

And devicesDefinition:-

A computer network is a group of computers that ~~helps~~ have the potential to transmit, receive, and exchange voice, data, and video traffic. A network connected can be set-up with the help of either cable or wireless medium.

The network and data communication are the essential factors to seize information technology in the world.

History:-

In 1957, when ~~spot~~ Sputnik satellite launched by Russia. An agency named Advanced Research project Agency (ARPA) was started by America. Then, they used ARPA-net to share the information on another computer. ARPA-net came to India 1969, and its name changed from Indian to network.

S.no	Year	Description
1.	1961	Leonard-Kleinrock proposed the earliest computer network, which was the idea of ARPA-net.
2.	1965	Donald Davies pointed out the term packet to describe how to send the data b/w computers on a network.
3.	1969	The first INP and network switch were sent to UCLA. On ARPA-net the first data transmission was sent using it.
4.	1971	In 1971, the first e-mail was sent to access a network to other users.
5.	1973	ARPA deployed the first international communication network connection known as Sat-net.
6.	1978	The TCP/IP protocol was developed.
7.	1988	In 1988, the first T-1 backbone was included with ARPA-net AT&T, Iosent, and NCR introduced the wave- lan LAN network technology.

8.	1990	The first network switch was developed.
9.	1996	An IP-V-6 was introduced as an improvement over IP-V.4
10.	1997	In June-1997, the 802.11 standards, containing transmission speeds upto 2Mbps, for Wi-fi were introduced.
11.	1999	The 802.11, A standards containing transmission speeds upto 25Mbps to use the 5gb band.
12.	2003	802.11-G devices contain transmission speed from 11Mbps in 1999 to 20Mbps in 2003 were available to public.
13.	2009	The 802.11-N standard can operate on the 2.4gh and 5gh bandwidth and offers higher transfer speed over 802.11-A and 802.11-G.
14.	2018	In January-2018, WPA-3 encryption was released by the Wi-fi alliance, which comprises security enhancement over WPA-2

Applications:-

- (A) Internet and world-wide-web (WWW):- In computer networks, we have a global internet, also known as WWW, that offers us various features like access to websites, online services and retrieval of informations.
- (B) Communication :- With the help of ~~computer~~ network communication is also easy because we can do e-mail, instant messaging, voice and video calls, and video ~~on~~ conferencing which helps us to communicate with each other effectively. People can use this features in their business and organization to stay connected with each other.
- (C) File sharing and data-transfer:- Data-transfer and file sharing are made possible by networks that connect different devices. This covers file sharing with a business-setting, File-sharing between personal devices and downloading/uploading of content from the internet.
- (D) Online-gaming:- Multi-player online games use computer network to link players from all over the world, enabling online competition and real time gaming experience.

- (E) Remote-access and control:- Networks enable user to access and control system and devices from a distance. This is helpful when accessing home automation systems, managing servers and providing remote IT support.
- (F) Social media:- We can use social media sites like Facebook, twitter, Whatsapp, and instagram to help people set-up their profiles and we can connect with others and share content on social media.
- (G) Online banking and e-commerce:- Online banking and e-commerce platforms where ~~for~~ customers conduct financial transaction and make online purchases, require secure computer networks.
- (H) Enterprise networks:- In computer network, we have some networks that are only used in business and organizations so they can store data and share files and resources like printers, Scanners etc.
- (I) Health care:- With the help of computer network in the health industry, we can share patient records and store records in the form of data i.e easy and a secure compare to file method. Networks are also necessary for telemedicine and remote patient monitoring.

(J) Education:- Schools use network to access online courses, virtual classrooms and other online learning materials. Campuses of colleges and universities frequently have ~~even~~ extensive computer network.

(K) Transportation and logistics:- The transportation sector uses computer networks to manage and track shipments, plan the best routes and coordinate logistics activities.

(L) Scientific research:- To share data, work together on projects and access high performance computing resources, for data analysis and scientific simulations, researchers use networks.

(M) Government and defence:- With the help of computer networks, we can communicate, share data and advance national defence. Government agency and the military, rely on secure networks.

These are just a few instances of many areas of ~~our~~ our lives where computer networks are used.

Categories:-

(A) LAN (B) WAN (C) MAN (d) PAN (e) CAN (f) CN

(A) Local Area Network (LAN):- Local area network (LAN) are network that are typically limited to a small geographic area, like a single office, home, or building. They link computers, printers, and servers to make resource sharing and communication possible within a constrained space. Ethernet cables or Wi-fi are frequently ~~are~~ used in LANs for connecting.

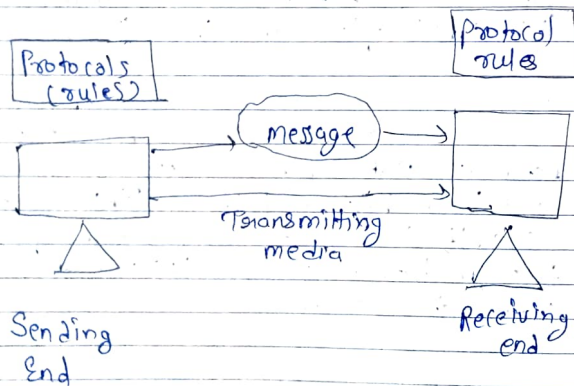
(B) Wide area Network (WAN):- Wide area Network connects LANs across multiple cities, regions ~~and~~ even entire ~~continent~~ countries. They typically cover a larger geographic area. An international example of WAN is Internet. For long distance communication, WANs employ a variety of ~~tech~~ technologies, including satellite links, fibre optics and leased lines.

(C) Metropolitan Area Network:- Metropolitan Area Network (MAN) network that spans a city or sizable campus and is in between LAN and WAN in terms of size. It is made to provide high speed data transfer between various LANs within a Metropolitan area.

Standard Organizations and protocols:

Computer networks depend on protocols and standards which play a vital role in enabling communication between different devices and systems that share data consistently. Network protocol ensures that different technology and components of the network compatible with one another, reliable and able to function together.

Protocol:- To make communication successful between devices some rules and procedure should be agreed upon at the sending and receiving ends of the system. Such rules and procedure are called protocols. Different types of protocols are used for different type of communication.



In the diagram, protocols are shown as a set of ~~rules~~ ^{rules} such that communication between sender and receiver is not possible without it/protocol.

Key elements:-

- (A) Syntax:- Syntax refers to the structure or the format of the data that gets exchanged between the devices.
- (B) Semantics:- Semantics defines data transmitted between devices. It provides rules known ~~terms~~ ^{terms} for understanding message or data and its element value and actions.
- (C) Timing:- Timing refers to the synchronization and coordination between devices while transferring the data. Timing ensures, at what time data should be sent and how fast data can be sent. For example, If a sender sends hundred Mbps but the receiver can ^{only} handle 1 Mbps, the receiver will over flow and loss data. Timing ensures preventing of data loss, collisions and other timing related issues.

(D) Sequence control:- It ensures the proper ordering of data packets

(E) Flow control:- Flow control regulates device data delivery. It limits the sender data or the receiver if it is ready for more.

(F) Error control:- Error control mechanism detects and fixes data transmission faults. They include error detection codes, data resend and error recovery.

(G) Security:- Network security protects data confidentiality, authenticity and integrity, access control and other security procedures. Network communication privacy and trustworthiness are protected by security standards.

Types:-

(A) Network layer protocol:- Network layer protocols operate in the network layer which is also known as layer-3 of network architecture. It is responsible for packet routing, forwarding, and addressing of data packets throughout the networks. (IP and ICMP are the network-layer protocols). ICMP - Internet Control Message Protocol.

(B) Transport-layer protocols:- Transport layer protocols work in the transport layer which provides end-to-end service ensuring data transfer across apps on different devices. (TCP and UDP are transport-layer protocols). Transmission Control Protocol (TCP), User Datagram Protocol (UDP)

(C) Application-layer protocols:- It works in the application layer of network architecture. It provides communication between applications running on different devices. The application layer protocols enable cross-device communication. They format, exchange, and interpret application data. (HTTP - Hypertext Transfer Protocol, FTP - File Transfer Protocol, SMTP - Simple Mail Transfer Protocol are examples)

(D) Wireless protocols:- Wireless protocols are basically used in wireless communication which enables data transfer through wireless networks. (Bluetooth, Wi-Fi, LTE - Long Term Evolution).

(E) Internet Protocol (IP):- It provides data communication through routing and forwarding data packets from one device to another, by a unique addressing scheme.

Standards:-

It is a set of rules for data communication that are needed for the exchange of information among devices. It is important to follow standards which are created by various standard organizations like ISO (Indian Standard organization), IEEE - Institute of electrical and electronics engineering, ANSI (American National Standard Institute) etc.

Types:-

(A) De-facto standards:- The meaning of the word "De-facto" is "By fact" or "By-convention". These are the standards that have not been approved by any organization but have been adopted as standards because of their widespread use. For example, Apple and Google are two companies that are established their own rules for their products which are different.

(B) De-jure standards:- The meaning of word "de-jure" is "by-law" or "by regulations". Thus, these are the standards that have been approved by officially recognised body ISO, IEEE, ANSI, etc. For example, all the data communication,

standard protocol like SMTP, TCP, IP, UDP etc. are important to follow the same when we need them.

Network topology

Topology defines the structure of the network or how all the components are interconnected to each other. There are two types of topology.

- (a) Physical topology
- (b) Logical topology.

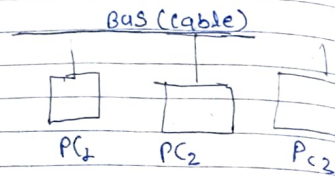
Types:-

Physical topology is the geometric representation of all the nodes in a network. There are six types of network topology which are

- (A) Bus topology
- (B) Ring topology
- (C) Tree topology
- (D) Star topology
- (E) Mesh topology
- (F) Hybrid topology.

A) Bus topology :-

The bus-topology is ~~defined~~ designed in such a way that all the stations are connected through a single cable known as a backbone cable.



Bus topology diagram

When a node wants to send a message over the network, it puts the message over the network. All the stations available in the network will receive the message whether it has been addressed or not.

Advantages :-

- Low cost cables :- In bus topology, ^{nodes} ~~nodes~~ are directly connected to the cable without passing to the hub. Therefore, the initial cost is low.
- Moderate data speed :- (Co-axial or twisted pair cables are mainly used in bus-based networks, that support upto 10Mbps.

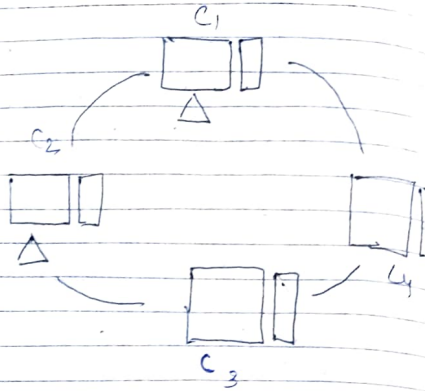
- Familiar technology :- The installation and troubleshooting techniques are well known and hardware components are easily available.

Disadvantages :-

- Signal interference :- If two nodes send the message simultaneously, then, the signals of both the nodes collide with each other.
- Reconfiguration difficulty :- Adding new-devices to the network would slow down the network.
- Attenuation :- ~~Attenuation~~ Attenuation is a loss of signal leads to communication issue. Repeaters are used to regenerate the signal.

(B) Ring topology:-

Ring topology is like a bus-topology, But with connected ends. The node that receives the message from the previous computer will transmit to the next node.



The data flows in one direction i.e. it is uni-direction. The data in a ring-topology flows in a clock-wise direction. It has no terminated ends. i.e. each node is connected to other node and having no termination point.

Advantage:-

- Network management:- faulty devices can be removed from the network without bringing the network down.
- Product availability:- Many hardware & software tools for network operation and monitoring are available.

- Cost:- Twisted pair cabling is inexpensive and easily available. Therefore, the installation cost is very low.
- Reliable:- It is more reliable network because the commⁿ system is not dependent on single host computer.

Disadvantage:-

- Difficult troubleshooting:- It requires specialized ~~it~~ requires special test equipment to determine the cable fault. If any fault occurs in the cable then it would disrupt the commⁿ for all the nodes.
- Failure:- The breakdown in one station leads to the failure of the overall network.
- Reconfiguration difficulty:- Adding new device to the network would slowdown the network.
- Delay:- Communication delay is directly proportional to the no. of nodes adding new devices, increase the commⁿ delay.

(C) Star-topology:-

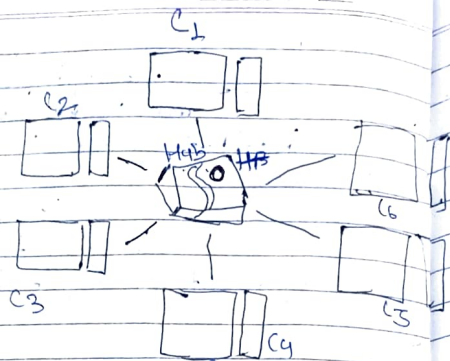
All host in star topology are connected to a central device known as hub device, using a

point-to-point connection. Star topology is an arrangement of the network in which every node is connected to the central hub, switch or central computer.

The central computer is known as a server, and the peripheral devices attached to the server are known as clients. Co-axial cable or RJ-45 cables are used to connect the computers. Hubs or switches are mainly used as connection devices in a physical star topology.

Advantage:-

- Efficient troubleshooting:- Troubleshooting is quite efficient in a star-topology as compared to bus topology.
- Network control:- Complex network control feature can be easily implemented in the star topology. Any changes made in the star



topology are automatically accommodated.

- Limited failure:- As each station is connected to the central hub with its own cable, therefore, failure in one cable will not affect the entire network.
- High data speed:- It supports a bandwidth of approx 100Mbps. Thus, star topology is used in abundant.

Disadvantage:-

- Central point of failure:- If a central hub or switch goes down, then all the connected nodes will not be able to communicate with each other.
- Cable:- Sometimes cable routing is difficult when a significant amount of routing is required.

(D) Hybrid topology:- The combination of various different topology is known as hybrid topology. A hybrid topology is connected between different links and nodes to transfer the data.

When two or more topologies are combined together is termed as hybrid topology.

and if similar topologies are connected with each other will not result in hybrid topology. For example, If there exist a ring topology in another one branch of ICICI bank and bus topology in another branch connecting this two topology will result in hybrid topology.

Advantage:-

- Reliable:- If a fault occurs, in any part of the network will not affect the functioning of the rest of the network.
- Scalable:- Size of the network can be easily expanded by adding new devices without affecting the functionality of the existing network.
- Flexible:- This topology is very flexible as it can be designed according to the requirements of the organizations.
- Effective:- It is very effective as it can be designed in such a way that the strength of network is maximised and weakness of the network is minimised.

Disadvantages:-

- Complex design:- The major drawback of the hybrid topology is the design of network. It is very difficult to design the architecture of hybrid network.
- Costly infrastructure:- The infrastructure cost is very high, as a hybrid network requires a lot of cabling network devices, hub etc.

Line configuration in C-networks

A network is two or more devices connected through a link. A link is a commⁿ path-way that transfers data from one device to other. Devices can be a computer, printer, or any other device i.e. capable to send and receive data.

Types:-

- Point-to-point connection:- A point-to-point connection provides a dedicated link between two devices. The entire capacity of the link is result for transmission between those two devices. Point-to-Point network topology is considered to be one of

the easiest and most conventional network topologies. It is also the simplest to establish and understand. For example, Point-to-point connection between the remote control and television, for changing the channels.

Features:-

- It uses a dedicated link to connect two devices.
- Simple and easy to set-up.
- It doesn't require a network interface card (NIC) or a hub/switch.

Advantages:-

- High bandwidth:- A point-to-point connection usually offers high bandwidth which makes them suitable for transferring large amount of data quickly.
- Security:- It is more secure than multi-point connections because the link is dedicated to only two devices.

Improved performance:- Point to point connection can improve network performance by reducing packet loss, and increasing the speed of data transmission.

Disadvantages:-

- Cost:- Setting up a point to point connection can be more expensive than setting up a shared link. This is because a dedicated link requires its own infrastructure. Such as cables, routers, and switches.
- Maintenance:- Because of point to point connection provides a dedicated link between two devices, it requires more maintenance than a shared link.

(B) Multi-point connection:- It is also called multi drop configuration. In this connection two or more devices, share a single link. If more the input devices share the link than the channel is considered, a shared channel with shared capacity, there can be two possibilities in a multipoint line configuration.

(a) Spacial sharing:-

If several devices can share the link simultaneously, it is called Spatially shared line configuration.

- b) Temporal (Time) Shared :- If users must take turns using the link then it is called temporally shared or time shared line configuration.

Features:-

- It uses a single link to three or more devices.
- More complex than point to point configuration.
- It can be efficient and cost effective for larger networks.
- Commonly used in large LANs, MANs

Advantage:-

- Cost effective :- Multi-point connections are usually less expensive than point to point connections because they allow multiple devices to share the same resources such as cables, routers and switches.
- Scalability :- Multi point connections are more scalable than point to point connection because they allow multiple devices to be connected to the same link.

- Increase Efficiency :- Multi-point connections can improve network efficiency by allowing multiple devices to transmit data simultaneously. This reduces the chances of network congestion and improves overall network performance.
- Greater access :- Multi-point connections can provide greater access to network resources, such as servers, printers, and storage devices. This allows users to share resources and collaborate more effectively, improving productivity and reducing cost.

Disadvantage:-

- Limited bandwidth :- Multi-point connection usually offer limited bandwidth because the link is shared by multiple devices as a result, the speed of the link may be affected by the no. of devices using it.
- Security :- Multipoint connections are less secure than point-to-point connections because the link is shared by multiple devices.

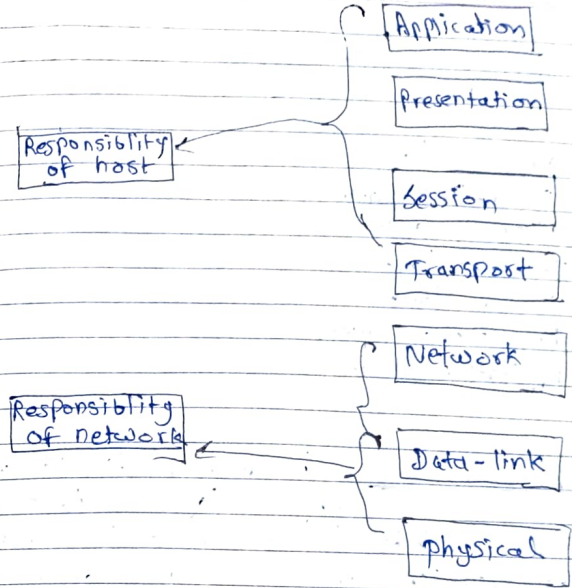
- Reliability :- Multi point connections are less reliable than point to point connection because the link is shared by the multiple devices.

OSI - model

OSI stands for Open System Interconnect is a reference model that describes how information from a software application in one computer moves through a physical medium to the software application in another computer.

OSI consists of seven layers and each layer performs a particular network function. OSI model was developed by International organization for standardization (ISO). in 1984.

Characteristics :-



The OSI model is divided into two layers upper layer and lower layer. The upper layer of OSI model mainly deals with the application related issues, and they are implemented only in the software. The lower layer of the OSI model deals with the data transport issue. The data link layer and the physical layer are implemented in hardware & software.

The physical layer is lowest layer of the OSI model and physical layer is mainly responsible for placing the information on the physical medium.

Layers of OSI model :-

- (A) Physical layer
- (B) Data-link layer
- (C) Network layer
- (D) Transport layer
- (E) Session layer
- (F) Presentation layer
- (G) Application layer

(A) Physical layer :- The main functionality of the physical layer is to transmit the individual bits from one node to another node. It establishes, maintains, and deactivates physical connections. It specifies the mechanical, electrical and procedural network interface specifications.

function :-

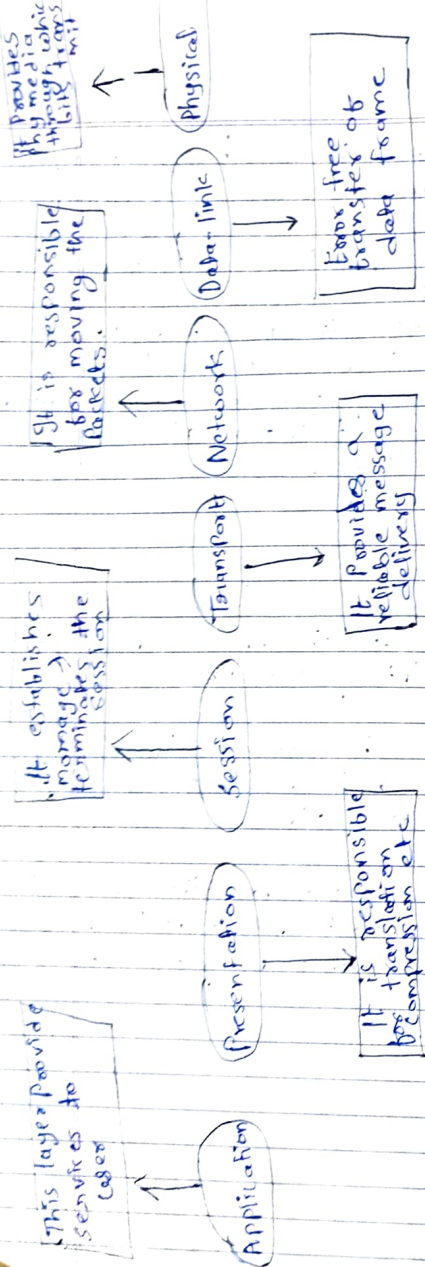
- Line configuration :- It defines the way how two or more devices can be connected physically.
- Data transmission :- It defines the transmission mode (Simplex, half duplex or full duplex mode)

• Topology :- It defines the way how network devices are arranged

- (B) Data-link layer :- This layer is responsible for error-free transfers of data-frames. It defines the format of the data on the network. It is mostly responsible for unique identification of each device that decide on a local network. It contains two sub-layer
- (a) Logic-link control layer.
 - (b) Media-access control layer.

functions :-

- Framing :- It translates the physical raw-bit stream into packets known as frames.
- Physical addressing :- The data-link layer adds a header to the frame that contains a destination address.
- Flow control :- It is the technic through which the constant data rate is maintain on both the sides so that no data get corrupted.



Flowchart of OSI Model

C) Network layer:- It is third layer of OSI model, that manages device addressing, tracks the location of devices on the network. It determines the best path to move data from source to destination based on the network conditions. The protocols used to route the network traffic are known as network layer protocols. eg- Protocols are IP and IPV-6.

Functions:-

- **Internet working:-** An internet provides a logical connection between different devices.
- **Addressing:-** It is used to identify the device on the internet.
- **Routing:-** It determines the best optimal path out of the multiple paths from source to the destination.

D) Transport layer:- The transport layer is the fourth layer of OSI-model, ensures that messages are transmitted in the order in which they are sent and there is no duplication of data. The main responsibility of transport layer is to transfer the data completely. It provides a point to point

connection b/w source and destination to delivery the data reliably. ~~The + reliability~~
The two protocols used in this layer!

(a) Transmission control protocol:- It establishes and maintains a connection b/w hosts.

(b) User data-gram protocol:- It is an unreliable transport protocol as in this case, receiver does not send any acknowledgement when the packet is received. The sender does not wait for any acknowledgement.

Function:-

- Service point addressing:- The transport layer adds the header that contains the address known as a service point address.
- Connection control:- Transport layer provides two service, connection oriented services and connection less service.

(c) Session layer:- It is a layer three of in OSI-model (responsibility of host). The session layer is used to establish, maintain and synchronises the interaction between communicating devices.

function:-

- Dialogue control:- It allows the communication between two processes which can be either half duplex or full duplex.
- Synchronisation:- If some error occurs in the middle of transmission of data then, the transmission will take place again from the check point. The process is known as synchronisation & recovery.

(d) Presentation layer:- A presentation layer is and mainly concerned with the syntax with the semantics of the information exchanged between the two systems. It acts as a data translator for a network. This layer is a part of the operating system that converts the data from one presentation format to another format. It is also known as the syntax layer.

Features:-

- Translation:- The process in two systems exchange the information in the form of character strings, no. and so on.
- Encryption:- Encryption is needed to maintain privacy. It is a process of converting the sender transmitted information into another form and send the resulting message over the network.
- Compression:- Data compression is a process of compressing the data i.e. it reduces the no. of bits to be transmitted. It is very important in multi-media such as text, audio, video.
- (G) Application layer:- An application layer serves as a window for users and application process to access network service. This layer provides the network services to the end users. It handles issues such as network transparency, resource allocations, etc.

Functions:-

- File transfer, access and management:- It allows a user to access the files in a remote computer, to retrieve

the files from a computer and to manage the files in a remote computer.

- Mail services:- It provides the facilities for e-mail forwarding.
- Dirac Directory Services:- It is used to provide that global information about various objects.

Types of tran

TCP/IP model (Transmission Control Protocol/IP)

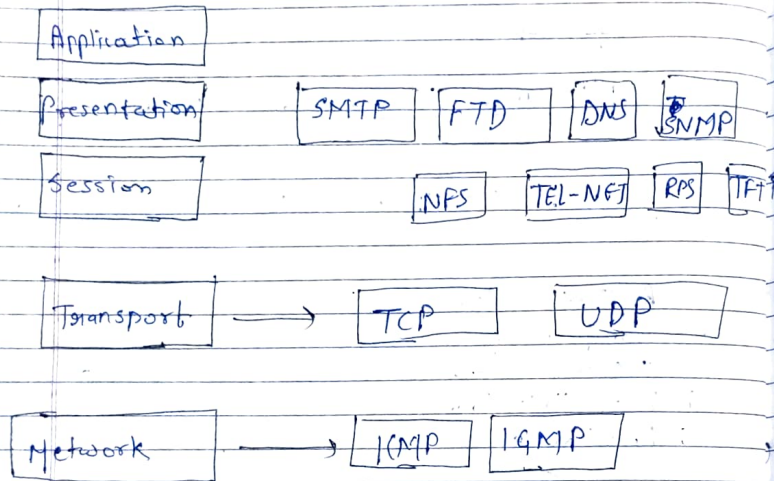
The TCP/IP model consists of five layers i.e. =

- (a) Application layer
- (b) Transport layer
- (c) Network layer
- (d) Data-link layer
- (e) Physical layer.

The first four layers provide physical standard network interface, internetworking and transport functions that corresponding to the first four layers of the OSI model. and these four layers are represented in TCP/IP model by a

Single layer called the application layer. TCP/IP is a ~~has~~ hierarchical protocols made up of interactive modules and each of them provides specific functionality. Here, ~~has~~ hierarchical means that each upper layer protocol is supported by two or more lower layer protocol.

Functions:-



(A) Application layer :- An application layer is the topmost layer in TCP/IP model. This layer allows the user to interact with the application. When one application layer protocol wants to communicate with another application layer, it forwards its data to the transport layer. Some main protocols used in the application layer are HTTP,

(a) Hyper-text transfer protocol :- This protocol allows us to access the data over the world wide web (www).

(b) Simple Network Management Protocol :- It is used as a framework used for managing the device on the internet by using the TCP/IP protocol suit.

(c) Simple mail transfer protocol :- The TCP/IP protocol that supports the e-mail is known as SMTP, and used to send the data to another e-mail address.

(d) Domain-Name System (DNS) :- An IP address is used to identify the connection of a host to the internet uniquely but people prefer to use the names instead of address. Therefore, the system that maps the

name to the address is known as DNS.

(E) Terminal Network (TEL-NET) :- It establishes the connection between the local computer and remote computer.

(F) File Transfer Protocol :- It is used for transmitting the files from one computer to another.

(B) Transport layer :- It is responsible for the reliability, flow control, and connection of data which is being sent over the network. The two protocols are used in transport layer are -

(a) User datagram protocol :- OSI model ←

(b) Transmission control Protocol :- OSI model ←

(C) Network layer :- It is the lowest layer of the TCP/IP model. A network layer is combination of physical layer & data-link layer defined in OSI reference model. It defines how the data should be sent physically through the network.

• Internet layer :- It is also known as network layer. It is second layer of the TCP/IP model. The main responsibility

of internet layer is to send the packets from any network, and they arrive at the destination irrespective of the route they take.

Following are the protocols in this layer -

(a) IP protocol :- Following are the responsibility of this protocol -

ii} IP addressing :- This protocol implements logical host addresses known as IP address.

iii} Host to host comm :-

iv} Data encapsulation & formatting :-

(b) ARP Protocol :- It is used to find the physical address from the IP address. The two terms are mainly associated. (a) ARP request (b) ARP reply.

(c) ICMP protocol :- It stands for Internet Control Message protocol. It is a mechanism used by the host or routers to send notifications regarding data-gram problems back to the sender. A data-gram travels from router to router until it reaches its destination. An ICMP protocol mainly uses two terms

(a) ICMP test (b) ICMP reply.

Types of transmission media

Transmission media is a communication channel that carries the information from the sender to the receiver. Data is transmitted through the electromagnetic signals. The main It is a physical path between transmitter and receiver in data communication.

In a copper based network, the bits in the form of electrical signals. In fibre based network, the bits in the form of light pulses.

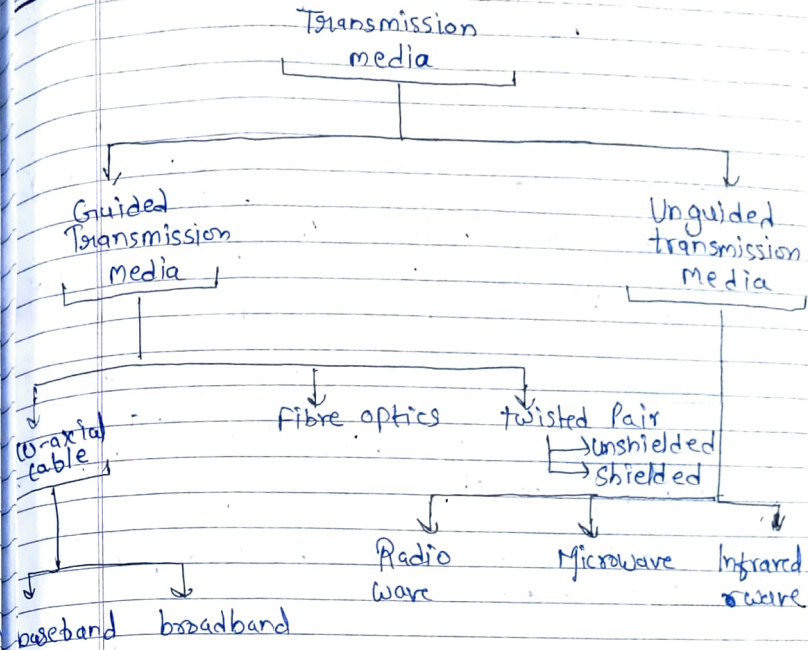
Factors:-

Following are the factors for designing transmission medium.

(A) Bandwidth:- The greater bandwidth of a medium the higher the data transmission rate of a signal.

(B) Transmission impairment:- When the received signal is not identical to the transmitted one due to transmission impairment. The quality of signal will get destroyed due to transmission impairment.

Classification:-



(A) Guided media :- It is defined as the physical media through which the signals are transmitted.

• Types :-

a) Twisted-Pair :- It is a physical media made up of a pair of cables twisted with each other. The frequency range for twisted pair cable is from 0-3.5 kHz. It is following types -

i) Unshielded :- It is widely used in tele-communication (telephone). It is cheaper, easy to instal, it can be used for high speed LAN. The

The main disadvantage that this cable can only be used for shorter distance.

ii) Shielded twisted-pair :- It is a cable that contains mesh surrounding the wire that allows the higher transmission rate. It has higher capacity as compare to unshielded twisted pair cable. The disadvantage is that it is more expensive, as compared to co-axial cable.

(b) Co-axial :- It commonly used transmission media for example T.V wire or DTH cable. The inner conductor of the co-axial cable is made up of copper. and the outer conductor is made up of copper mesh. The middle core is made up of non-conductive cover that separates the inner conductor from outer conductor.

The middle core is responsible for the data transferring whereas the copper mesh prevents from the EMI. (Electromagnetic Interference). It has following types -

i) Baseband transmission :- It is defined as the process of transmitting a single signal at high speed.

ii) Broadband :- It is defined as the process of transmitting multiple signals simultaneously.

The advantages of Co-axial is that the data can be transmitted at high speed, it has better shielding, as compared to twisted pair. The disadvantage is that it is more expensive, If any fault occurs in the cable causes the failure in the entire network.