COMPUTER NETWORKS

Computer Network:

→ A computer Network is a set of devices connected through links. In simple terms computers connected together

■ Network: A network is a set of devices that are connected with a physical media link. In a network, two or more nodes are connected by a physical link or two or more networks are connected by one or more nodes. A node can be any devices which is capable of sending or receiving the data. The links connecting the nodes are known as communication channels.
In simple term, network is a collection of devices connected to each other to allows sharing of data.

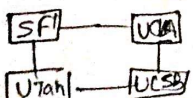
Brief History:

- In 1969, ARPANET (Advanced Research Project Agency Network) becomes the first connected computer Network.
  - It implemented the TCP/IP protocal, which later become the Internet.
- ARPANET was developed by Advanced Research Project Agency (ARPA), a subset of US Department of defence (DoD).

? Why did the DoD need to develop network computers?

→ Because of the cold war betⁿ US & USSR (Union Sovict Socialist Republics). The goal of ARPANET was to keep lines of communication open if the USA and the USSR decied to Exchang nuclear devices.

- ARPANET revolutionized communications by using packet-switching instead of direct connection. Data that is communicated through a packet-switching system is formated into packets with an address of destination machine. and sent onto the network and pick up by the next machine. The address in protocal tells the machine where to send the packets. This way the info. will reach its intended destination, even if there isn't a direct connection betⁿ two machines.
- While it changed the need for there to be direct connections between machines to communicate, the ARPANET relies on phone lines. It was originally a four-node network between university computers of Stanford, the University of Utah, UCLA (University of California LA) and UCSB (University of California, Santa Barbara).

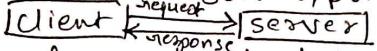


~~# Bits~~

Basic Terms in Computer Network :-

1. **Client** :- A client is a computer Hardware device or software that acessess a service made available by a server.. The server is often (but not always) located on a separate physical comp.

2. **Server** :- A server is a physical computer dedicated to run services to serve the needs of other computers. Depending on the services that is running, it could be a file server, database server, home media server, print server, web server.



3. **Host** :- A host is a computer, connected to other computers for which it provides data or services over the network. In theory, every computer connected to a network act as a host to other peers on the network

4. **Peer** :- A Peer is a node that provides the same functionality as another. Eg two computers in network are peers, but a computer and a server are not peers as they perform different operations.
A peer is something or someone that is an equal member of group, where there's some kind of relationship beth the members of the group.

5. **Bandwidth** : Network bandwith is a measurement indicating the maximum capacity of a wired or wireless communication link to transmit data over a network connection in a given amount of time. Typically, bandwidth is represented in the numbers of bits, kilobits, megabits or gigabits. that can be transmitted in 1 second. Synchro. Synonymous with capacity bandwidth describes data transfer rate.

- **Speed** : Speed refers to rate at which data can be transmitted while the bandwith is the capacity for that speed.

1 gbps = 10^9 bits/s

1 mbps = 1000000 bits/s

1 kbps = 1000 bits/s

16 Jitter :- Information is transported from your data packets across the internet. They are usually set at regular intervals and take a set amount of time. Jitter is when there is a time delay in the sending of these data packets over your network connection. This is often caused by network congestion, and some times route changes.
The longer data pkts take to arrive, the more jitter can negatively impact the video and audio quality.

17 Packets :- A packet is a small segment of a larger message. Data sent over computer network such as internet, is divided into packets. These packets are then recombined by the computers or device that recievers them.

- Packet Header :- A packet Header is a "label" of sort, which provides information about the packets contents, origin, destination.

Packets consist of two portions: the Header & the payload.
The Header contains info about the packet, such as origin, destination IP address etc. while the payload is actual data.

18 Segments :- If the Tranport protocal is TCP, the unit of data sent from TCP to network layer is called segments.

19 Frame :- A frame is also a unit of data, it is a protocal Data Unit of a Data link layer.

NOTE
- The PDU of Transport layer is called as Segments
- The PDU of Network layer is called as Packets
- The PDU of Data Link layer is called as Frames.

10 Local Host :- local host is your own computer. Local Host can be seen as server that is used on your own computer. Local Hast has the IP Add : 127.0.0.1.

11 Bit-Rate: Line coding :- The process of turning binary data into a time-based signal is known as line coding.
BitRate :- Network connections can send bits very fast. We measure that speed using Bit-rate. The number of bits of data that are sent each second.

12 Latency :- Latency measures how late the bits arrive.
Latency is the time between the sending of data msg and recieving of that msg, measured in milliseconds.

13 Noise :- Noise is any undesired signal in communication circuit. Noise is a unwanted disturbance superimposed or a useful signal, which tends to obscure its information content.

Types :- Thermal, Intermodulation, Crosstalk and impulse noise.

14 Attenuation :- Attenuation means lass of signal strength in networking cables or connections. This is measured in decibels(dB) or voltage. and can occur due to varity of factors, It may cause signals to become distorted or indiscernible Ex :- is wifi signal, strength. is weaker than the router.

Distortion :- interruption of transmitting signals that causes an unclear reception.

What is WEB and whats the Difference betn web & internet?

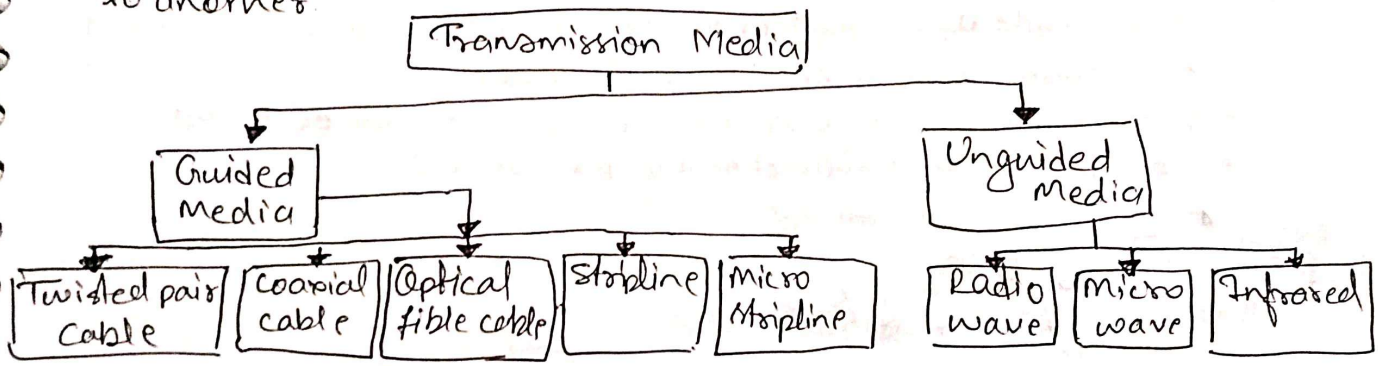
→ The internet is a global network of networks while the web or World Wide Web (www) is a collection of information that is assessed via the internet.

◆ The internet is infrastructure while the web is served on top of that infrastructure.

• Web applications uses HTTP protocal which is a layer over TCP protocal, whereas internet applications can either use TCP or UDP protocal.

Transmission Media :.

→ A Transmission media a path between transmitter & Receiver. i.e. it is the channel through which data is sent from one place to another



1. **Guided Media** :- Wired or Bounded ~~Guided~~ transmission Media.
   - Signals being transmitted via physical link.

Features –
- High speed
- Secure
- Used for shorter distance.

Types →

(i) **Twisted Pair Cable** :- consist of 2 separately insulated conductor wires wound about each other. several such pairs are bundled together in protective sheath. Two types

- **Unshielded Twisted Pair (UTP)**
  → Consist of two insulated copper wire. twisted around each other.
  → ability to block interference and doesn't depend on physical shield.
  → Used in the telephonic Application
  • Leavst Expensive • Easy to install • High speed • Short distance transmission due to Attenuation.

- **Shielded Twisted Pair**
  → Consist of special jacket (copper braid covering or foil shild) to block external interfedence
  → Used in fast data rate Ethernet.
  • more Expensive • Bulky • diff. to install • Better performance.

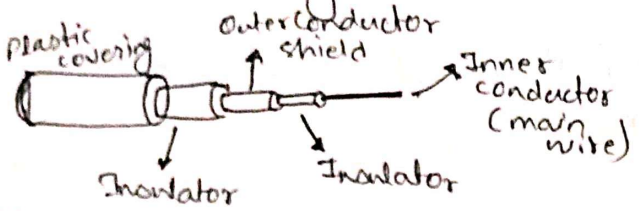
(ii) Coaxial Cable :- It has an outer plastic covering containing an insulation layer made of PVC or Teflon and 2 parallel conductors each having separated insulated protection cover.

→ Transmit information in two modes:

① Baseband mode : dedicated cable Bandwith

② Broad band mode: cable bandwith is split into separate ranges.

→ Cables TVs and analog TV network uses coaxial cables



Advantages:

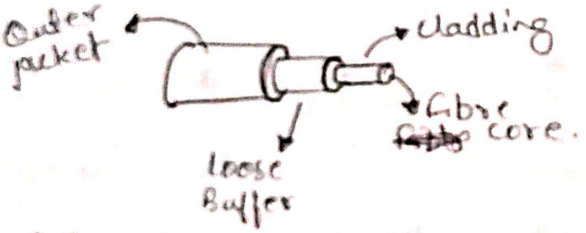
- High Bandwidth
- Better Noise Immunity
- Easy to install and Expand
- Inexpensive

Disadvantages :-

- Single cable failure can disrupt the entire network.

(iii) Optical Fiber Cable :- It uses the concept of reflection of light through a core made up of glass or plastic. The core is surrounded by a less dense glass or plastic called cladding.

- This is used for large transmission of large volumes of data.
- The cable can be unidirectional or bidirectional.



Advantages

- Increased capacity & Bandwidth
- Lightweight
- Less Signal Attenuation
- Immunity to electromagnetic interference
- Resistance to corrosive materials.

Disadvantages

- Diff. to install & maintain
- High cost
- Fragile

(iv) Stripline :- It is a transvers Electromagnetic transmission line medium invented by Robert M. Barrett in 1950's.

- Stripline is the earliest form of planar transmission line
- Uses a conducting material to transmit high frequency wave.
- In this, the conducting material is sandwiched bet^n two layer of ground plane which are usually shorted to provide EMI immunity.

(v) MicroStripline :-

- In this, the conducting material is separated from the ground plane by a layer of dielectric.

2. **Unguided Media** :- also refered as Wireless or Unbounded transmission media

→ No. physical medium is required.

Features :- • The signal is Broadcasted through air.
• Less Secure
• Used for large distances.

Types :-

(i) **Radio Waves** :- • easy to generate
• can penetrate through buildings.
• Sending & Recieving antennas need not be aligned.
• Range : 3 KHz – 1 GHz.
• AM & FM radios and cordless phones uses Radio waves.

(ii) **Microwaves** :- • Sending and Recieving antennas need to be properly aligned with each other.
• Distance covered by signals is directly proportional to height of antenna.
• Fre. Range : 1 GHz – 300 GHz.
• Mainly used for mobile phone communication & Television Distribution

(iii) **Infrared** :- • Used for short distance communication.
• cannot penetrate through obstacles
• Fre. Range : 300 GHz – 400 THz.
• Used in TV Remote, wireless mouse etc.

Computer Network Devices :-

1. **Hub** :- • Works at physical layer and hence connect devices physically
• It uses Twisted pair cables to connect devices.
• They are designed to transmit the packets to other appended devices without alternating any of the transmitted packets recieved.
• They transmit the info regardless of the fact if data packet is destined for the device connected or not.

Two Categories :-

(i) **Active Hub (Repeaters)** :- • Smarter than the passive Hub, They provide path for signals also they regenerate, concentrate and strengthen the signal before sending to destination. It is also called as "Repeaters".

(ii) **Passive Hub** :- They more like a point contact for the wires to built in the physical Network. They have nothing to do with modifing the signals.

2 Ethernet Hub :- It is a device connecting multiple Ethernet devices together and make them perform like the functions as a single unit.
- They vary in terms of speed.
- It communicates in half-duplex mode where chance of data collision are inevitable most of the time.

3 Switches : Switches are the linkage points of an Ethernet network.
- Devices in switches are connected through twisted pair cables.
- Switches transfer data packets only to that port which is connected to destination devices. A switches does so by having a built-in learning of MAC address of devices connected to it.
- Since transmission of data signals are well defined in a switch hence the network performance enhanced.
- Switches Operates in full duplex mode where devices send & received data simultaneously.

4 Modem :- Modulator-Demodulator (Modem) is a device which converts computer-generated digital signals to analog signals, and also capable of again converting analog signals to digital signals at receiving end.
Common types include :- half-duplex modem, full-duplex modem, 2 wire modem, 4-wire modem, synchronous and Asynchronous modem.
Modem stands for Modulator-Demodulator device assists computer in transferring data and information over telephone lines.
It act as modulator when it converts digital data into analog signal and it act as demodulator when it converts analog into digital signal.

5 Gateways :- A Gateway is not a hardware device, itself, it is a software firmware which save configuration settings of the device mostly the gateway address in routers is 192.168.0.1 or 192.168.1.1.
It acts as a 'gate' between two networks. It may be routers, firewall, server or other devices that enables traffic to flow in and out of the network. while a gateway protects the nodes within network it also a node itself.

6 Wifi Routers :- Similar like modem is also Modulator and Demodulator the additional feature is wireless connectivity, which is called as wifi. It has 4-ethernet ports and its having routing, DHCP so that connect 240 pc and devices modem internet with wired or wireless.

7 **Routers**:- When a device in LAN needs to communicate with a device on another ~~lan~~ LAN, it must send traffic to a specialized device connected to the LAN called a Router. whose purpose is to find the best path for the message to take to arrive at the intended target device, and to send the message along its way following that path.

- Routers are Network layer devices and are particularly identified as Layer-3 devices of the OSI Model.
- They process logical addressing information in the Network ~~add~~ header of the packet such as IP Address.
- It has the ability to connect dissimilar LAN on the same protocol.

Functionality:-

- When a Router receives the data, it determines the destination addr by reading the header of the packet. Ones the address is determined, it searches in its Routing table to get know how to reach the destination and then forwards the packet to the higher hop on the route. The hop could be the final destination or another routers.

Routing table:- It plays a very pivotal role in letting the router makes a decision. Thus a routing table is ought to be updated and complete. The ways through which a router can recieve information are:-

(i) **Static Routing**:- The routing information is fed into the routing table manally, It does not becomes a time-taking but gets prone to errors as well. Static Routing is feasible for tinniest environment with minimum of one or two Routers.

(ii) **Dynamic Routing**:- For larger environment ~~of~~ Dynamic Routing proves to be the practical solution. The process involves use of peculiar routing protocals to hold communication. The purpose of these protocal is to enable the other routers to transfer information about other routers. So that the other routers can built their own routing tables.

8 **Repeater**:- ~~Repeat~~ Repeater is used to extend the range of radio signal so that the signal can cover longer distances, a repeater is an electronic device that recieves a signal and re-transmits it. Repeaters is used for wired medium as well as wireless medium.

Types of Repeaters

- Analog Repeater
- Digital Repeater
- Microwave Repeater
- Satellite Repeater
- Wifi Repeater/WLAN Repeater
- LTE Repeater
- Optical Repeater.

9 **Bridges:-** A network bridge device is primarily used in LAN's because they can potentially flood and clog a large network thanks to their ability to broadcast data to all the nodes if they dont know the destination nodes MAC Address.

A bridge is a type of network device that provides interconnection with other bridge networks that uses the same protocal.

A bridge is a computes network device that builts the connection with other bridge network that uses the same protocal.

It works at the Data link layer of the OSI model and connects different networks together and develops communication between them.

Bridges are similar to repeater & Hubs in that they broadcast data to every node, However Bridge maintain the Media Access Control (MAC) address table as soon as they discover new segments, so subsequent transmissions are sent to only to the desired recipient.

A bridge uses database to ascertain where to pass, transmit or discard the data frame.

1. If the frame received by the bridge is meant for a segment that resides on the same host network, it will pass the frame to that node and the receiving bridge will then discard it.
2. If the bridge receives a frame whose node MAC Address is of the connected network, it will forward the frame toward it.

Types:- Transparent Bridge ② Source Route Bridge ③ Translation Bridge.

10 **Brouters:-** Brouters are the combination of both the bridge and routers. They take up the functionality of the both networking devices serving as a bridge when forwarding data between networks, and serving as a router when routing data to individual systems.

Brouters functions as a filter that allows some data into the local network and redirects unknown data to the other network.

Brouters operate at both the network layer for routable protocals and at the data link layer for non-routable protocals. As network continue to become more complex a mix of both routable and non routable protocals has led to the need of the combined features of Bridge and routers.

Brouters handle both routable and non routable features by acting as routers for routable protocals and bridges for non-routable protocal.

11 **Network Card** :- also known as Network Interface Card (NIC's) are hardware devices that connects a computer with the network.

- It is installed on the mother board
- They are responsible for developing a physical connection between the network and the computer.

Computer data is translated into electrical signals send to the network via Network Interface Card.

- They also mange some important data-conversion function.

12 **Network Protocol** : Network protocols define a language of instruction and conventions for communication between the network devices. It is essential that a networked computer must have one or more protocol drivers. Usually for two computers to interconnect on a network, they must use identical protocols. At a time, computers are designed to use multiple protocols. Network protocols like HTTP, TCP/IP offer a basis on which much of internet stands.

13 **Integrated Services Digital Network (ISDN)** :- ISDN are used to send over graphical or audio data files. It is a WAN Technology that can be used in place of a dial up link.
It surely provides higher speed than a modem and has the capability to pick up the line and drop it considerably at a faster rate.

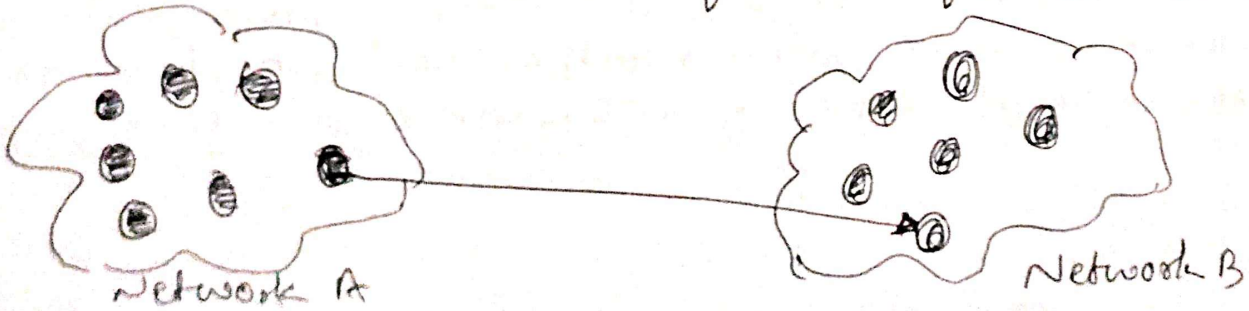
Unicast, Broadcast & Multicast

Cast :- cast term signifies some data (stream of packets) is being transmitted to the recipient from client.

1 **Unicast** :- • One-to-One transmission

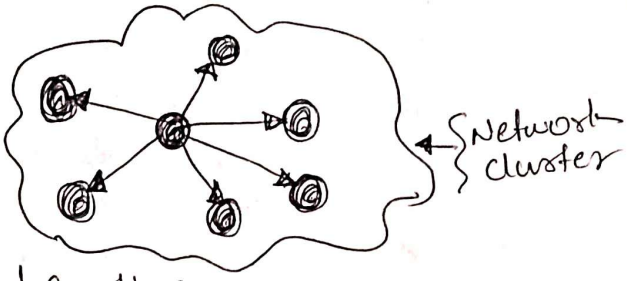
- This type of information transfer is useful when there is participation of single sender and single recipient.

For Example : a device having IP address 10.1.2.0. in a network wants to send the traffic stream (data packets) to the device with IP address 20.12.4.2 in other network, then unicast comes into picture.
This is the most common form of data transfer over the Network.

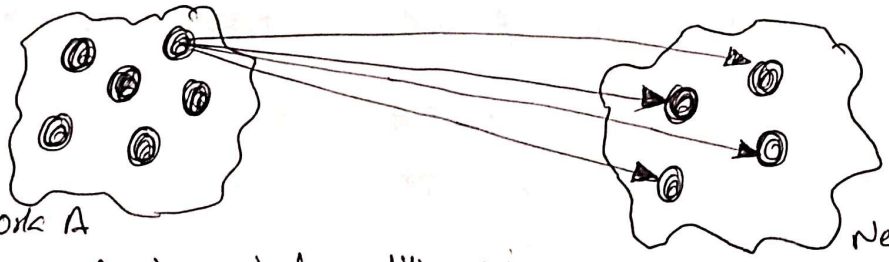


2. **Broadcast** : Broadcasting transfer (one-to-all) techniques can be classified into two types.:-

(i) **Limited Broadcasting** :- Suppose you have to send stream of packets to all devices over the network that you reside, this Broadcasting comes handy. For this to achieve, it will append 255.255.255.255 (i.e. all the 32 bits of IP address set to 1) called as Limited Broadcast Address in the destination address of datagram(packet) header which is reserved for information transfer to all the recipients from a single client (sender over a Network).



(ii) **Direct Broad Casting** :- This is useful when a device in one network wants to transfer packet stream to all the Devices over the other network. This is achieved by translating all the Host ID part bits of destination Address to 1, reffered as Direct Broadcasting Address in datagram Header for information transfer.



— This mode is mainly utilized by television network for video & Audio distribution.

— One important protocol of this class in computer Network is Address Resolution Protocol (ARP) that is used for Resolving IP Address into physical Address which is necessary for underlying communication.

3. **Multicast** :- In multicast one/more senders and one/more recipients participate in data transfer traffic. ~~Earlier~~, Multicast lets server's direct single copies of data stream that are then simulated and routed to hosts that request it.

IP multicast requires support of some other protocols like IGMP (Internet Group Management Protocol), Multicast routing for its working. Also in classful IP Addressing Class D is reserved for multicast group.

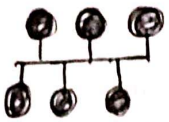
Topologies :

→ Network Topologies describe the methods in which all the elements of network are mapped, Network Topology specifies the layout of a computer network. It shows how devices and cables are connected to each other.

1 Point to Point (P-2-P)

→ In this method, the network consist of direct link bet^n two computers.
→ Fastest & highly reliable than other types, since there is direct connect^n.
→ No need for network Operating System
→ No need of an expensive server as individual workstations are used to access the files.
→ You can't backup files.
→ Used for small areas only where computers are in close proximity.
→ No security.

2 Bus Topology :-

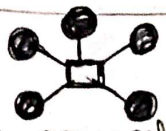


→ Bus Topology is a network topology in which all nodes are connected to a single cable known as central cable or bus
→ It acts as shared communication medium i.e. If any device wants to send the data to other devices, then it will send the data over the bus which in turn sends the data to all attached devices.
→ Useful for small numbes of devices.
→ As if the bus is damaged then the whole network fails.

3 Ring Topology :-

→ Ring topology is a network topology in which nodes are exactly connected to neighboring devices for communication purpose. and thus forming a single continuous path for transmission. It is called a ring topology as its formation is like a ring.
→ Does not need any central server to control the connectivity among the nodes.
→ If single node is damaged, whole network fails.
→ Ex. SONET network, SDH network etc.

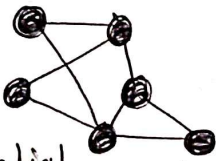
4 Star Topology :-



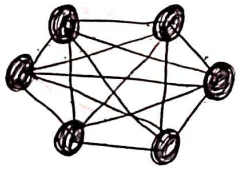
→ In this, all nodes are connected to a single device known as a central device.
→ Requires more cables as compaire to other topologies. Therefore it is more robust as a failure in one cable will only disconnect a specific computer connected to that cable.
→ If the central device fails, whole network fails.
→ Easy to install, manage and troubleshoot. used in home & office

5 Mesh Topology :-

→ In this, all the nodes are individually connected to other nodes
→ Does not need any central hub or switch.
→ It is robust as a failure in one cable will only disconnect the specific computer. connected to this cable.
→ Offers a high level of redundancy, so even if one network cable fails, still has alternative path for data to reach the destination.
→ two types :-
① Partial Mesh Topology :- In this, all nodes are not connected to each other
② Full Mesh Topology :- all nodes are connected to each other.



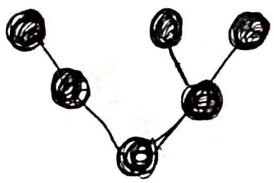
Partial mesh



Full Mesh

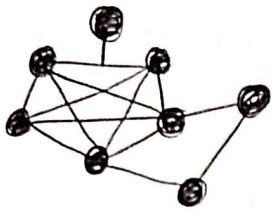
6 Tree Topology :-

→ Tree topology have a root node, and all the other nodes are connected which form a hierarchical topology.
→ In this, All the star networks are connected to a single bus.
→ In this the whole network is divided into segments known as star networks which can be easily maintained. If one segment is damaged there is no effect on other segments.
→ Tree topology depends on the main bus and if it breaks, then the whole network gets damaged



7 Hybrid Topology:-

→ A Hybrid Topology is a combination of different topologies.
→ For example if star topology is connected with different topology, then it becomes a Hybrid topology.
→ It provides flexibility as it can be implemented in a different network environment.
→ The design of Hybrid topology is complex.



Different Types of Networks:-

→ Network can be divided on the basis of area of distribution:-

1 LAN (Local Area Network)

→ It is a group of network devices that allow communication between various connected devices. Private ownership has control over LAN rather than public
→ LAN ~~not~~ has short propagation delay than MAN and WAN.
→ Used for small geographical location like office, shool etc.

2 MAN (Metropolitan Area Network)

→ It covers a larger area than LAN such as small towns, cities etc.
→ MAN connects two or more computers that reside within the same or completely different cities.
→ MAN is expensive and should or might not be owned by one organizat^{n}.

3 WAN (Wide Area Network)

→ Covers larger area than LAN and MAN such as country
→ PSTN or statellite medium is used for wide area network.
→ WAN also might not be owned by one organization.
→ Transmission speed is low.

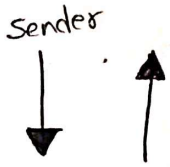
Other than that -

- PAN (Personal Area Network):- Range is limited upto 10 meter. Created for personal use, Generally personal Devices are connected to this network.
- CAN (Campus Area Network):- It is a connection of devices within campus area which links to other departments of organizat^{n} within same campus
- GAN (Global Area Network):- It uses satellites to connect devices over the global area.

OSI Model

OSI Model :- OSI stands for Open System Interconnection Model is a conceptual framework used to describe the functions of a networking system. developed by International Organization for Standardization (ISO) in the year 1984. It is a 7 layer architecture with each layer having specific functionality to perform. All these 7 layers work collaboratively to transmit the data from one person to another across the globe.

7 layers Are :-



1. Application Layer
2. Presentation Layer
3. Session Layer

} Software Layer

4. Transport layer
5. Network layer
6. Data Link layer
7. Physical Layer.

} Hardware Layer

Brief Explanation of All Layers :-

1. Physical Layer [Layer 1] :-

- The lowest layer of OSI model is physical layer
- It is responsible for the actual physical connection between the devices
- The physical layer contains information in the form of bits.
- It is responsible for transmitting individual bits from one node to other. When receiving data, this layer will get the signal received and converts it into 0's and 1's and send them to the Data link layer, which will put the frame back together.
- Function of Physical layer :-

(i) Bit Synchronization :- The physical layer sync provides the synchronization of bits by providing a clock. This clock controls both sender and receiver thus providing synchronization at bit level.

(ii) Bit rate control :- The physical layer also defines transmission rate, i.e. the number of bits sent per second.

(iii) Physical topologies : Physical layer specifies the way in which the devices/nodes are arranged or connected in a network. i.e. bus, star, or mesh etc. topology.

(iv) Transmission Mode :- Physical layer also defines the way in which data flows between two connected device. The various transmission modes possible are Simplex, Half-duplex, full duplex.

NOTE :- Hub, Repeater, Modem, Cables are Physical Layer Devices

- Network layer, Data link layer, and Physical layers are also known as Lower Layers or Hardware Layers.

2. Data Link Layer [Layer2]

→ Data Link Layer is responsible for the node-to-node delivery of the message.

→ The main function of this layer is to make sure data transfer is error-free from one node to another, over the physical layer.

→ When a packet is arrived in a network, it is the responsibility of Data link Layer to transmit it to Host using its MAC Address.

→ Data Link Layer is divided into two sublayers.

1. Logical Link Control (LLC)
2. Media Access Control (MAC)

→ The packet received from the Network layer is further divided into frames depending on the size of NIC (Network Interface card)

DLL also encapsulates Sender's and Receiver's MAC address in the Header

→ The receiver's MAC Address is obtained by placing an ARP (Address Resolution Protocol) request onto the wire asking "who has that IP Address?" and the destination Host will reply with its MAC Address.

→ Functions of DLL Are :-

(i) Framing :- Framing is a function of DLL. It provides a way for a sender to transmit a set of bits that are meaning full to the receiver. This can be accomplished by attaching special bit pattern to the beginning and end of the frame (AKA. Header & Footer)

(ii) Physical Addressing :- After creating frames, DLL adds physical address (MAC Address) of sender and/or receiver in the Header of each frame.

(iii) Error Control :- Data Link Layer provides the mechanism of error control in which it detects and retransmits damaged or lost frames.

(iv) Flow Control : The data rate must be constant on both sides else the data may get corrupted thus, flow control coordinates the amount of data that can be sent before receiving acknowledgement

(v) Access Control : when a single communication channel is shared by multiple devices, the MAC sub-layer of data link layer helps to determine which device has control over the channel at a given time.

NOTE : Packets in Data Link Layer is refered as **Frames**.

- Data Link Layer is handled by the NIC (Network Interface Card) and device drivers of Host machine.
- Switch & Bridge are Data Link Layer devices.

3. Network Layer [Layer3] :

→ Network layer works for the transmission of data from one host to the other located in different network.

→ It also takes care of packet routing i.e. selection of shortest path from one host to other host to transmit the packet, from the number of routers available (Hop-By-Hop routing).

→ The Sender & Receiver's IP addresses are placed in the header by network layer

→ Functions of Network Layer :-

(i) Routing :- The network layer protocols determine which route is suitable from source to destination. This function of Network layer is called Routing.

(ii) Logical Addressing :- In order to identify each device on internetwork uniquely, the network layer defines an addressing scheme. The Senders & Receiver's IP addresses are placed in the Header by the network layer. Such an address distinguishes each devices uniquely and universally.

NOTE : Packets in Network layer is referred as ~~Segments~~ **Packets**

- Network layer is implemented by networking devices such as routers.

4. Transport Layer [Layer4]

→ Transport layer provides services to the application layer and takes services from the network layer.

→ Data in Transport Layer is refered as **Segments**.

→ It is responsible for End-to-End Delivery of the complete message. The transport layer also provides the acknowledgement of successful data transmission and retransmit the data if an error is found.

(i) At Sender's side :-

→ This layer receives data from upper layer and perfor segmentation and also implements Flow & Error control. to ensure proper data transmission

→ It also adds source & destination port number in the Header and then forward it to Network layer.

Generally, this destination port no. is configured either by default or manually.

NOTE :- The Sender need to know the port No. assosiated with the receiver's requested Application.

(iii) At Receiver's Side :-

→ Transport Layer reads the port Number from its Header and forward the Data which it has received to the respective application. Also perform sequencing and reassembling of the segmented data.

Functions of Transport Layer :-

(i) Segmentation & Reassembly : This layer accepts the message from the session layer, breaks the message into smaller units. Each of the segments produced has a header associated with it. Transport layer at destination station reassemble the message.

(ii) Service Point Addressing (SPA) :- In order to deliver the message to correct process, the transport layer header includes a type of address called service point Address or Port Address. Thus by specifying this address, the transport layer makes sure that the message is delivered to the correct process.

Services provided by the Transport Layer :-

(i) Connection-Oriented Services :- It is a three-phase process (or 3way or 3-way Hand Shake that includes :-

- Connection Establisment
- Data Transfer
- Termination / Disconnection.

■ In this type of transmission, the receiving device sends an acknowledge-ment, back to the source after a packet or group of packets is received. This type of transmission is reliable and secure.

(ii) Connectionless Service :- It is a one-phase process and includes Data transfer. In this type of transmission, the receivers does not acknowledge receipt of a packet. This approach allows for faster communication between devices.

[NOTE] : Data in Transport layer is called segments.

- Transport layer is operated by the Operating System. It is a part of the OS and communicates with the Application layer by making system calls.
- Transport Layer is called as Heart of OSI Model.

Session Layer [Layer 5]

→ This layer is responsible for the establishment of connection, maintain-maintenance of sessions, authentication, and also ensure security.

→ Functions of session Layer are :-

(i) Session Establishment, maintenance and termination :- This layer allows the two processes to establish, use and terminate a connection.

(ii) Synchronization :- This layer allows the process to add checkpoints which are considered as synchonization points into the data. These synchronization points helps to identify the errors so that the data is re-synchronized properly, and ends of the message are not cut prematurely so that the data loss is avoided.

(iii) Dialog Controller :- The session layer allows two systems to start communication with each other in half duplex or full duplex.

NOTE : Implementation of these 3 layers (session, Presentation & Application) is done by the network application itself. These are known as Software layers.

Presentation Layer [Layer6] :-

→ Presentation Layer also called as Translation layer.
→ The Data from the application layer is extracted here and manipulated as per the required formate to transmit over the network.
→ Functions of the Presentation Layer.

(i) Translation : For Ex. ASCII to EBCDIC. [Extended Binary Code Decimal Interchange Code]

(ii) Encryption/Decryption :- • Encrypts the data or decrypts the data.
• The encrypted data is known as cipertext and decrypted data is known as plain text. A key value is used for encrypting and decrypting the data.

(iii) Compression :- Reduces the number of bits that need to be transmitted on the network.

Application Layer [Layer7]

→ Application Layer is implemented by the network Applications. These applicatn produce the data, which has to be transmitted/Transfered over the Network.
→ This app layer also serves as a window for the application services to access the network and for displaying the received information to Users.
Ex. Application like Browsers, messenger etc.

NOTE : Application layer is also known as Desktop layer.

→ Functions of Application layer.

(i) Network Virtual Terminal
(ii) FTAM - File Transfer Access and Management
(iii) mail Services
(iv) Directory Services.

" OSI Model acts as a reference Model and its not implemented on Internet. TCP/IP Model is being Used "

TCP/IP Model

#TCP/IP Model : The TCP/IP model was designed and developed by Department of Defense (DoD) in 1960's and is based on standard protocols. It stands for Transmission Control Protocol/ Internet Protocol.
The TCP/IP model is a concise version of OSI model. It contains four layers, unlike ~~14~~ 7 layers in OSI model. The layers are :-

1. Process/Application Layer
2. Host-To-Host Layer/Transport Layer
3. Internet Layer
4. Network Access/Link Layer.

— The first layer Process layer is on the behalf of sender and Network Access layer on the behalf of Receiver.

#Explanation of layers :-

1. Network Access Layer

→ This layer corresponds to the combination of Data link layer & physical layer in OSI model.
→ It looks out for Hardware addressing and the protocols present in this layer allows for the physical transmission of Data.

2. Internet Layer (Network Layer)

→ This layer parallels the functions of OSI's Network Layer. It defines the protocols which are responsible for logical transmission of Data over the network.
Main Protocol residing at this layer :-

(i) IP (Internet Protocol) :- Responsible for delivering packets from source host to destination host by looking at the IP addresses in the Header. two versions :- IPv4 & IPv6. IPv4 is the one that most of the websites are using currently but IPv6 is growing as IPv4 is limited.

(ii) ICMP (Internet Control Message Protocol) :- It is encapsulated within IP datagram and is responsible for providing hosts with info. about network problems.

(iii) ARP (Address Resolution Protocol) : Its job is to find Hardware address of a host from a known IP address. ARP has several types! Reverse ARP, Proxy ARP, Gratuitous ARP, Inverse ARP.

3 Host-to-Host Layer (Transport Layer)

→ This layer is similar to Transport Layer of OSI model.
→ It is responsible for End-to-End communication and Error-free delivery of data.
→ It shields the upper layer applications from complexities of data.
→ Main Protocol Presents are :-

(i) Transmission Control Protocol :- It is known to provide reliable and Error-free communication between end systems. It performs sequencing and segmentation of data.
It also has acknowledgement features and controls the flow of data through flow control mechanism.
It is very effective protocol but has alot of overhead due to such feature. Increased overhead leads to increase cost.

(ii) User Datagram Protocol :- It does not provides such features like TCP. It is the go-to protocol if the application does not require reliable transport as it is very cost effective. Unlike TCP, which is connection-Oriented protocol, UDP is connectionless.

4 Application Layer

→ This layer performs the functions of top three levels of OSI model i.e. Application Layer, Presentation and Session Layer
→ It is responsible for node-to-node communication and controls user-interface specifications.
→ Some important protocols in Application Layer are: HTTP, HTTPS, FTP, TFTP, Telnet, SSH, SMTP, NTP, DNS, DHCP, NFS, X window, LPD.
Some of them are :-

(i) HTTP and HTTPS :- stands for HyperText Transfer protocol. It is used by world wide web to manage communication betn web browsers and servers. while HTTPS stands for HTTP-Secure. it is a combination of HTTP with SSL (Secure Socket Layer). It is efficient in cases where the browser need to fill out forms, sign-in, authenticate and carries bank transf transactions.

(ii) SSH :- stands for Secure Shell. It is a terminal emulations software like Telnet. The reason SSH is more preferred because of its ability to maintain encrypted connection. It sets up a secure session over a TCP/IP connection.

(iii) NTP :- Stands for Network Time Protocol. It is used to synchronize the clock on our computer to one Standard Time Source. It is very useful in situation like bank transactions. Assum a situation without NTP, suppose you carry out a transaction where your computer reads the time 2:00 PM while Server records it 2:30 PM. The Server can crash very badly if its out of sync.

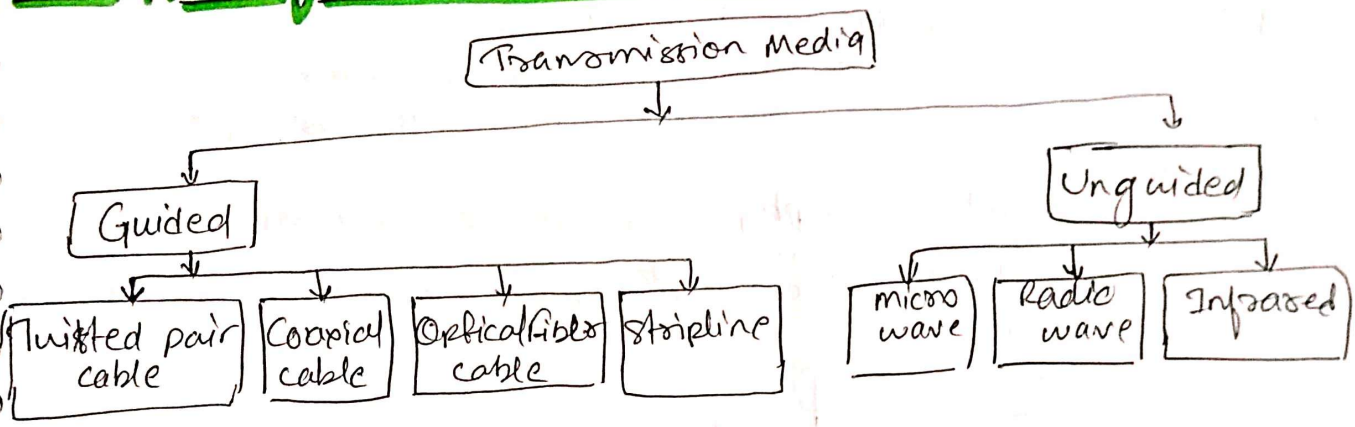
1. Physical Layer

Networking Devices:

- HUB, Switches, Routers, Gateway, Brouters, NICs etc.

** Already Covered **

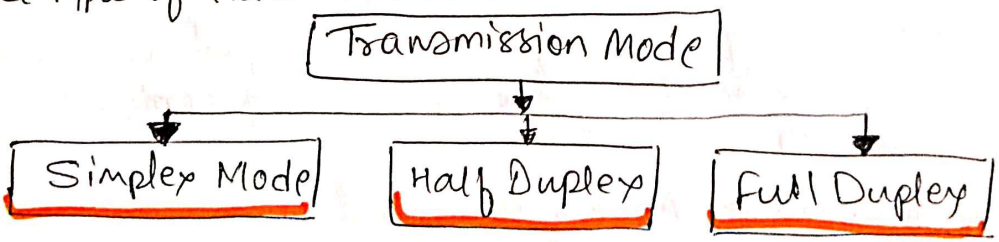
Types of Transmission Media



** Already Covered **

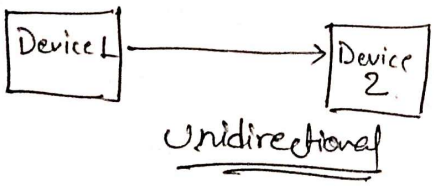
Transmission Modes in Computer Network

→ It means transferring data between two devices. It is also known as communication mode.
→ Three types of Transmission Mode.



1. Simplex Mode :-

→ Communication is unidirectional.
→ The simplex mode can uses the entire capacity of the channel to send data in one direction.
Eg Keyboard only input and monitor only output.



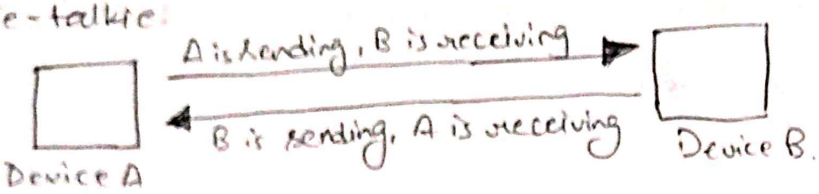
Unidirectional

2. Half Duplex :

→ In Half Duplex, each station can both transmit and receives, but not at the same time. When one device is sending, other can only receive at that time. and vice versa,

→ The entire capacity of channel can be utilized for each direction

Ex Walkie-talkie



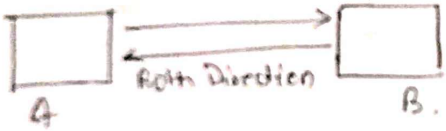
3. Full Duplex :

→ Full Duplex mode, both station can transmit and receive simultaneously.

→ In full Duplex mode, signal going in one direction share the capacity of the link with signal going in another direction. This sharing occurs in two ways :

- Either the link contain two physically separate transmission path, one for sending, one for receiving
- Or the capacity is divided between signals travelling in both direction

Ex Telephone Network



Analog to Digital

Digital Signal : A digital signal is a signal that represents data as a sequence of discrete values; at any given time, it can only take on one of a finite numbers of values.

Analog Signal : An analog signal is any continuous signal for which the time varying feature of signal represents of some other time varying quantity.

Following Technique used for Analog to Digital

1. Pulse code Modulation
   - (i) Sampling
   - (ii) Quantization
   - (iii) Encoding
2. Delta Modulation
3. Adaptive Delta Modulation

1. **Pulse Code Modulation** : It is a common technique to change analog to digital. It has three process :

(i) **Sampling** : It is a process of measurement of ~~Att~~ amplitude of continuous-time signal at discrete instants, and converting the continuous-signal into discreate signal three sampling method.
(a) Ideal sampling (b) Natural sampling (c) Flat top sampling.

(ii) **Quantization**: The ~~digization~~ digitization of analog signals involves the rounding ~~off~~ the of the values which are approximately equal to analog values. The method of sampling chooses a few points to the analog signal, then this points are joined to round off value to a near stabilized value. Such a process is called Quantization.
Quantization introduces various types of sources of errors in your algo. such as rounding errors, underflow or Overflow.

(iii) **Encoding** : After each sample is quantized and the number of bits per sample is decided, each sample can be changed to an n bit code.
Encoding also minimize bandwidth used.

2. **Delta Modulation** : since PCM is very complex technique, other techniques have been developed. The simplest is delta modulation.
→ Delta Modulation finds the change from previous value.

Modulator: It is used at sender site to create a stream of bits from analog signal.
→ The process records small positive change called delta.
If delta is positive process records 1 other wise 0.

3. **Adaptive Delta Modulation** : The performance of delta modulation can be improved by making step size of modulation assume a time varing form.

#Digital to Analog Conversion

→ Techniques are:-

1. **Amplitude data keying**:- In this carrier signal is analog and data to be modulated is digital. The amplitude of analog signal is modified to reflecting binary data.

~~2. Frequency key shi~~

2. **Frequency shift keying**: In this modulation the frequency of analog carrier signal is modified to reflect binary data.

3. **Phase Shift keying**: In this modulation the phase of the analog carrier signal is modified to reflect binary data. The The amplitude and fre. of carrier signal remains same.

#Design Issues in Physical Layer

- The physical layer is basically concerned with transmitting raw bits over a communication channel.
- Mainly the design issues here deal with electrical, mechanical, timing interface, and physical transmission medium, which lies in it.
- Design issue has to do with making sure that when 1 bit send from one side it is received 1 bit by other side also not as a 0 bit.