s. Let us find the bandwidth-delay product in this case. From the image, we can say that this product 1 x 5 is the maximum number of bits that can fill the link. There can be close to 5 bits at any time on the link.

Case 2: Assume a link is of bandwidth 3bps. From the image, we can say that there can be a maximum of 3 x 5 = 15 bits on the line. The reason is that, at each second, there are 3 bits on the line and the duration of each bit is 0.33s.

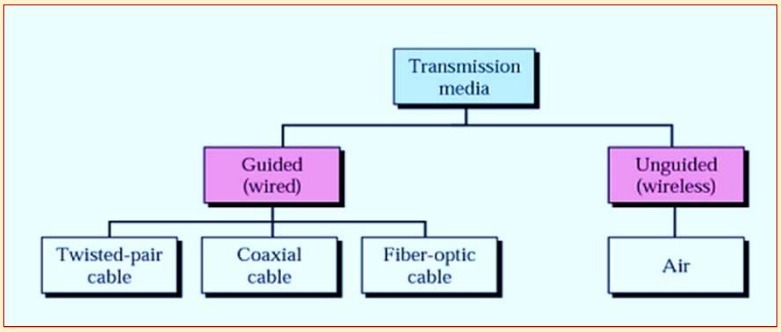
- For both examples, the product of bandwidth and delay is the number of bits that can fill the link.
- It gives the maximum amount of data that can be transmitted by the sender at a given time before waiting for acknowledgment

5. Jitter

- Jitter is another performance issue related to delay. In technical terms, jitter is a "packet delay variance".
- It can simply mean that jitter is considered as a problem when different packets of data face different delays in a network and the data at the receiver application is time-sensitive, i.e. audio or video data.
- Jitter is measured in milliseconds(ms).
- It is defined as an interference in the normal order of sending data packets.

TRANSMISSION MEDIA

- A transmission medium can be broadly defined as anything that can carry information from a source to a destination



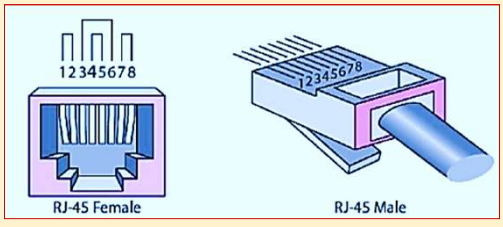
❖Twisted-Pair Cable

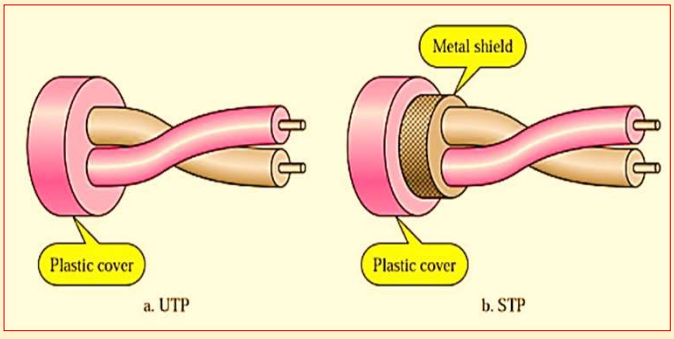
- A twisted pair consists of two conductors (normally copper), each with its own plastic insulation, twisted together.
- One of the wires is used to carry signals to the receiver, and the other is used only as a ground reference. The receiver uses the difference between the two.
- Noise and crosstalk may affect both wires and create unwanted signals.
- In one twist, one wire is closer to the noise source and the other is farther; in the next twist, the reverse is true.
- Twisting makes it probable that both wires are equally affected by external influences (noise or crosstalk).

- This means that the receiver, which calculates the difference between the two, receives no unwanted signals. The unwanted signals are mostly canceled out.
- The number of twists per unit of length (e.g., inch) has some effect on the quality of the cable.

- The most common twisted-pair cable used in communications is referred to as **unshielded twisted-pair (UTP).** IBM has also produced a version of twisted-pair cable for its use called **shielded twisted-pair (STP).**

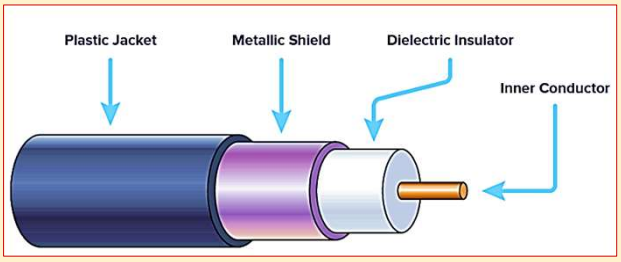
- The most common UTP connector is **RJ45** (RJ stands for registered jack)
- Twisted-pair cables are used in telephone lines to provide voice and data channels. Local-area networks also use twisted-pair cables.





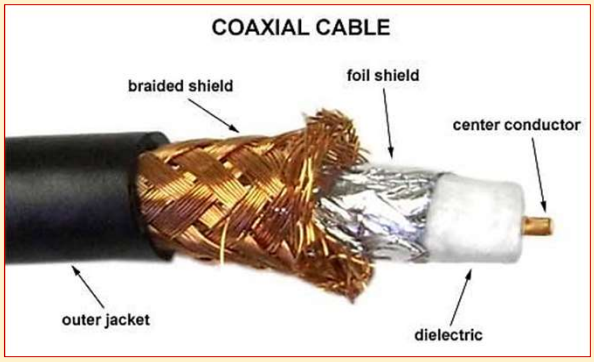
❖Coaxial Cable

- Coaxial cable (or coax) carries signals of higher frequency ranges than those in twisted pair cable.
- Instead of having two wires, coax has a central core conductor of solid or stranded wire (usually copper) enclosed in an insulating sheath, which is, in turn, encased in an 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 second conductor, which completes the circuit.
- This outer conductor is also enclosed in an insulating sheath, and the whole cable is protected by a plastic cover.



Category	*Impedance*	*Use*
RG-59	75 Ω	Cable TV
RG-58	50 Ω	Thin Ethernet
RG-ll	50 Ω	Thick Ethernet

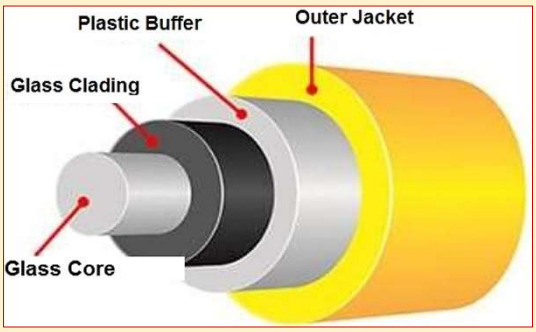
- Coaxial cables are categorized by their radio government (RG) ratings.
- To connect coaxial cable to devices, we need coaxial connectors. The most common type of connector used today is the Bayone-Neill-Concelman (BNC) connector.

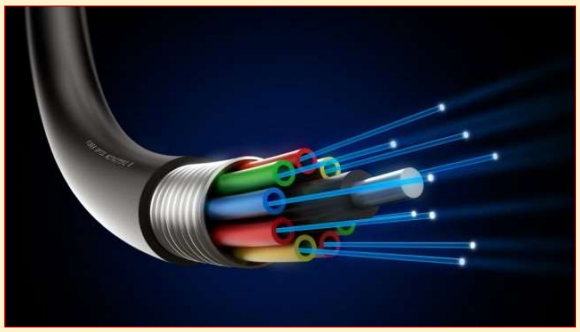


- Coaxial cable was widely used in analog telephone networks.
- Cable TV networks also use coaxial cables.
- Another common application of coaxial cable is in traditional Ethernet LANs

❖Fiber-Optic Cable

- A fiber-optic cable is made of glass or plastic and transmits signals in the form of light.
- Optical fibers use reflection to guide light through a channel. A glass or plastic core is surrounded by a cladding of less dense glass or plastic
- Current technology supports two modes (multimode and single mode) for propagating light along optical channels, each requiring fiber with different physical characteristics.
- Multimode can be implemented in two forms: step-index or graded-index.





- There are three types of connectors for fiber-optic cables
- The subscriber channel (SC) connector is used for cable TV. It uses a push/pull locking system. The straight-tip (ST) connector is used for connecting cable to networking devices. It uses a bayonet locking system and is more reliable than SC. MT-RJ is a connector that is the same size as RJ45.

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

➢ **Advantages:**

✓Higher bandwidth.

✓Less signal attenuation.

✓Immunity to electromagnetic interference.

✓Resistance to corrosive materials.

✓Light weight.

✓Greater immunity to tapping.

➢ **Disadvantages:**

✓Installation and maintenance

✓Unidirectional light propagation

✓Cost

UNGUIDED MEDIA (WIRELESS)

- Unguided media transport electromagnetic waves without using a physical conductor.
- This type of communication is often referred to as wireless communication. Signals are normally broadcast through free space and thus are available to anyone who has a device capable of receiving them.
- Unguided signals can travel from the source to destination in several ways: **ground propagation**, **sky propagation**, and **line-of-sight propagation**

❖ground propagation

- Radio waves travel through the lowest portion of the atmosphere, hugging the earth.
- These low-frequency signals emanate in all directions from the transmitting antenna and follow the curvature of the planet.
- Distance depends on the amount of power in the signal: The greater the power, the greater the distance

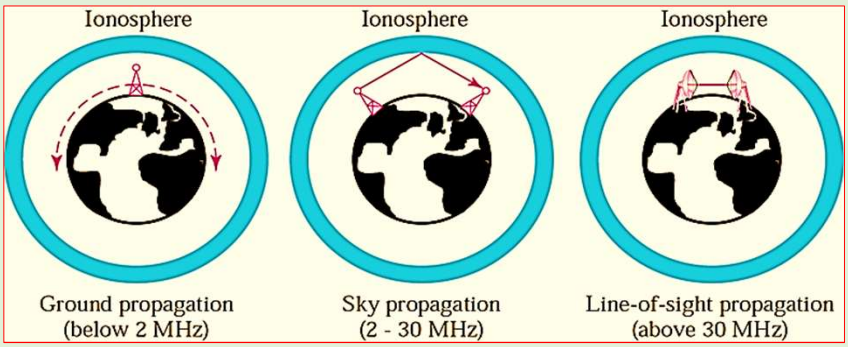
❖Sky propagation

- Higher-frequency radio waves radiate upward into the ionosphere (the layer of atmosphere where particles exist as ions) where they are reflected back to earth.

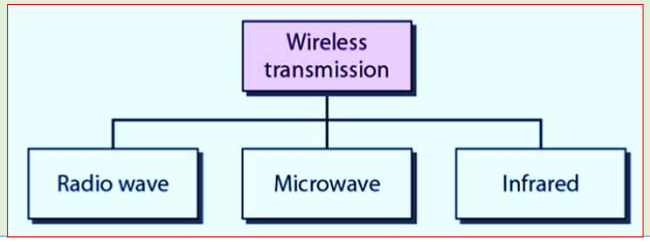
- This type of transmission allows for greater distances with lower output power.

❖Line-of-sight propagation

- Very high-frequency signals are transmitted in straight lines directly from antenna to antenna.
- Antennas must be directional, facing each other and either tall enough or close enough together not to be affected by the curvature of the earth.
- Line-of-sight propagation is tricky because radio transmissions cannot be completely focused.



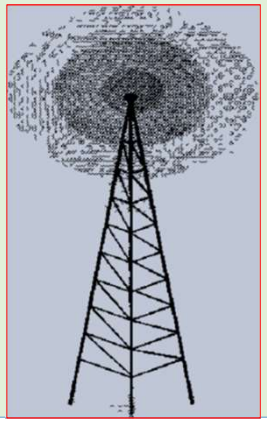
❖Wireless Transmission Waves



❖Radio Waves

- Electromagnetic waves ranging in frequencies between 3 kHz and 1 GHz are normally called radio waves.
- Radio waves are omnidirectional and use omnidirectional antennas.
- 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.
- Radio waves that propagate in the sky mode, can travel long distances. This makes radio waves a good candidate for long-distance broadcasting such as AM radio

- Radio waves, particularly those of low and medium frequencies, can penetrate walls
- Radio waves are used for multicast communications, such as radio and television, and paging systems.



Omnidirectional antenna

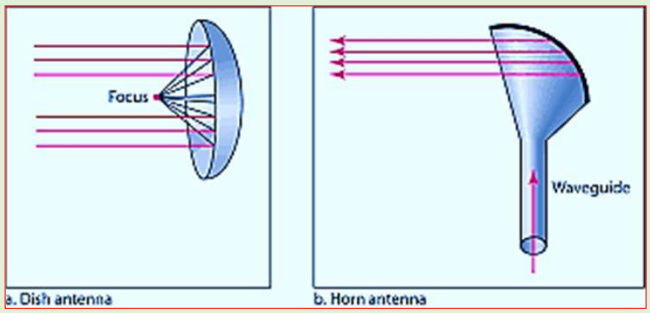
❖Microwaves

- Electromagnetic waves having frequencies between 1 and 300 GHz are called microwaves.
- Microwaves are unidirectional.
- The sending and receiving antennas need to be aligned.

➢Characteristics of microwave propagation:

- Microwave propagation is line-of-sight
- Very high-frequency microwaves cannot penetrate walls
- The microwave band is relatively wide, almost 299 GHz
- Use of certain portions of the band requires permission from authorities

- Microwaves need unidirectional antennas that send out signals in one direction.

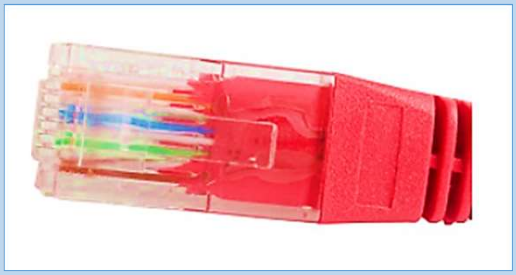


- Microwaves are very useful when unicast (one-to-one) communication is needed between the sender and the receiver.
- They are used in cellular phones, satellite networks and wireless LANs.

❖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.
- Infrared signals useless for long-range communication.
- We cannot use infrared waves outside a building because the sun's rays contain infrared waves that can interfere with the communication
- The Infrared Data Association (IrDA)has established standards for using these signals for communication between devices such as keyboards, mice, PCs, and printers.

RJ 45 Connector



network interface card (NIC)

Router

PHYSICAL LAYER DEVICES

1. Repeater

- A repeater operates at the physical layer.
- Its job is to regenerate the signal over the same network before the signal becomes too weak or corrupted so as to extend the length to which the signal can be transmitted over the same network.
- An important point to be noted about repeaters is that they do not amplify the signal.
- When the signal becomes weak, they copy the signal bit by bit and regenerate it at the original strength.
- It is a 2 port device.

2. Hub

- A hub is basically a multiport repeater.
- A hub connects multiple wires coming from different branches, for example, the connector in star topology which connects different stations.
- Hubs cannot filter data, so data packets are sent to all connected devices.
- Transmission mode is half duplex.
- Also, they do not have the intelligence to find out the best path for data packets which leads to inefficiencies and wastage.

❖Types of Hub

➢Active Hub

- These are the hubs that have their own power supply and can clean, boost, and relay the signal along with the network.
- Active hubs amplify and regenerate the incoming electrical signals before broadcasting them

• Passive Hub

- These are the hubs that collect wiring from nodes and power supply from the active hub.
- Can't be used to extend the distance between nodes.

➢Intelligent Hub

- It works like active hubs and includes remote management capabilities.
- They also provide flexible data rates to network devices.
- It also enables an administrator to monitor the traffic passing through the hub and to configure each port in the hub.