DATA COMMUNICATIONS

→ When we communicate, we are sharing inf(n). This sharing can be local or remote.

→ Between individuals, local com(n) usually occurs face to face, while remote com(n) takes place over distance.

→ Data refers to information presented in whatever form is agreed upon by the parties creating and using data.

→ Data Communications are the exchange of data b/w two devices via some form of transmission medium such as wire cable.

↳ For data communication, the communicating devices must be part of com(n) system made up of combination of h/w (physical equipment) and s/w (programs).

→ The effectiveness of a data comm(n) system depends on four characteristics.

(1) Delivery — The system must deliver data to the correct destination.

— Data must be received by the intended device/user and only by that device/user.

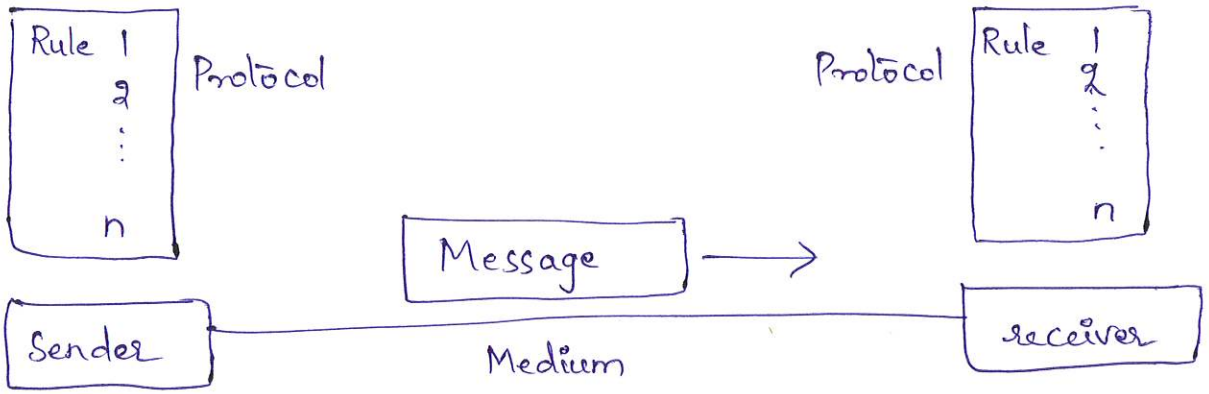
(2) Accuracy — The system must deliver the data accurately. Data that have been altered in transmission and left uncorrected are unusable.

(3) Timeliness — The system must deliver data in a timely manner. Data delivered late are useless.

↳ Delivering data as they are produced without significant delay is called real-time transmission.

(4) Jitter — Jitter refers to the variation in the packet arrival time.

⟹ Components :- A data com(n) system has five components



(1) Message — The message is the inf(n) (data) to be communicated.

— Eg:- text, numbers, pictures, audio and video.

(2) Sender — The sender is the device that sends the message.

Eg:- computer, workstation, video camera

(3) Receiver — The receiver is the device that receives the message.

(4) Transmission medium — It is the physical path by which a message travels from sender to receiver. Eg:- twisted-pair wire, coaxial cable fiber optic cable & radio waves.

(5) Protocol — A protocol is a set of rules that govern the data communications.

— It represents an agreement b/w the communicating devices. Without protocol, two devices may be connected, but not communicating.

⟹ Data representation :-

Information may be in any of the form like text, numbers, images, audio & video.

(1) Text — In data comm^(n), text is represented as a bit pattern, a sequence of bits (0s or 1s).

— Different sets of bit patterns have been designed to represent text symbols.

— Each set is called a code and the process of representing symbols is called coding.

Eg :- Unicode, ASCII.

(2) Numbers — Numbers are also represented by bit patterns.

— ASCII code is not used to represent

— No is directly converted to binary no.

(3) Images — Represented by bit patterns.

— An image is composed of matrix of pixels. where each pixel is a small dot.

— The size of the pixel depends on the resolution.

(4) Audio — It refers to the recording / broadcasting of sound or music.

— It is continuous, not discrete.

(5) Video — It refers to the recording / broadcasting of a picture or movie.

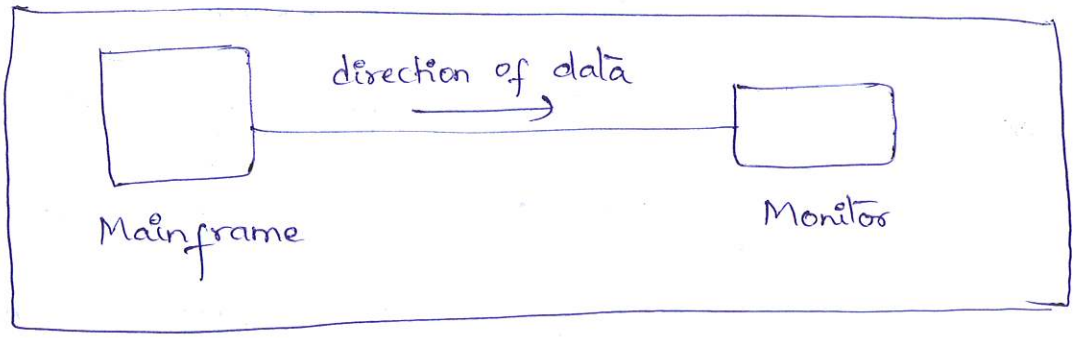
⟹ Data Flow :-

Communication b/w two devices can be simplex, half-duplex or full-duplex.

(1) Simplex :- In this mode, the com(n) is unidirectional as on a one-way. Only one of the two devices on a link can transmit, the other can only receive.

Eg :- Keyboards, monitors.

— The simplex mode can use the entire capacity of the channel to send data in one direction.

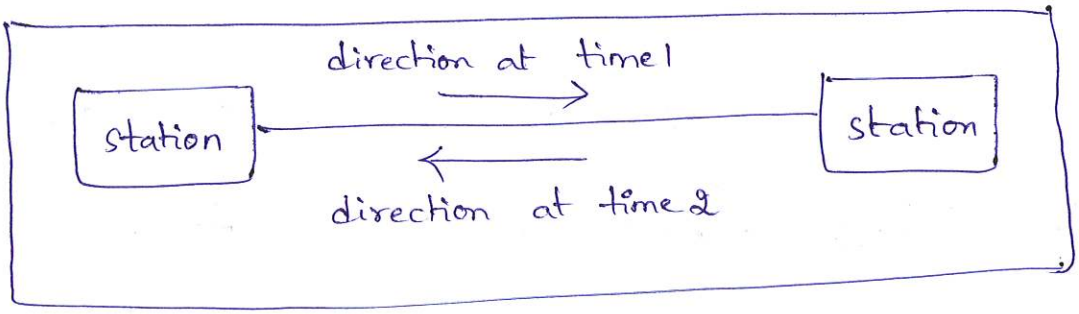


(2) Half - Duplex :-

→ On this mode, each station can both transmit and receive, but not at sametime.

→ When one device is sending, the other can only receive and vice versa.

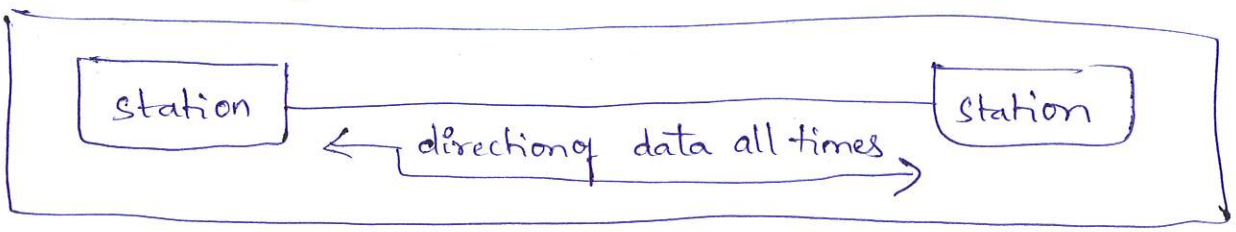
Eg - Walkie - Talkie and CB (Citizens band)



(3) Full - Duplex :- Also called as Duplex.

→ Both stations can transmit and receive simultaneously. Eg - telephone.

→ This mode is a two-way street with traffic flowing in both directions at the same time.



NETWORKS

→ A network is a set of devices (nodes) connected by communication links.

— A node can be computer, printer capable of sending and/or receiving data.

⟹ Distributed processing :-

On this processing, a task is divided among multiple computers. Most networks use distributed processing. CN is a telecommunication channel through which we can share our data. It is also called as data n/w. Ex: Internet

⟹ Network Criteria :- A n/w must be able to meet,

→ performance

→ reliability

→ security

(1) Performance :- It 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 b/w an inquiry and a response.

→ The performance of a n/w depends on no of users, type of transmission medium, the capabilities of connected h/w and efficiency of the s/w.

→ Performance is evaluated by throughput & delay.

(2) Reliability :-

It can be measured by the frequency of failure, the time it takes a link to recover from a failure, the n/w robustness.

(3) Security :-

N/w security issues includes protecting data from unauthorized access, from damage and development and implementing policies & procedures for recovery from breaches and data losses.

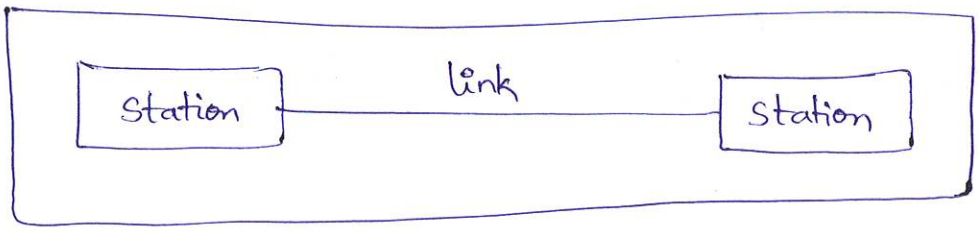
⟹ Physical Structures :- N/w attributes are,

(1) Type of Connection :- A n/w is a link b/w two or more devices. A link is a com(n) pathway that transfers data from one device to another.

There are two possible types.

(a) Point-to-point :-

A point-to-point connection provides a dedicated link b/w devices.

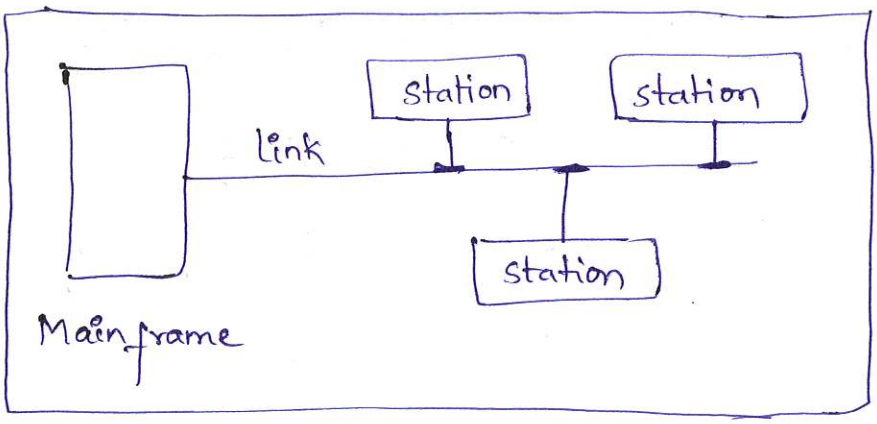


(b) Multipoint :- Also called as multidrop connection, in which more than two specific devices share a single link.

→ If several devices can use the link simultaneously it is a spatially shared connection.

→ If users must take turns, it is a timeshared connection.

(2) Physical topology :-

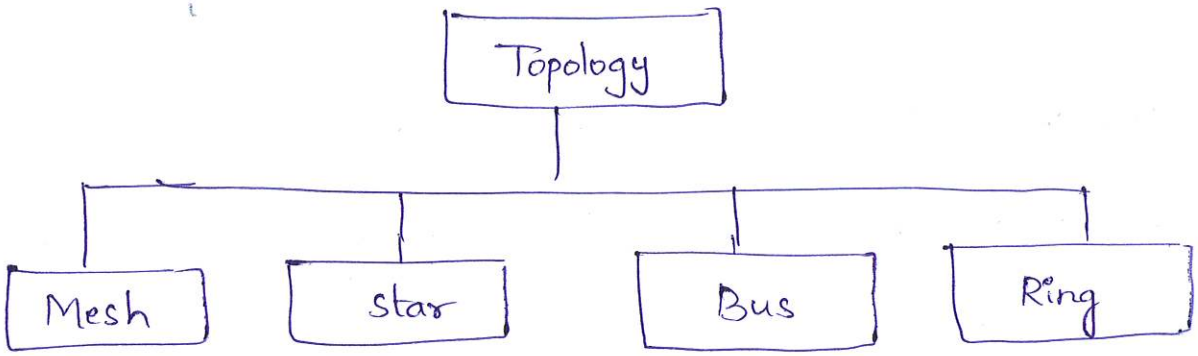


→ physical topology refers to the way in which a n/w is laid out physically.

→ Two or more devices connect to a link, two or more links form a topology.

→ The topology of a n/w is the geometric representation of the relationship of all links and linking devices to one another.

→ There are four basic topologies.



(i) Mesh topology :-

→ In this, every device has a dedicated point-to-point link to every other device.

→ To find the no of physical links in a mesh topology, with 'n' nodes, we need to calculate $n(n-1)/2$

⇒ Advantages :-

(1) The use of dedicated links guarantees that each con(n) can carry its own data load, which eliminates the traffic problems.

(2) It is robust — i.e., if one link is unusable,

it doesn't affect entire system.

(3) Privacy or security — only intended recipient can receive the data.

(4) point-to-point links make fault identification and fault isolation easy.

⟹ Disadvantages :—

(1) Increased Amount of cabling and no of I/O ports.

(2) Every device must be connected to every other device, installation and reconnection are difficult

(3) Bulk of wiring can be greater than the available space.

(4) The h/w required to connect each link can be expensive.

Eg :- Telephone regional offices.

(2) Star topology :—

In this, each device has a dedicated point-to-point link only to a central controller, called a hub.

→ The devices are not directly linked to one another.

→ The controller acts as an exchange — if one device wants to send data to another, it sends to

controller, which then sends to connected device.

→ Advantages :-

(1) Less expensive.

(2) Needs only one link & one I/o port to connect it to any no. of others.

(3) Easy to install and reconfigure.

(4) Robustness – If one link fails, only that link is affected.

(5) Easy fault identification & fault isolation.

→ Disadvantages :-

(1) Dependency of the whole topology on one single point, the hub. If the hub goes down, the whole system is dead.

Eg :- LANs.

(3) Bus topology :-

Note :- This topology is multipoint. One long cable acts as a backbone to link all the devices in a n/w.

→ Nodes are connected to the bus cable by drop lines and taps.

→ A drop line is a con(n) running b/w the device and the main cable.

→ A tap is a connector.

⟹ Advantages :-

(1) Ease of installation.

(2) Requires less cabling.

⟹ Disadvantages :-

(1) Difficult reconnection and fault isolation.

(2) A fault or break in the bus cable stops all transmission.

Eg :- Ethernet LANs.

(4) Ring topology :-

On this, each device has a dedicated point-to-point connection with only two devices on either side of it.

→ Signal is passed along the ring in one direction from device to device, until it reaches destination.

→ Each device in the ring incorporates a repeater.

⟹ Advantages :—

(1) Easy to install and reconfigure.

↳ Each device is linked only to its immediate neighbors. So to add/delete devices requires changing only two connections.

(2) Fault isolation is simplified.

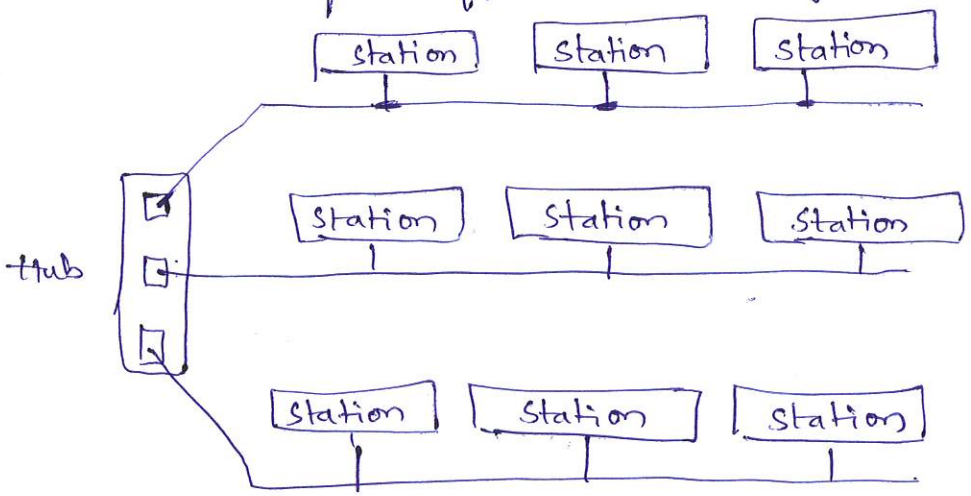
⟹ Disadvantages :—

(1) Unidirectional traffic.

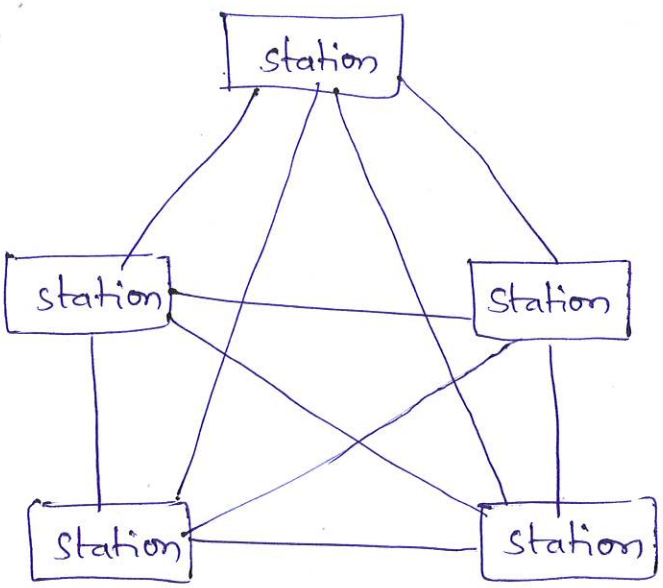
Eg :- higher-speed LANs.

(4) Hybrid topology :— A n/w can be hybrid.

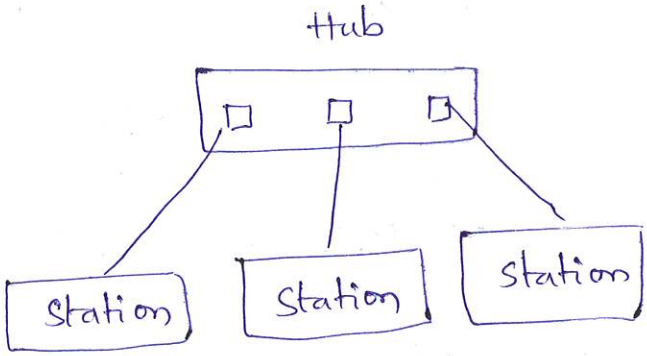
Combination of different topologies.



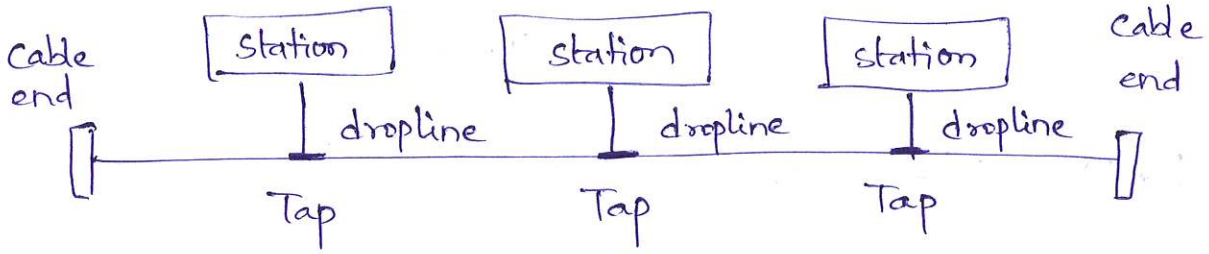
Mesh topology



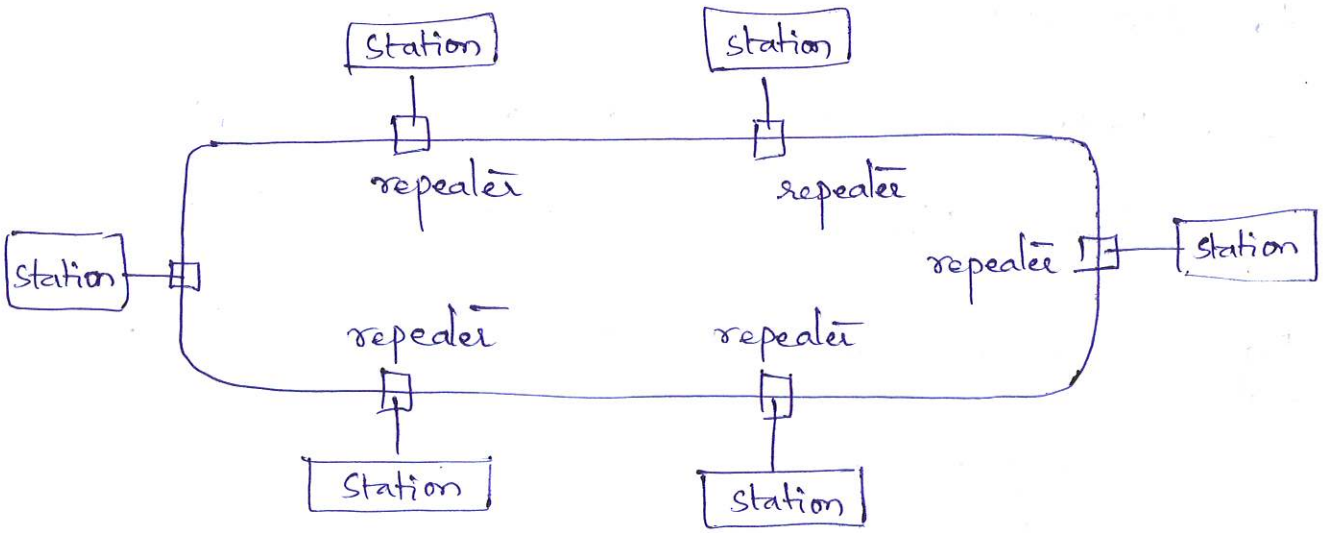
Star topology



Bus topology



Ring topology



⟹ Network Models :-

(1) OSI — The Open Systems Interconnection model defines a seven layer n/w.

(2) Internet model — defines a five layer n/w.

⟹ Categories of networks :-

There aree three different types of networks categories.

(1) LAN
(2) WAN
(3) MAN

(1) LAN (Local Area Network) :-

A LAN is privately owned and links the devices in a single office. LAN can be limited to few kilometers.

→ LANs are designed to allow resources to be shared b/w personal computers or workstations.

Eg:- Business environments, accounting PCs, engineering workstations.

→ Most common LAN topologies are bus, ring, star. Speed is 100 or 1000 Mbps.

(2) WAN (Wide Area Network) :-

A Wide Area Network provides long distance transmission of data, image, audio and video inf(n) over large geographic areas that may comprise a country, a continent or even the whole world.

Eg :- X.25, asynchronous transfer mode n/w.

(3) MAN :- (Metropolitan Area Networks)

It is a n/w with a size b/w a LAN and a WAN. It normally covers the area inside a town or a city. It is used where high-speed connection is required.

Eg :- telephone company n/w, cable TV n/w.

⟹ Internetwork :-

When two or more networks are connected, they become an internetwork or internet.

INTERNET

→ The Internet is a structured, organized system.

⟹ A brief history :—

A n/w is a group of connected, communicating devices such as computers & printers.

→ An internet is two or more n/w that can communicate with each other.

→ found by ARPA (Advanced Research Projects Agency). ARPA presented its ideas for ARPANET, a small n/w of connected computers.

→ on this, each computer is attached to a specialized computers, called an IMP (Interface Message Processor).

→ A s/w called NCP (N/w Control Protocol) provided com^(n) b/w the hosts.

PROTOCOLS AND STANDARDS.

→ Protocols is nothing but rules.

→ Standards means agreed-upon rules.

⟹ Protocols :-

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 – It refers to the structure or format of data, meaning the order in which they are presented.

→ Semantics – It refers to the meaning of each section of bits.

→ Timing – It refers to two characteristics

(1) When data should be sent.

(2) How fast they can be sent.

⟹ Standards :-

Data communication standards fall into two categories. 1. de facto (by fact / by convention)

2. de jure (by law / by regulation).

⇒ Standards Organizations :-

1. ISO (International Organization for Standardization)
2. ITU-T (International Telecommunication Union Telecommunication Standards Sector).
3. ANSI (American National Standards Institute)
4. IEEE (Institute of Electrical and Electronics Engineers)
5. EIA (Electronic Industries Association)

⇒ Internet Standards :-

An internet standard is a thoroughly tested specification that is useful to those who work with the internet.

Layering in computer networks :-

In computer programming, layering is the organization of programming into separate functional (programming) components that interact in some sequential and hierarchical way, with each layer usually having an interface only to the layer above it and the layer below it.

Ex. OSI is two multilayered, TCP/IP is example of two layer.

OSI MODEL

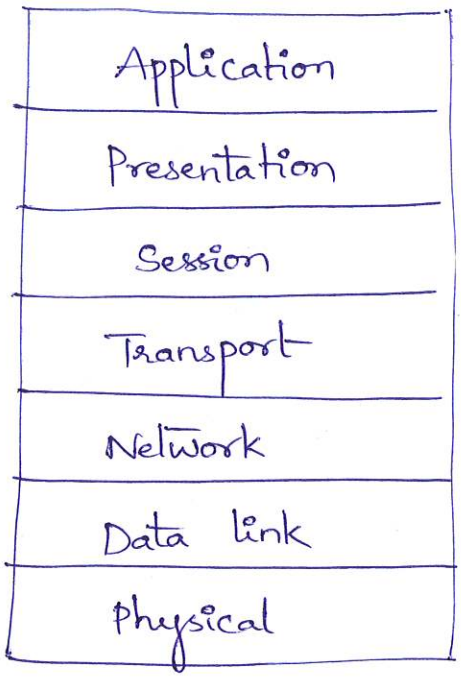
An open system is a set of protocols that allows any two different systems to communicate regardless of their underlying architecture.

The purpose of the OSI model is to show how to facilitate com(n) b/w different systems without requiring changes to the logic of the underlying h/w & s/w.

→ The OSI model is not a protocol. It is a model for understanding and designing a n/w architecture that is flexible, robust and interoperable.

→ The OSI model is a layered framework for the design of n/w systems that allows com(n) b/w all types of computer systems. It consists of seven separate but related layers, each of which defines a part of the process of moving inf(n) across a n/w.

Seven layers of the OSI model.



(1) Physical layer :-

It is responsible for movement of individual bits from one hop (node) to the next.

→ This layer coordinates the functions required to carry a bit stream over a medium.

→ It deals with the mechanical & electrical specifications of the interface & medium.

→ It also defines the procedures & functions that physical devices & interfaces have to perform for transmission to occur.

(1) physical characteristics of interfaces & medium.

(2) Representation of bits.

(3) Data rate

(4) Synchronization of bits.

(5) Line configuration.

(6) physical topology

(7) Transmission mode.

(2) Data Link Layer :- This layer transforms the physical layer, to a reliable link.

This layer is responsible for moving frames from one hop to the next.

⟶ It makes the physical layer appear error-free to the upper layer.

(1) Framing

(2) physical addressing.

(3) flow control

(4) Error control

(5) Access control.

(3) Network layer :- It is responsible for the delivery of individual packets from the source host to the destination host.

⟶ N/w layer ensures that each packet gets from its point of origin to its final destination.

(1) Logical addressing.

(2) Routing

(4) Transport Layer :- This layer is responsible for the delivery of a message from one process to another.

→ A process is an application program running on a host.

→ This layer ensures that the whole message arrives intact and in order.

(1) Service - point addressing.

(2) Segmentation and reassembly.

(3) Connection control.

(4) Flow control

(5) Error control.

(5) Session Layer :- This layer is responsible for dialog control and synchronization.

→ It maintains, establishes and synchronizes the interaction among communicating systems.

(1) Dialog control.

(2) Synchronization.

(6) Presentation Layer :- It is responsible for translation, compression and encryption.

→ It concerned with syntax & semantics of the inf(n) exchanged b/w two systems.

(1) Translation

(2) Encryption

(3) Compression.

(7) Application Layer :- It is responsible for providing services to the user.

→ It provides user interfaces & support for services such as e-mail, remote file access & transfer, shared database management and other types of distributed inf(n) services.

(1) Network virtual terminal

(2) File transfer, access & mgmt.

(3) Mail services.

(4) Directory services.

TCP/IP PROTOCOL SUITE

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

(1) host-to-network

(2) internet

(3) transport

(4) application

→ Host-to-N/W layer is equivalent to the combination of physical & datalink layers.

→ The internet layer is equivalent to the network layer.

→ Application layer is doing the job of session, presentation and application layers.

→ TCP/IP is a hierarchical protocol made up of interactive modules, each of which provides a specific functionality.

→ The term hierarchical means that each upper level protocol is supported by one or more lower-level protocols.

(1) Physical and Datalink layers :-

On these layers, TCP/IP does not define any specific protocol. It supports all the standard and proprietary protocols. A n/w in a TCP/IP internetwork can be a local-area n/w or wide area n/w.

(2) Network layer :-

On this layer, TCP/IP supports the internet working protocol. IP uses four supporting protocols.

ARP (Address Resolution Protocol)

RARP (Reverse Address Resolution Protocol)

ICMP (Internet Control Message Protocol)

IGMP (Internet Group Message Protocol)

(3) Internetworking Protocol :- (IP)

The IP is the transmission mechanism used by the TCP/IP protocols.

→ It is an unreliable and connectionless protocol — a best-effort delivery service.

↳ i.e., IP provides no error checking or tracking.

→ IP transports data in packets called datagrams, each of which is transported separately.

→ Datagrams can travel along different routes and can arrive out of sequence or be duplicated.

→ IP doesn't keep track of the routes and has no facility for reordering datagrams once they arrive at their destination.

(a) ARP :-

It is used to associate a logical address with a physical address.

→ On a physical n/w, each device on a link is identified by a physical or station address usually imprinted on the n/w interface card. (NIC)

→ ARP is used to find the physical address of the node when its Internet address is known.

(b) RARP :-

It allows a host to discover its internet address when it knows only its physical

address. It is used when a computer is connected to a n/w for the first time or when a diskless computer is booted.

(c) ICMP :-

It is a mechanism used by hosts and gateways to send notification of datagram problems back to the sender.

→ ICMP sends query and error reporting messages.

(d) IGMP :-

It is used to facilitate the simultaneous transmission of a message to a group of recipients.

(3) Transport layer :-

This layer was represented in TCP/IP by two protocols. TCP & UDP.

→ IP is a host-to-host protocol, i.e., it can deliver a packet from one physical device to another.

→ UDP & TCP are transport level protocols responsible for delivery of a message from a process to another process.

(a) UDP :- (User Datagram Protocol)

It is a process-to-process protocol that adds only port addresses, checksum error control, and length info(n) to the data from the upperlayer.

(b) TCP :- (Transmission Control Protocol)

It provides full transport-layer services to applications.

→ TCP is a reliable stream transport protocol.

→ Stream means connection-oriented.

→ A connection must be established b/w both ends of a transmission before either can transmit data.

→ At the sending end of each transmission, TCP divides a stream of data into smaller units called segments.

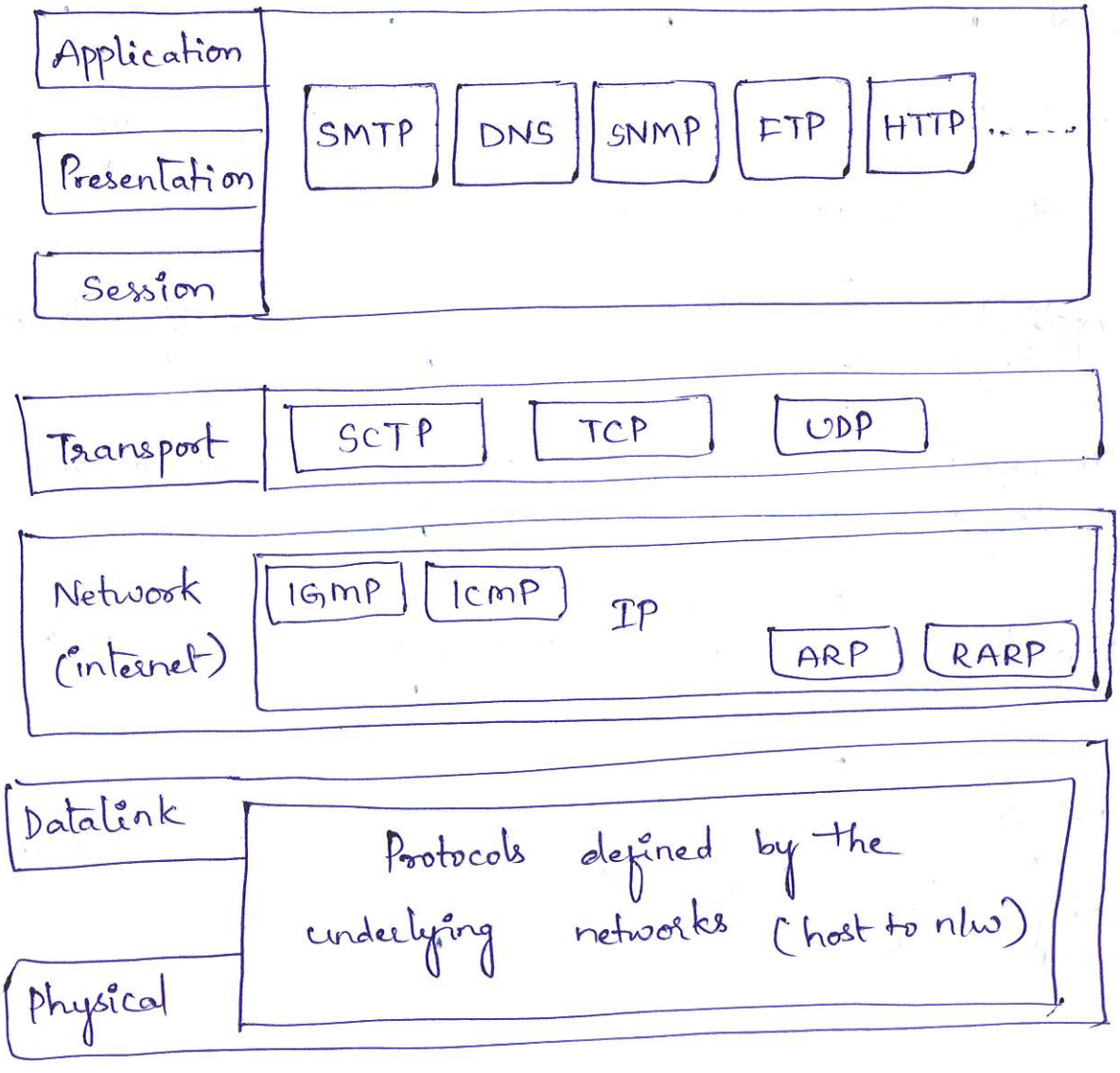
(c) SCTP :- (Stream Control Transmission Protocol)

It provides support for newer applications such as voice over the internet. It is a transport layer protocol that combines the best features of UDP & TCP.

(4) Application Layer :- It is equivalent to the combined session, presentation and application layers, in OSI model. The protocols defined are,

- SMTP (Simple Mail Transfer Protocol)
- SNMP (Simple N/w Message Protocol)
- FTP (File Transfer Protocol)
- HTTP (Hyper Text Transfer Protocol)
- DNS (Domain Name System)
- TELNET (Terminal Network)

TCP/IP and OSI model



ADDRESSING

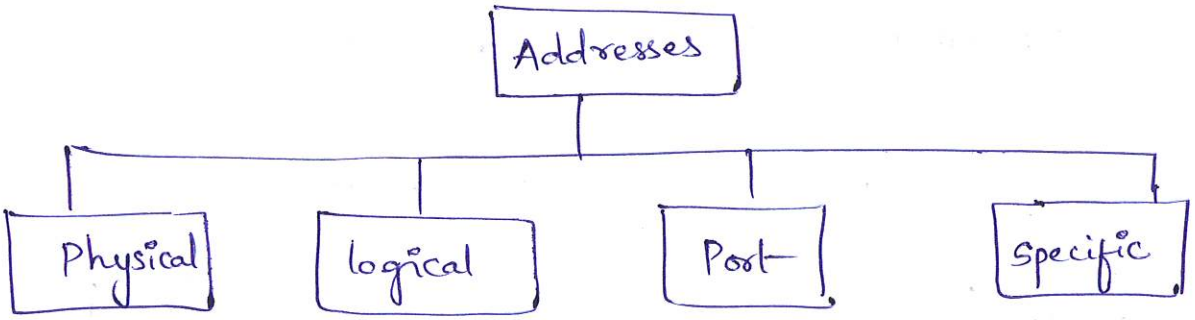
Four levels of addresses are used in TCP/IP protocols.

(1) physical (link) addresses

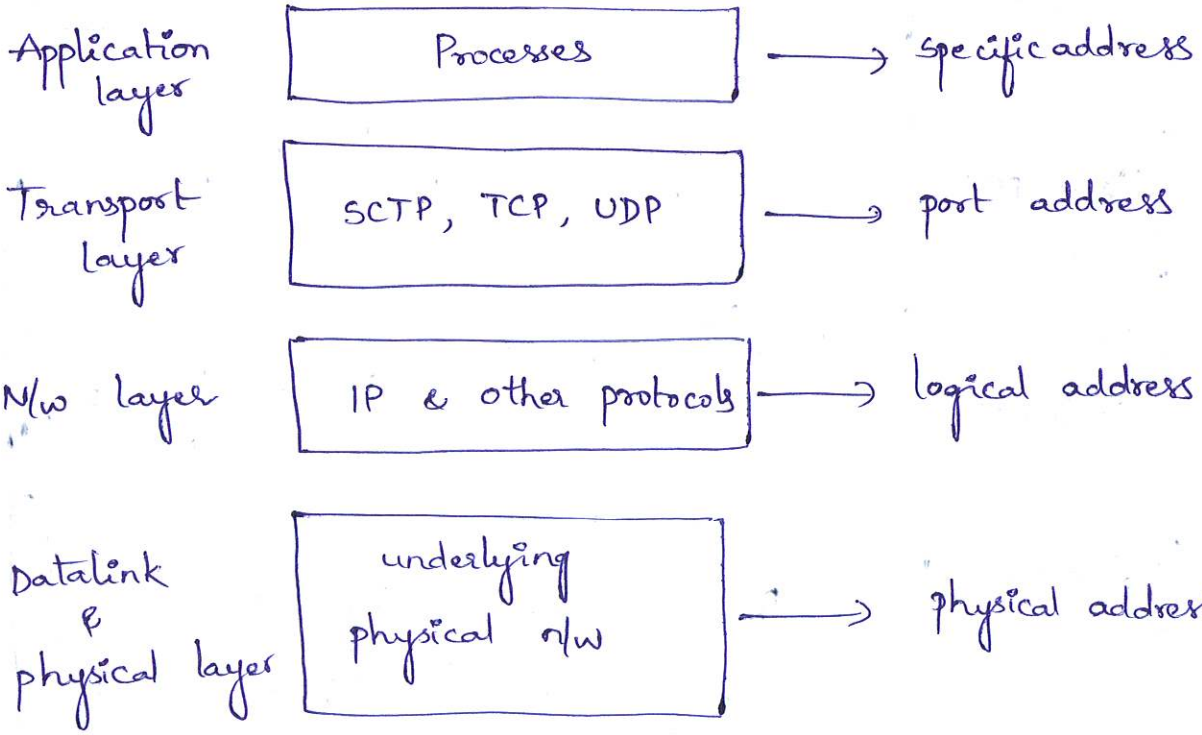
(2) Logical (IP) addresses

(3) port addresses

(4) specific addresses



→ Each address is related to a specific layer in the TCP/IP architecture.



(1) Physical Addresses :-

→ These are known as link addresses.

→ It is the address of a node as defined by its LAN or WAN.

→ It is included in the frame used by the data link layer. It is the lowest-level address.

→ The size & format of these addresses vary depending on the n/w.

(2) Logical Addresses :-

A logical address in the Internet is currently a 32-bit address that can uniquely define a host connected to the n/w.

Note :- No two hosts on the internet can have the same IP address.

⟹ The physical addresses will change from hop to hop, but the logical addresses usually remain the same.

(3) Port Addresses :- On TCP/IP architecture, the label assigned to a process is called a port address.

→ A port address is 16 bits in length.

→ The objective of internet com(n) is a process communicating with another process.

→ 16-bit port address represented as one single number.

(4) Specific Addresses :—

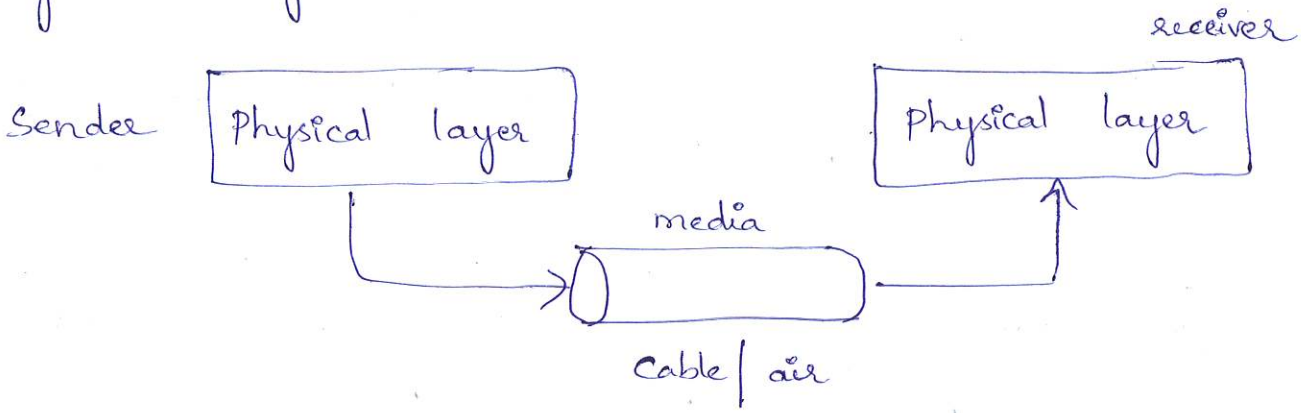
Some applications have user-friendly addresses that are designed for that specific address.

Eg :- e-mail address, URL

→ These addresses get changed to the corresponding port and logical addresses by the sending computer.

TRANSMISSION MEDIA

Transmission media are actually located below the physical layer and directly controlled by the physical layer.



⟹ Transmission media can be broadly defined as anything that can carry inf(n) from a source to a destination.

⟶ On data comm(n),

↳ The transmission medium is a free space, metallic cable or fiber optic cable.

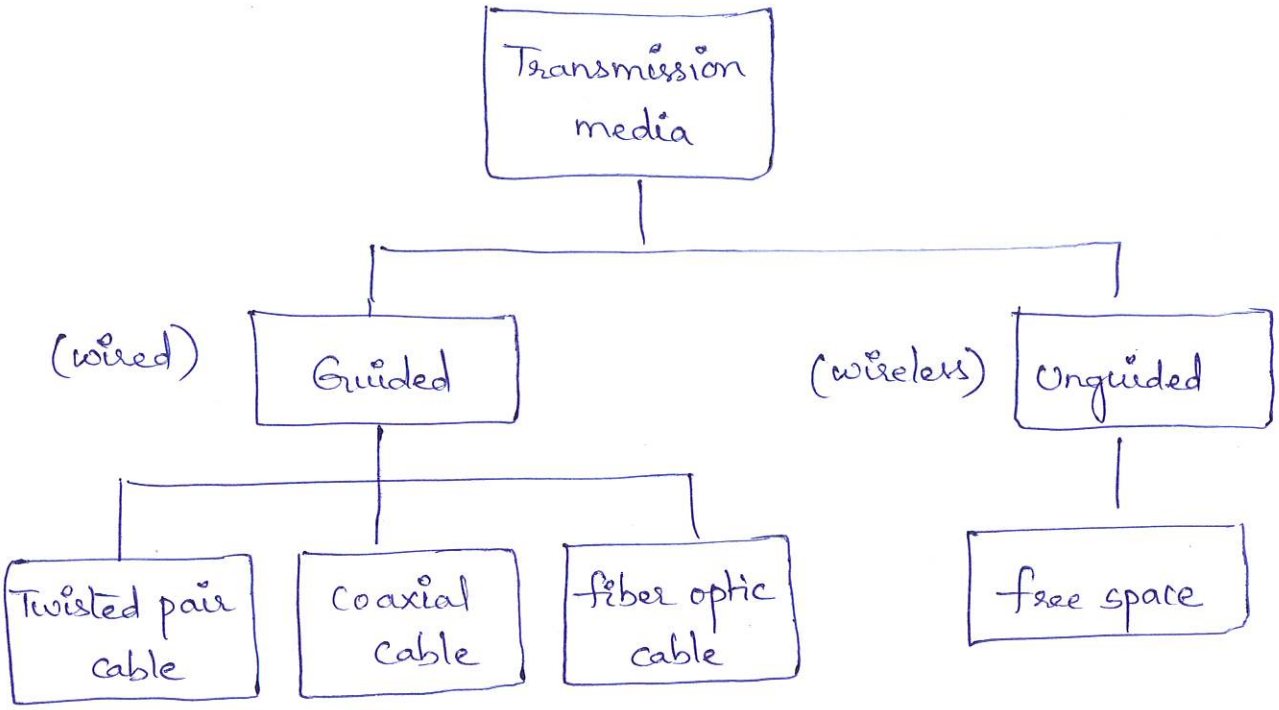
↳ The inf(n) is a signal that is a result of a conversion of data from another form.

⟶ On telecommunications, transmission media can be divided into two broad categories.

(a) Guided (twisted pair, coaxial, fiberoptic)

(b) Unguided (free space).

Classes of transmission media



GUIDED MEDIA

Guided media include twisted-pair cable, coaxial cable and fiber-optic cable.

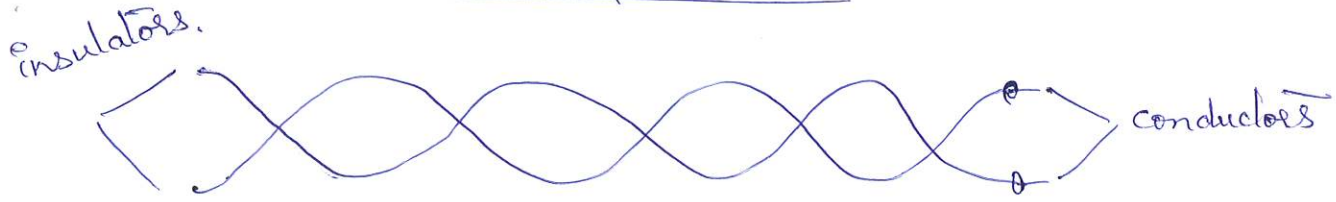
→ Twisted-pair and Coaxial cable use metallic (copper) conductors that accept and transport signals in the form of electronic current.

→ Optical fiber is a cable that accepts and transports signals in the form of light.

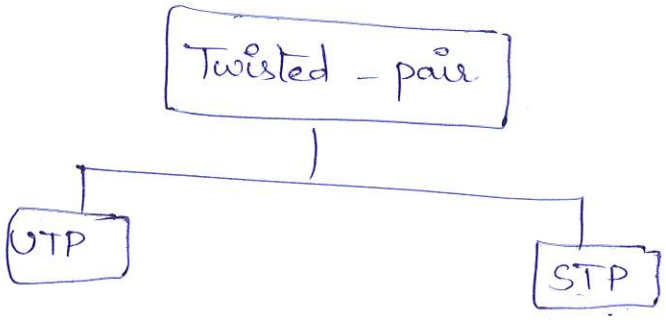
(1) Twisted-Pair Cable :-

A twisted-pair consists of two conductors each with its own plastic insulation, twisted together,

Twisted pair cable.



→ One of the wires is used to carry signals to the receiver, and the other is used as a ground reference. The receiver uses the difference b/w the two.



→ The most common twisted-pair cable used in com(n) is referred to as Unshielded Twisted Pair.

⟹ UTP :-

→ It is a set of twisted pairs of cable within a plastic sheet. It is an ordinary telephone wire.

→ This is the least expensive of all transmission media, commonly used for LAN, easy to work and simple to install.

→ UTP is used in computer n/w. It can transfer

data at 1 to 100 Mbps over 100 meters.

→ EIA developed 5 different categories based on quality.

⇒ Characteristics of UTP :-

(1) Transmission rate of 10 - 100 Mbps.

(2) Less expensive than FOC & co-axial

(3) Max cable length is 100 m.

(4) Very flexible & easy to work.

(5) UTP uses RJ-45 Connector (Registered Jack)

⇒ Advantages of UTP :-

(1) It is easy to terminate.

(2) Cost of installation is less.

(3) High installed base.

⇒ Disadvantages of UTP :-

(1) It is very noisy.

(2) It covers less distance.

(3) Suffers from interference.

3 ⟹ STP:- (Shielded Twisted Pair)

→ It offers a protective sheathing around copper wire. STP provides better performance at lower data rates.

→ This is not commonly used in n/w.

→ Installation of STP is easy. Special connectors are used for installation.

→ Cost is expensive.

→ Distance is limited to 100m to 500m.

→ It suffers from outside interference.

⟹ Applications of Twisted-pair :-

(1) TP cable used for both analog & digital signals.

(2) TP cables are used in telephone n/w.

(3) LAN also use these TP cables.

(2) Coaxial Cable :-

→ It is made up of two conductors that share common axis. It consists of a hollow outer cylindrical conductor that surrounds a single inner wire conductor.

→ It carries signals of higher frequency ranges.

→ This is used to transmit both analog & digital signals.

→ Coaxial cables are categorized by Radio Government (RG) ratings.

↳ categories are,

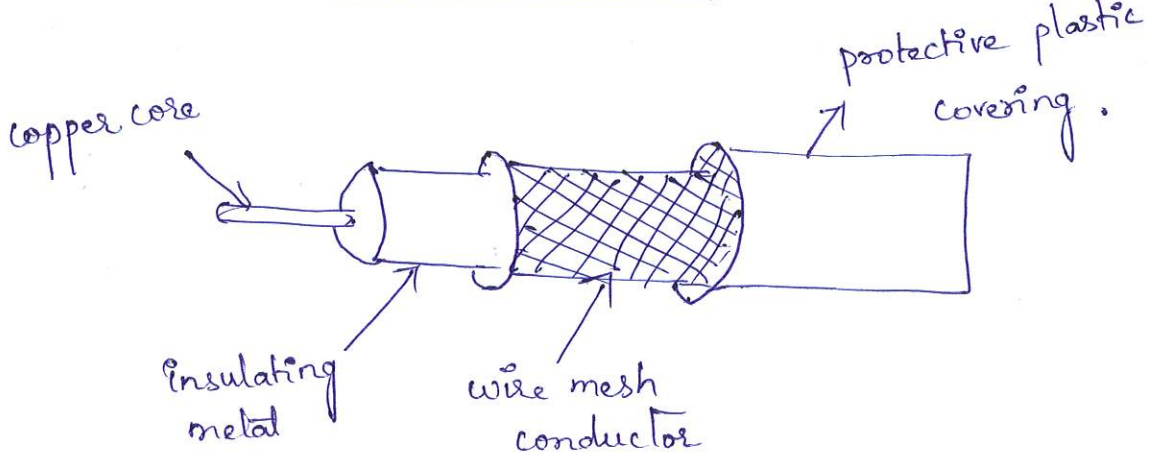
* RG-59 → Cable TV
* RG-58 → Thin ethernet
* RG-11 → thick ethernet.

→ It is inexpensive. The cost for thin coaxial cable is less than STP. Thick co-axial is more expensive than STP.

→ Installation is simple.

→ Coaxial cable is grounded & terminated.

co-axial cable



4 ⟹ Characteristics of co-axial cable :-

(1) 10 Mbps is transmission rate.

(2) Max cable length for thinnet is 185 meters and for thicknet is 500 meters.

(3) Flexible and easy to work with thinnet.

(4) Ethernet designation to 10 Base 2 (thinnet) or 10 Base 5 (thicknet).

(5) Less expensive than fiber optics cable but more expensive than TP.

(6) Good resistance to electrical interference.

⟹ Advantages :-

(1) It is used for both (digital-data & analog data) transmission.

(2) It has higher bandwidth.

(3) Easy to handle & relatively inexpensive as compared to fiber optic cables.

(4) It uses for longer distances at higher data rates.

(5) Excellent noise immunity.

(6) It use BNC Connector.

⟹ Disadvantages :-

(1) Distance is limited.

(2) No of node connection is limited.

(3) Proper connectors and termination is must.

⟹ Applications :-

(1) In analog & digital data transmission.

(2) telephone n/w.

(3) ethernet LANs.

(4) television n/w.

(3) Fiber optic Cable :- (FOC)

A fiber optic cable is made of glass or plastic and transmits signals in the form of light.

⟶ Light is an electromagnetic signal and can be modulated by inf(n).

⟶ FOC transmits light signals rather than electrical signals.

⟶ Cable may contain a single fiber, fibers are bundled together in the centre of cable.

⟶ FOC may be single mode or multimode.

5 → Multimode fibers use multiple light paths where as singlemode fibers allows a single light-path and used with laser signalling. It has greater bandwidth.

→ There are 3 types of connectors.

* SC connector (Subscriber channel)
  ↳ used for cable TV.
* ST Connector (straight-tip).
  ↳ used for cable n/w devices.
* MT-RJ connector (similar to RJ45).

⟹ Characteristics :-

(1) Transmission rate of 100 Mbps ✓
(2) Not affected by electrical interference.
(3) Most expensive cable. ✓
(4) FOC supports cable length of 2Km or more
(5) It supports voice, video and data.
(6) It provides most secured media.
(7) Used as backbones b/w buildings and token ring n/w.
(8) Not very flexible, difficult to work.

⟹ Applications :-

⟶ LAN (100 Base - FX n/w (Fast Ethernet) and 1000 Base - X) use fiber - optic cable.

⟹ Advantages :-

(1) Higher bandwidth.

(2) Less signal attenuation.

(3) Immunity to electromagnetic interference.

(4) Resistance to corrosive materials.

(5) Light weight

(6) Greater immunity to tapping.

⟹ Disadvantages :-

(1) Installation & maintenance.

(2) Unidirectional light propagation.

(3) Cost.

UNGUIDED MEDIA

→ Unguided media transport electromagnetic waves without using a physical conductor. This type of com$^{(n)}$ is referred to as Wireless com$^{(n)}$.

→ Signals are normally broadcast through free space

→ Unguided signals can travel from source to destination in several ways.

(1) ground propagation ✓

(2) sky propagation ✓

(3) line-of-sight propagation ✓

→ (1) On ground propagation, radio waves travel through the lowest portion of the atmosphere, hugging the earth.

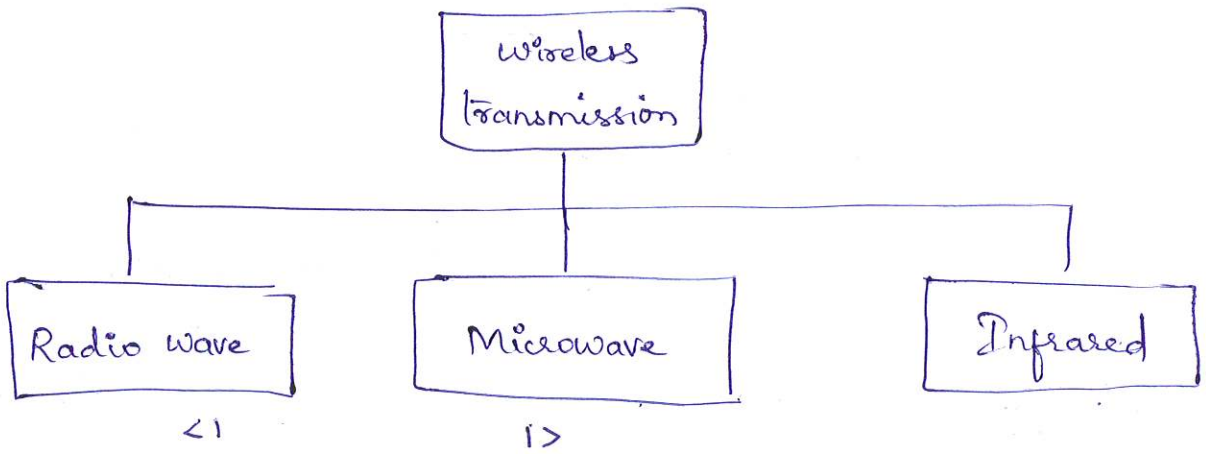
↳ Distance depends on power (amount of) in signal. The greater the distance (ie the greater the power)

→ (2) On sky propation, higher-frequency radio waves radiates upward into the ionosphere, where they are reflected back to earth.

↳ This allows for greater distances with lower o/p power.

→ (3) on line-of sight propagation, very high-freq. signals are transmitted in straight lines directly from antenna to antenna.

Wireless transmission can be divided into three broad groups.



(1) Radio Waves :-

→ The electromagnetic waves ranging in frequencies b/w 3 KHz and 1 GHz are called radio waves.

→ These are Omnidirectional, which send out signals in all directions.

→ Can travel long distances.

⟹ Applications :-

(1) Used for multicasting.

(2) AM & FM radios, televisions, cordless phones and paging.

(2) Microwaves :-

Electromagnetic waves having frequencies b/w 1 and 300 GHzs are called microwaves.

⟶ Microwaves are unidirectional, sendout signals in one direction.

⟹ Characteristics of microwave propagation;

(1) Line of sight

(2) Very high - freq. waves can't penetrate walls.

(3) The microwave band is relatively wide almost, 299 GHz.

(4) Use of certain portions of the band requires permission from authorities.

⟹ Applications :-

(1) Cellular phones.

(2) Satellite n/w.

(3) Wireless LANs.

(3) Infrared :-

→ The waves with frequencies from 300 GHz to 400 THz are called infrared waves.

→ Used for short-range com(n).

→ Having high frequencies.

→ Applications :-

(1) Keywords, mice, PCs & printers.

(2) Indoor LANS.

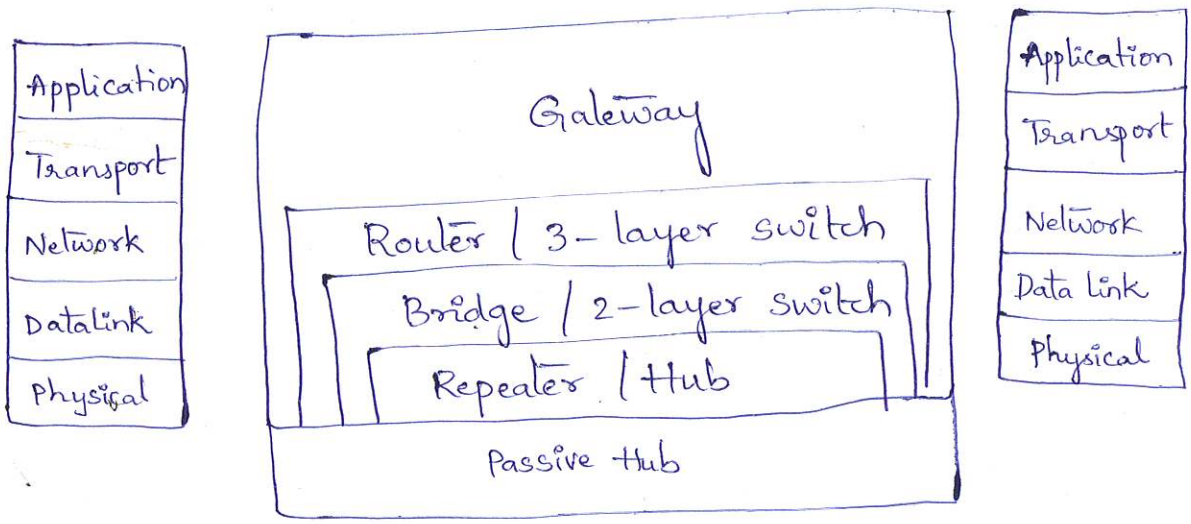
Comparison of UTP & STP.

S.No.	Parameter	UTP	STP
1.	Data rate	10-100 Mbps	150 Mbps.
2.	Cable length	100 meters	500 m.
3.	electrical - interference	Most susceptible to crosstalk	less susceptible to crosstalk.
4.	Installation	easy to install.	very easy to install.
5.	Cost	lowest	little costly.

Connecting Devices

→ Connecting devices are divided into five different types based on the layer in which they operate in a n/w.

→ The device which operates below the physical layer such as passive hub.



→ A repealer or an active hub operales at the physical layer.

→ A bridge or a 2-layer switch operales at the physical and data link layers.

→ A router or layer three switch operates at the physical, data link and n/w layers.

→ Those which can operates at all five layers (i.e., galeway)

(1) Hubs :-

→ All networks require a central location to bring media segment together. These central locations are called hubs.

→ Hubs are special repeaters that overcome the electromechanical limitations of a media signal path.

→ The hub organizes the cables and transmits incoming signals to the other media segments.

→ There are three main types of hubs.

(1) passive
(2) Active
(3) Intelligent.

(1) Passive hub :-

→ It is just a "connector".

→ It combines the signals of n/w segments.

→ There is no signal regeneration.

→ It is a type of transmission media.

9 → Its location in the internet model is below the physical layer.

→ The hub is the collision point. A passive hub reduces by half the max. cabling distances permitted.

↳ With passive hub, each computer receives the signal sent from all the other computers connected the hub.

(2) Active hub :-

→ An active hub is actually a multiport repeater

→ It regenerates or amplifies the signals.

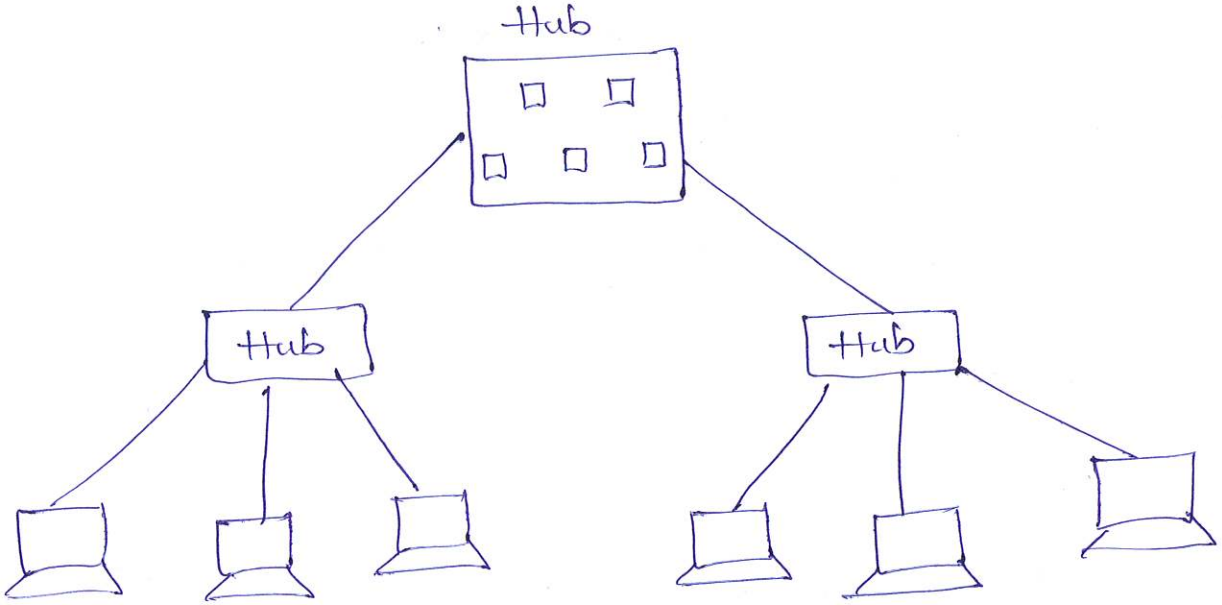
→ By using these the distance b/w devices can be increased.

→ It is normally used to create connections b/w stations in a physical star topology.

→ It is expensive.

→ Hubs can also be used to create multiple levels of hierarchy.

→ Disadvantage is they amplify noise along signals.



Hierarchy of Hubs.

(2) Repealers :-

→ Repealer is an "electronic device". It operates only in the physical layer.

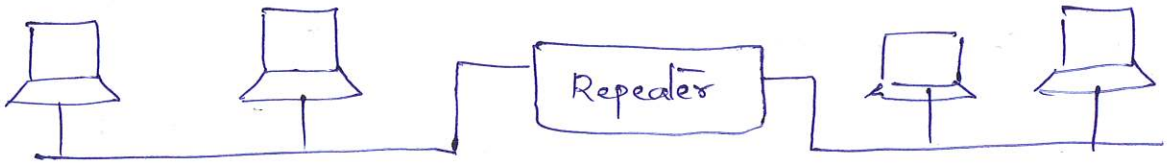
→ The basic purpose of a repeater is to extend the distance of LAN.

→ A repealer receives a signal & before it becomes too weak or corrupted, regenerates the original bit pattern.

→ The repeater does not actually connect two LANs ; it connects two segments of the same LAN.

→ The repeater not a device that can connect two LANs of different protocols.

10 ⟶ A repeater doesn't amplify the signal; it regenates the signal.



⟹ Characteristics of repeater :-

(1) Used to regenerate an existing baseband signal.

(2) It will pass a broadcast.

(3) It is used in a co-axial bus topology.

(4) It operates at physical layer of OSI model.

(5) Segments connected by a repeater must use same media access control method.

(6) It doesn't filter packets.

(7) It can pass traffic b/w different types of media.

(8) It doesn't accelerate or change the signal. It simply regenerates it.

(9) Segments connected by a repeater must have the same n/w address.

⟹ Types of repealers :—

(1) Single port repeater — operates with two segments.

(2) Multiport repealer — has one i/p & multipe o/p ports.

(3) Smart repealer — hybrid device (works as Bridge)

(4) Optical repealer — repeats optical signals.

(3) Bridges :—

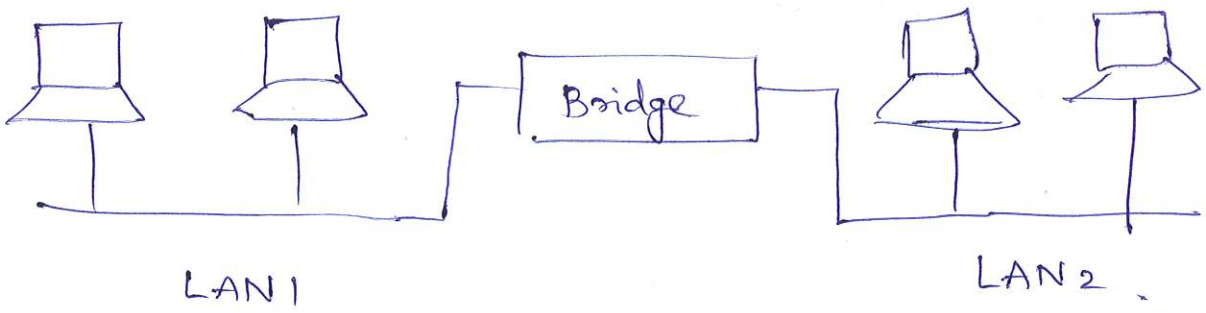
→ A bridge operates in both physical & data link layer.

→ A bridge extends the max distance of n/w by connecting separate n/w segment.

→ A bridge passes on all the signals it receives.

→ It reads the address of all the signal it receives.

→ Bridge performs datalink functions such as error detection, frame formatting and frame routing.



⇒ Functions of Bridge :—

(1) Frame filtering and forwarding.

(2) Learning the address.

(3) Routing.

⇒ Types of Bridges :—

(1) Fixed - routing bridges.

(2) Transparent or spanning tree bridges.

(3) Source routing bridges.

(4) Remote bridges.

⇒ Features of Bridge :—

(a) Bridge can do —

↳ filter traffic by reading packet address.

↳ link dissimilar n/w.

↳ link segments of a n/w together.

(b) Bridge can't do —

↳ determine the most efficient path

↳ traffic mgmt function.

(c) Benefits :—

(1) Expand the length of an existing n/w.

(2) increase the no of workstations on the n/w.

(3) reduce traffic congestion.

(4) provide a connection to a dissimilar n/w.

(5) Move data across a intermediate n/w with a dissimilar protocol.

(4) Switches :—

→ It supports transmitting, receiving and controlling traffic with other computers on the n/w.

⇒ Types of switches :—

(1) Layer 2 switch — operates at physical & datalink layers

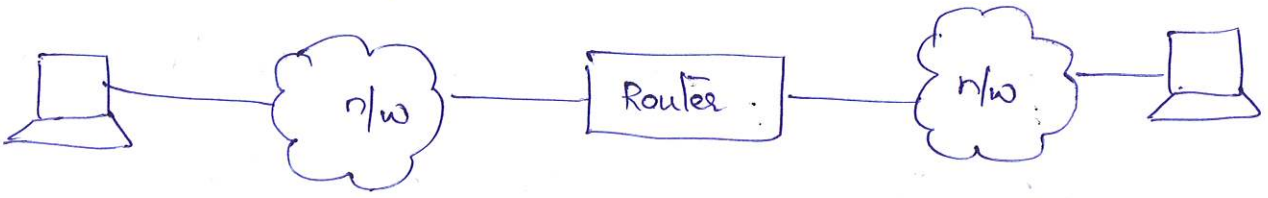
(2) layer 3 switch — used network or IP address

(3) layer 4 switch — coordinates com(n) b/w systems.

(5) Routers :-

→ It is a three layer device that routes packets based on their logical addresses.

→ Router connects two or more n/w. It consists of combination of the h/w & s/w.



→ Router connects LANs & WANs in the internet and has a routing table that is used for making decisions about route.

→ Routers connect dissimilar n/w together and have access to inf(n) from physical, datalink & n/w layer

→ Key feature is to determine the shortest path to destination.

→ Router uses one or more routing alg(m) to calculate the best path through an internetwork.

(6) Gateways :-

→ Gateway connects two independent n/w.

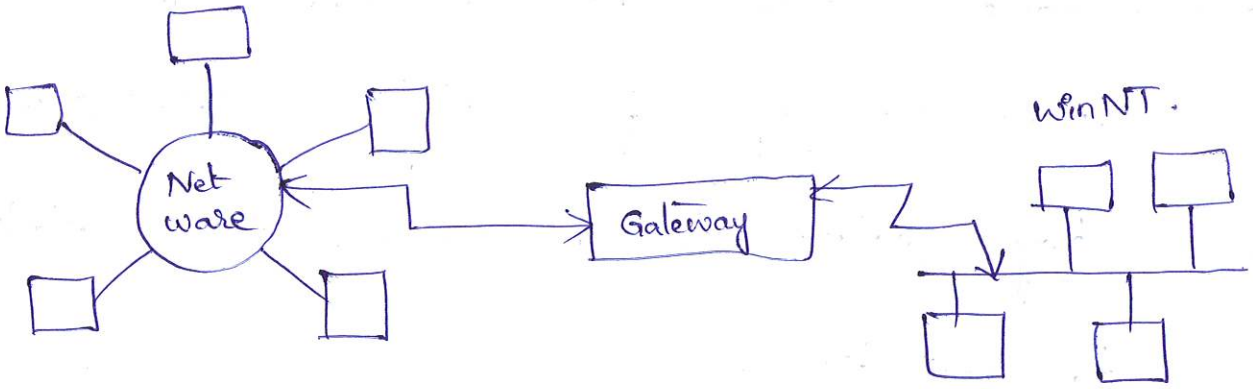
→ A gateway is protocol converter.

→ It operates in all 7 layers of OSI model.

→ A gateway accept a packet formatted for one protocol and convert it to a packet formatted for another protocol.

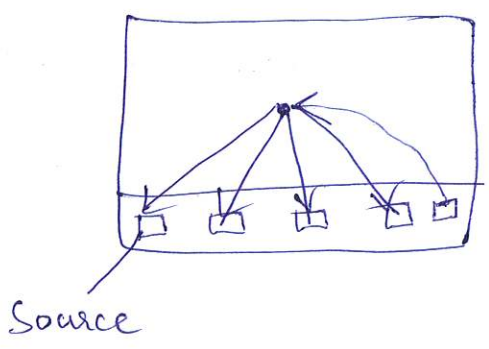
→ The gateway must adjust the data rate, size and data format.

→ It is generally s/w installed within a router.

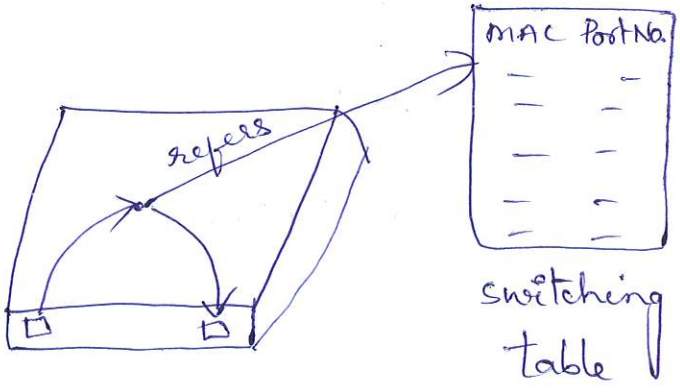


Gateway

Hub	Switch
(1) It is a broadcasting device.	(1) It is a point-to-point com(n) device.
(2) It operates at physical layer.	(2) It operates at data link layer.
(3) Hub is not an intelligent device, so it is cheap.	(3) Switch is an intelligent device, so it is expensive.
(4) Hub broadcasts the incoming packet.	(4) Switch uses switching table to find the correct destination.
(5) Hub can't be used as a repeater.	(5) Switch can be used as a repeater.
(6) Hub is an ordinary type of device, which is not widely used.	(6) Switches are sophisticated devices and widely used.



Hub



Switch

Bridge	Repeater
(1) It operates at data link layer.	(1) It operates at physical layer.
(2) It understands the complete frames.	(2) Don't understand complete frames.
(3) It will not forward a collision from one segment to another.	(3) Collision occurs on one segment, it causes the same to occur on another segment.
(4) It uses the destination address whether to forward a frame.	(4) It can't understand the destination address.
(5) It performs frame filtering.	(5) It can't perform frame filtering.
(6) This is a hardware device used to extend a LAN.	(6) It is also a h/w device used to extend a LAN.

14

Router	Bridge
(1) Operates at network layer.	(1) Operates at datalink layer.
(2) Routers are expensive.	(2) These are inexpensive.
(3) Difficult to setup and configure.	(3) Easy to configure.
(4) Router focuses on protocol address.	(4) Bridge focuses on MAC address.
(5) Router can accommodate multiple paths.	(5) Bridge can accommodate single path.
(6) Can route packets to reduce n/w bottlenecks.	(6) Filter packets faster than routers.
(7) Routers are good solution for joining remote n/w.	(7) Bridges are good for segment n/w.
(8) It joins two different n/w.	(8) It extends the existing n/w.
(9) Routers are both h/w & s/w device.	(9) Bridges are both h/w & s/w device.
(10) Can't route some common protocol. (within n/w)	(10) Can't route the packet.