Network Technology Questions Answer

Short questions

1)What are components of Network?

Ans :-

➔ Computer networks components comprise both physical parts as well asthe software required for installing computer networks, both at organizations and at home.

➔ The hardware components are the server, client, peer, transmission medium, and connecting devices. The software components are operating system and protocols

2)Define multicast and broadcast.

Ans:-

Broadcast Transmission (One-to-All)

In Broadcast transmission, the data is transmitted from one or more senders to all the receivers within the same network or in other networks. This type of transmission is useful in network management packets such as ARP (Address Resolution Protocol) and RIP (Routing Information Protocol) where all the devices must see the data.

There are two types of broadcast transmission –

Directed Broadcast, and

Limited Broadcast

Multicast Transmission (One-to-Many)

When the data is transmitted from a single source host to a specific group of hosts having the interest to receive the data, it is known as multicast transmission. Multicast can be more efficient than unicast when different groups of receivers need to see the same data.

Example – Multicast is the technique used in Internet streaming of video or audio teleconference, sending an email to a particular group of people, etc.

3) Define Intranet.

Ans:-

- The intranet is a private network that belongs to a particular organization.
- It is designed for the exclusive use of an organization and its associates, such as employees, customers, and other authorized people.
- It offers a secure platform to convey information and share data with authorized users.
- Confidential information, database, links, forms, and applications can be made available to the staff through the intranet.
- So, it is like a private internet or an internal website that is operating

within an organization to provide its employees access to its information and records.

- Each computer in intranet is identified by a unique IP Address.
- It is based on internet protocols (TCP/IP) and is protected from unauthorized access with firewalls and other security systems.
- The firewall monitors the incoming and outgoing data packets to ensure they don't contain unauthorized requests. So, users on the intranet can access the internet, but the internet users can't access the intranet if they are not authorized for it.
- Furthermore, to access the intranet, the authorized user is required to be connected to its LAN (Local Area Network).

4) Define Internet

Ans :-

- Internet is a global network that connects billions of computers across the world with each other and to the World Wide Web.
- It uses standard internet protocol suite (TCP/IP) to connect billions of computer users worldwide. It is set up by using cables such as optical fibers and other wireless and networking technologies.
- At present, internet is the fastest mean of sending or exchanging information and data between computers across the world.
- It is believed that the internet was developed by "Defense Advanced Projects Research Agency" (DARPA) department of the United States. And, it was first connected in 1969.
- Inter + Net =Interconnected Network

5) What is Active and Passive Hub?

Ans :-

Active hubs repeat and strengthen incoming transmissions. They are also sometimes referred to as repeaters.

Passive hubs simply serve as a point of connectivity, without any additional capabilities.

6) Define Gateways.

Ans:-

A gateway is simply a device or hardware that acts as a "gate" between the networks. We can also define it as a node that acts as an entry for other network nodes. It is also responsible for facilitating the traffic flow within the network. Gateway uses more than one communication protocol, so its activities are more complicated than a router or a switch. A gateway is essentially a system used to communicate between networks with different protocols and are responsible for converting one protocol into another. The gateway is a computer device that's responsible for routing traffic from the primary workstation to the outside network for every workplace form. It is responsible for providing access to the internet for households, thereby serving as an internet service provider. Since gateways and routers perform completely different functions, both are important for a network. A gateway serves as a single access point and a converter to connect dissimilar networks using different protocols, while a router sets the shortest path for the data packets to travel from source to destination.

7) What is Access Point?
Ans :-
An access point is a device that creates a wireless local area network, or WLAN, usually in an office or large building. An access point connects to a wired router, switch, or hub via an Ethernet cable, and projects a Wi-Fi signal to a designated area. For example, if you want to enable Wi-Fi access in your company's reception area but don’t have a router within range, you can install an access point near the front desk and run an Ethernet cable through the ceiling back to the server room.

8) What is Router?
Ans :-
A router is a network (internetworking) device which is responsible for routing traffic from one to another network.
These two networks could be a private company network to a public network.
You can think of a router as a traffic police who directs different network traffic to different directions.
A router is device that connects two networks. If you happened to have 2 LANs (local area networks) in your home or office and wanted to connect them, the router is the device that you would need.
The network that most home network connect to is the world’s biggest WAN (wide area network) the INTERNET
Router maintains Routing table
Router cannot connect directly to pc first, pc connect through switch and switch connects to router
Router used in wan mostly because its costly but you can used it in LAN too if you want. Router has 4 to 8 port

9) What is MODEM?
Ans :-
Most everyone wants to connect to the internet. A broadband modem is used to take a high speed Internet connection provided by an ISP (Internet Service Provider) and convert the data into a form that your local network can use. The high speed connection can be DSL (Digital Subscriber Line) from a phone company or cable from a cable television

provider.
A Modem is somewhat a more interesting network device in our daily life.
So if you have noticed around, you get an internet connection through a wire (there are different types of wires) to your house. This wire is used to carry our internet data outside to the internet world
However, our computer generates binary data or digital data in forms of 1s and 0s and on the other hand, a wire carries an analog signal and that's where a modem comes in.
A modem stands for (Modulator+Demodulator).
That means it modulates and demodulates the signal between the digital data of a computer and the analog signal of a telephone line.

10) What is topology? Define the types of topologies.
Ans :-
Topology :- The arrangement of a network which comprises of nodes and connecting lines viasender and receiver is referred as network topology.
The various network topologies are:

Type of topology :-
1.mesh topology
2.bus topology
3.star topology
4.ring topology
5.tree topology
6.hybrid topology

11) What is Network topology?
Ans :-
The arrangement of a network which comprises of nodes and connecting lines viasender and receiver is referred as network topology.

12) Define Baud rate.
Ans :-

13) Define Nyquist bit rate
Ans :- Nyquist gives the upper bound for the bit rate of a transmission system by calculating the bit rate directly from the number of bits in a symbol (or signal levels) and the bandwidth of the system

14) Write about the concept of client and server.
Ans :-
Server:
A server is a computer in network that provides services to the client computers such as logon requests processing, files access and storage,

internet access, printing access and many other types of services. Servers are mostly equipped with extra hardware such as plenty of external memory (RAM), more data store capacity (hard disks), high processing speed and other features.

Client:

The client is a process that sends a message to a server process requesting that the server perform a task

Client programs usually manage the user-interface portion of the application, validate data entered by the user, dispatch requests to server programs, and sometimes execute business logic. The client-based process is the front- end of the application that the user sees and interacts with. Theclient process contains solution-specific logic and provides the interface between the user and the rest of the application system.

15) Define HTTP and HTTPS

Ans :-

- HTTP stands for HyperText Transfer Protocol and HTTPS stands for HyperText Transfer Protocol Secure.
- URL begins with "http://" whereas URL starts with "https://"
- HTTP uses port number 80 for communication and HTTPS uses 443
- HTTP is considered to be insecure and HTTPS is secure
- HTTP Works at Application Layer and HTTPS works at Transport Layer
- In HTTP, Encryption is absent and in HTTPS Encryption is present.
- HTTP does not require any certificates and HTTPS needs SSL Certificates
- HTTP speed is faster than HTTPS and HTTPS speed is slower than HTTP
- HTTP does not improve search ranking while HTTPS improves search ranking.
- HTTP does not use data hashtags to secure data, while HTTPS will have the data before sending it and return it to its original state on the receiver side.
- HTTPS uses TLS or SSL to encrypt HTTP requests and responses. So basically, the only difference between the two protocols is that HTTPS uses TLS (SSL) to encrypt normal HTTP requests and responses.

16) Define Telnet and FTP.

Ans :-

❖ TELNET

TELNET is basically the short form for TErminal NETwork.It is basically a TCP/IP protocol that is used for virtual terminal services

- It is a general-purpose client/server application program.
- This program enables the establishment of the connection to the remote system in such a way that the local system starts to appear as a terminal

at the remote system.

- It is a standard TCP/IP protocol that is used for virtual terminal service.
- In simple words, we can say that the telnet allows the user to log on to a remote computer. After logging on the user can use the services of the remote computer and then can transfer the results back to the local computer.
- TELNET makes the use of only one TCP/IP connection.

➢ FTP(file transfer protocol)

○ FTP stands for File transfer protocol.
○ FTP is a standard internet protocol provided by TCP/IP used for transmitting the files from one host to another.
○ It is mainly used for transferring the web page files from their creator to the computer that acts as a server for other computers on the internet.
○ It is also used for downloading the files to the computer from other servers.

17) What is UTP and STP?
Ans :-
Unshielded twisted pair (UTP):-
There is no shield in unshielded twisted pair means no mental foil in UTP
UTP cable is more common than STP cables because it's costs less than STP and easily available dua to its many use
Dua to its low cost ,UTP cabling is widely used for local-area networks (LANs) and telephone connections because of its low cost
Unshielded twisted-pair cables do not provide high bandwidth or good protection from interference like coaxial or fiber optic cables ,but UTP cables are low-cost and easier to work with.

Shielded twisted pair (STP) :-

These types of cables have metal foil covering each pair of insulator conductors.
Shielded in STP cable helps to prevent electromagnetic noise and also eliminates crosstalk. The data transmission rate is higher in STP.
Because of mental foil covering .these cables are more expensive than coaxial and unshielded twisted pairs.

18) What is Co-axial?
Ans :-

Coaxial cable has two wires of copper .
The core/inner copper wire is in the center and is made of the solid conductor which is used for actual data transmission .it is enclosed in an

insulating sheath.
The second /external copper wire is wrapped around and used to protect against external electromagnetic interference (noise).
This all covered by plastic cover used to protect the inner layers from physical damage such as fire or water.

19) Why twists are required in Twisted pair cable?
Ans :- The twisting is necessary to minimize electromagnetic radiation and resist external interference. It also helps to limit interference with other adjacent twisted pairs (cross-talk)

20) Define UDP and TCP
Ans :-
UDP :-

o UDP stands for User Datagram Protocol.
o UDP is a simple protocol and it provides non sequenced transport functionality. o UDP is a connectionless protocol.
o This type of protocol is used when reliability and security are less important than speed and size.
o UDP is an end-to-end transport level protocol that adds transport-level addresses, checksum error control, and length information to the data from the upper layer.
o The packet produced by the UDP protocol is known as a user datagram

TCP :-

o TCP stands for Transmission Control Protocol.
o It provides full transport layer services to applications.
o It is a connection-oriented protocol means the connection established between both the ends of the transmission. For creating the connection, TCP generates a virtual circuit between sender and receiver for the duration of a transmission.

21) What is an IPv4 address?
Ans :-
Internet protocol version 4 . it consists of 4 numbers separated by the dots . each number can be from 0-255 in decimal
Since each number N can represented by a group of 8 digit binary digits . so, a whole IPv4 binary address can be represented by 32-bits of binary digits. In IPv4 a unique sequence of bits is assigned to a computer , so a

total of (2^32) devices approximately = 4,294,967,296 can be assigned with IPv4.
IPv4 can be written as :

    189.123.123.90

22) What is an IPv6 address?
Ans :-
There is a problem with the IPv4 address . with IPv4 , we can connect only the above number of 4 billion devices uniquely , and apparently , there are much more devices in the world to be connected to the internet So , gradually we are making our way IPv6 address which is a 128-bit IP address .
In human-friendly form , IPv6 written as a group of 8 hexadecimal numbers separated with colons (:) . but in the computer-friendly form , it can be written as 128 bits of 0s and 1s.
IPv6 can be written as:

 2011:0bd9:75c5:0000:0000:6b3e:0170:8394

23) What is MAC address?
Ans :-
MAC Addresses are unique 48-bits hardware number of a computer, which is embedded into network card (known as Network Interface Card) during the time of manufacturing. MAC Address is also known as Physical Address of a network device. In IEEE 802 standard, Data Link Layer is divided into two sublayers –

Logical Link Control(LLC) Sublayer
Media Access Control(MAC) Sublayer

24) What is IP address?
Ans :-
An IP address is the identifier that enables your devices to send or receive data packets across the internet. It holds information related to your location and therefore makes devices available for two-way communication . the internet requires a process to distinguish between different networks , routers and websites.
An IP address is represented by a series of number segregated by periods (.). they are expressed in the form of four pairs -an example address might be 255.255.255.255 wherein each set can range from 0 to 255.

25) What is PAN?
Ans :-
A personal area network (PAN) connects electronic devices within a user's immediate area. The size of a PAN ranges from a few centimeters to a few meters. One of the most common real-world examples of a PAN is the connection between a Bluetooth earpiece and a smartphone. PANs can also connect laptops, tablets, printers, keyboards, and other computerized devices.

26) What is MAN?
Ans :-
MAN stands for 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 organization.

27) What is WAN?
Ans :-
WAN stands for wide area network. It covers a large area than LAN as well as a MAN such as country/continent etc. WAN is expensive and should or might not be owned by one organization. PSTN or satellite medium is used for wide area networks.

28) What is LAN?
Ans :-
LAN stands for local area network. It is a group of network devices that allow communication between various connected devices. Private ownership has control over the local area network rather than the public. LAN has a short propagation delay than MAN as well as WAN. It covers smaller areas such as colleges, schools, hospitals, and so on.

29) What is the use of PORT number?
Ans :-
Port numbers identify a particular application or service on a system. An IP address identifies a machine in an IP network and determines the destination of a data packet, while port numbers identify particular applications or services on a system.

30) List out the connectionless protocol.
Ans :- HTTP (hypertext transfer), ICMP, IP, IPX, UDP, and TIPC.

31) List out the connection oriented protocol.
Ans :- telnet, rlogin, and ftp.

32) Give the full form of SMTP, DNS and POP with their port number
Ans :- SMTP :- Simple Mail Transfer Protocol :- port 587
DNS :- Domain Name System :- port 53
POP :- Point of Presence Or Post Office Protocol :- port 995:

33) Give the full form of HTTP, HTTPS and FTP with their port number.
Ans :-
HTTPS :- HyperText Transfer Protocol Secure :- port 443
FTP :- File Transfer Protocol :- port 21 and 20

34) Define layer of OSI Model. Which layer is a heart of OSI model?
Ans :-

Application layer
Presentation layer
Session layer
Transport layer
Network layer
Data link layer
Physical layer

Transport layer is a heart of OSI model

35) Which layer of OSI is responsible for Encryption and Decryption of data?

Ans :- Presentation layer

36) What is the purpose of Presentation layer?
Ans :-
A Presentation layer is mainly concerned with the syntax and 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.
The Presentation layer is also known as the syntax layer.

37) What are the functions of Data link layer?
Ans :-
Framing: The data link layer translates the physical's raw bit stream into packets known as Frames. The Data link layer adds the header and trailer to the frame. The header which is added to the frame contains the hardware destination and source address.
Physical Addressing: The Data link layer adds a header to the frame that contains a destination address. The frame is transmitted to the destination address mentioned in the header.
Flow Control: Flow control is the main functionality of the Data-link layer. It is the technique through which the constant data rate is maintained on both the sides so that no data get corrupted. It ensures that the transmitting station such as a server with higher processing speed does not exceed the receiving station, with lower processing speed.
Error Control: Error control is achieved by adding a calculated value CRC (Cyclic Redundancy Check) that is placed to the Data link layer's trailer which is added to the message frame before it is sent to the physical layer. If any error seems to occur, then the receiver sends the acknowledgment for the retransmission of the corrupted frames.
Access Control: When two or more devices are connected to the same communication channel, then the data link layer protocols are used to determine which device has control over the link at a given time.

38) What are the functions of Network layer?
Ans :-
Internetworking: An internetworking is the main responsibility of the network layer. It provides a logical connection between different devices.
Addressing: A Network layer adds the source and destination address to the header of the frame. Addressing is used to identify the device on the internet.
Routing: Routing is the major component of the network layer, and it determines the best optimal path out of the multiple paths from source to the destination.
Packetizing: A Network Layer receives the packets from the upper layer and converts them into packets. This process is known as Packetizing. It is achieved by internet protocol (IP).

39) What are the functions of Transport layer?
Ans :-
Service-point addressing: Computers run several programs simultaneously due to this reason, the transmission of data from source to the destination not only from one computer to another computer but also from one process to another process. The transport layer adds the header that contains the address known as a service-point address or port

address. The responsibility of the network layer is to transmit the data from one computer to another computer and the responsibility of the transport layer is to transmit the message to the correct process.

Segmentation and reassembly: When the transport layer receives the message from the upper layer, it divides the message into multiple segments, and each segment is assigned with a sequence number that uniquely identifies each segment. When the message has arrived at the destination, then the transport layer reassembles the message based on their sequence numbers.

Connection control: Transport layer provides two services Connection-oriented service and connectionless service. A connectionless service treats each segment as an individual packet, and they all travel in different routes to reach the destination. A connection-oriented service makes a connection with the transport layer at the destination machine before delivering the packets. In connection-oriented service, all the packets travel in the single route.

Flow control: The transport layer also responsible for flow control but it is performed end-toend rather than across a single link

Error control: The transport layer is also responsible for Error control. Error control is performed end-to-end rather than across the single link. The sender transport layer ensures that message reach at the destination without any error.

40) Which protocols are used in Application Layer?
Ans :-
The following are some of the protocols which are provided by the application layer.
TELENET
DNS
DHCP
FTP
SMTP
HTTP
NFS
SNMP

41) What is MANET? What are their types?
Ans :-
MANET stands for Mobile adhoc Network also called as wireless adhoc network or adhoc wireless network. They consist of a set of mobile nodes connected wirelessly in a self-configured, self-healing network without

having a fixed infrastructure. MANET nodes are free to move randomly as the network topology changes frequently.
Types of MANET
Vehicular Ad hoc Network (VANETs)
Smart Phone Ad hoc Network (SPANC)
Internet based Mobile Ad hoc Network (iMANETs)
Hub-Spoke MANET
Military or Tactical MANETs
Flying Ad hoc Network (FANETs)

42) What is Packet? Use of Datagram Packet
Ans :- Datagram packets are used to implement a connectionless packet delivery service. Each message is routed from one machine to another based solely on information contained within that packet. Multiple packets sent from one machine to another might be routed differently, and might arrive in any order

43) Define different types of transmission mode.
Ans :- **The transmission modes are of three major types:**
Simplex Transmission Mode.
Half Duplex Transmission Mode.
Full Duplex Transmission Mode.

44) What is Absolute URL?
Ans :- An absolute URL is the full URL, including protocol (http / https), the optional subdomain (e.g. www), domain (example.com), and path (which includes the directory and slug). Absolute URLs provide all the available information to find the location of a page.

45) What is Relative URL?
Ans :- A relative URL is a URL that only includes the path. The path is everything that comes after the domain, including the directory and slug. Because relative URLs don't include the entire URL structure, it is assumed that when linking a relative URL, it uses the same protocol, subdomain and domain as the page it's on.

- ❖ Long questions

1) Explain types of networks in detail

Ans:-

- **Local Area Network (LAN)** –

LAN or Local Area Network connects network devices in such a way that personal computers and workstations can share data, tools, and programs. The group of computers and devices are connected together by a switch, or stack of switches, using a private addressing scheme as defined by the TCP/IP protocol. Private addresses are unique in relation to other computers on the local network. Routers are found at the boundary of a LAN, connecting them to the larger WAN.

Data transmits at a very fast rate as the number of computers linked is limited. By definition, the connections must be high-speed and relatively inexpensive hardware (Such as hubs, network adapters, and Ethernet cables). LANs cover a smaller geographical area (Size is limited to a few kilometres) and are privately owned. One can use it for an office building, home, hospital, school, etc. LAN is easy to design and maintain. A Communication medium used for LAN has twisted-pair cables and coaxial cables. It covers a short distance, and so the error and noise are minimized. Early LANs had data rates in the 4 to 16 Mbps range. Today, speeds are normally 100 or 1000 Mbps. Propagation delay is very short in a LAN. The smallest LAN may only use two computers, while larger LANs can accommodate thousands of computers. LAN has a range up to 2km. A LAN typically relies mostly on wired connections for increased speed and security, but wireless connections can also be part of a LAN. The fault tolerance of a LAN is more and there is less congestion in this network. For example A bunch of students playing Counter-Strike in the same room (without internet).

Advantages:

Provides fast data transfer rates and high-speed communication.

Easy to set up and manage.

Can be used to share peripheral devices such as printers and scanners.

Provides increased security and fault tolerance compared to WANs.

Disadvantages:

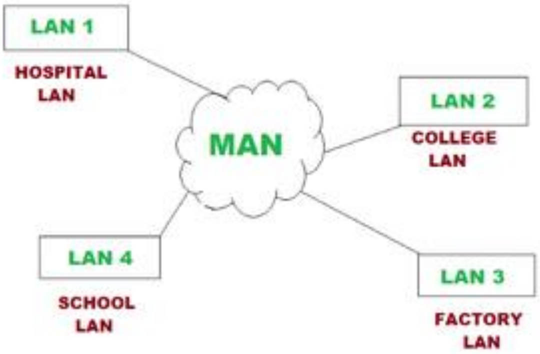
Limited geographical coverage.

Limited scalability and may require significant infrastructure upgrades to accommodate growth.

May experience congestion and network performance issues with increased usage.

- Metropolitan Area Network (MAN) –

MAN or Metropolitan area Network covers a larger area than that covered by a LAN and a smaller area as compared to WAN. MAN has a range of 5-50km. It connects two or more computers that are apart but reside in the same or different cities. It covers a large geographical area and may serve as an ISP (Internet Service Provider). MAN is designed for customers who need high-speed connectivity. Speeds of MAN range in terms of Mbps. It's hard to design and maintain a Metropolitan Area Network.



The fault tolerance of a MAN is less and also there is more congestion in the network. It is costly and may or may not be owned by a single organization. The data transfer rate and the propagation delay of MAN are moderate. Devices used for transmission of data through MAN are Modem and Wire/Cable. Examples of a MAN are part of the telephone company network that can provide a high-speed DSL line to the customer or the cable TV network in a city.

Advantages:

Provides high-speed connectivity over a larger geographical area than LAN.

Can be used as an ISP for multiple customers.

Offers higher data transfer rates than WAN in some cases.

Disadvantages:

Can be expensive to set up and maintain.

May experience congestion and network performance issues with increased usage.

May have limited fault tolerance and security compared to LANs.

- Wide Area Network (WAN) –

WAN or Wide Area Network is a computer network that extends over a large geographical area, although it might be confined within the bounds of a state or country. WAN has a range of above 50 km. A WAN could be a connection of LAN connecting to other LANs via telephone lines and radio waves and may be limited to an enterprise (a corporation or an organization) or accessible to the public. The technology is high-speed and relatively expensive.

There are two types of WAN: Switched WAN and Point-to-Point WAN. WAN is difficult to design and maintain. Similar to a MAN, the fault tolerance of a WAN is less and there is more congestion in the network. A Communication medium used for WAN is PSTN or Satellite Link. Due to long-distance transmission, the noise and error tend to be more in WAN. WAN's data rate is slow about a 10th LAN's speed since it involves increased distance and increased number of servers and terminals etc. The speed of WAN ranges from a few kilobits per second (Kbps) to megabits per second (Mbps). Propagation delay is one of the biggest problems faced here. Devices used for the transmission of data through WAN are Optic wires, Microwaves, and Satellites. An example of a Switched WAN is the asynchronous transfer mode (ATM) network and Point-to-Point WAN is a dial-up line that connects a home computer to the Internet.

Advantages:

Covers large geographical areas and can connect remote locations.

Provides connectivity to the internet.

Offers remote access to resources and applications.

Can be used to support multiple users and applications simultaneously.

Disadvantages:

Can be expensive to set up and maintain.

Offers slower data transfer rates than LAN or MAN.

May experience higher latency and longer propagation delays due to longer distances and multiple network hops.

May have lower fault tolerance and security compared to LANs.

2)What is Network topology? Explain various types of topologies with merits and demerits

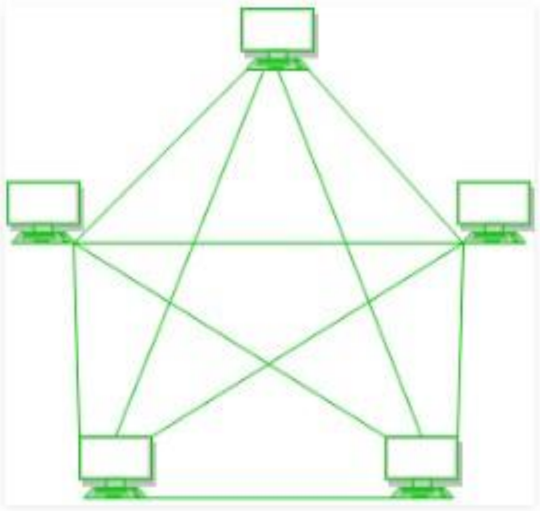
Ans :-

- Network Topology:

The arrangement of a network which comprises of nodes and connecting lines viasender and receiver is referred as network topology. The various network topologies are:

- Mesh Topology:

➔ A mesh topology, every device has a **dedicated point-to-point** link to every other device.
➔ The term dedicated means that the link carries traffic only between the two devices it connects.
➔ If suppose, N number of devices are connected with each other in mesh topology, then total number of ports that is required by each device is N-
In the Figure , there are 5 devices connected to each other, hence total number of ports required is 4.
➔ If suppose, N number of devices are connected with each other in mesh topology, then total number of dedicated links required to connect them is ${}^{N}C_2$ i.e. N(N-1)/2. In the Figure , there are 5 devices connected to eachother, hence total number of links required is 5*4/2 = 10.



Every device is connected with another via dedicated channels. These channels are known as links.

Advantages:

No traffic problem as there are dedicated links.
Robust as failure of one link does not affect the entire system.
Security as data travels along a dedication easy
Point to point links mark fault identification easy
Provides security and privacy.

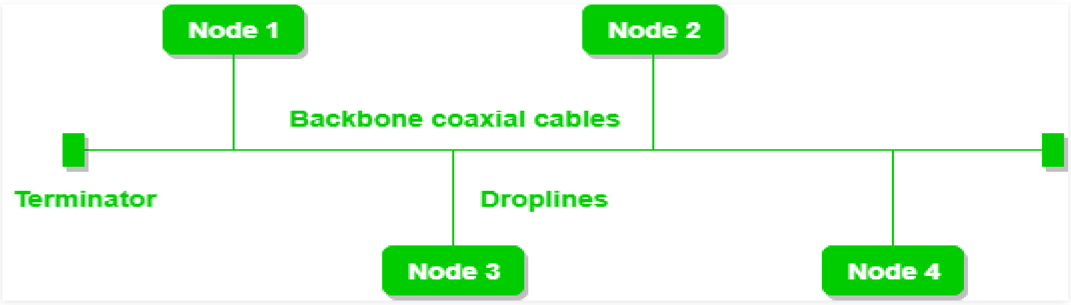
Disadvantages:

There is mesh of wiring which can be difficult to manage
Installation and configuration is difficult.
Cost of cables is high as bulk wiring is required, hence suitable for less number of devices.

Cost of maintenance is high.

- Bus Topology:

➔ Physical Bus Network Topology is the simplest and most widely used of the network designs.
➔ It consists of one continuous length of cable (trunk) and a terminating resistor (terminator) at each end.
➔ Data communication message travels along the bus in both directions until it is picked up by a workstation or server NIC.
➔ If the message is missed or not recognized, it reaches the end of the cabling and dispelled at the terminator.
➔ Bus Network Topology requires a multipoint connection.
➔ All nodes on the bus topology have equal access to the trunk
➔ This is accomplished using short drop cables or direct T-connectors.
➔ The number of devices and the length of the trunk can be easily expanded.



A bus topology with shared backbone cable. The nodes are connected to the channel via drop lines

Advantages:

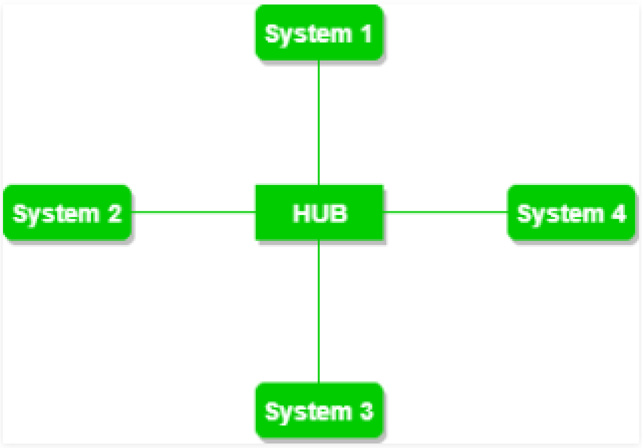
It uses established standards and it is relatively easy to install.
It requires a less media than other topologies.
Cost of the cable is less as compared to other topology, but it is used to builtsmall networks (LAN).
Does not require any special networking device

Disadvantages:

The bus networks are difficult to reconfigure, especially when the acceptablenumber of connections or maximum distance have been reached.
If the common cable fails, then the whole system will crash down.
If the network traffic is heavy, it increases collisions in the network.

- Star Topology:

➔ Physical star Network Topology is the most widely used of the network designs.
➔ It uses a central controlling hub / switch with dedicated pointing in all directions like points of a star.
➔ Each network device has a dedicated point-to-point link t the central hub.
➔ This strategy prevents troublesome collisions and keeps the lines of communications open and free of traffic This Network Topology, obviously, require a great deal cabling.
➔ This design provides an excellent platform for reconfiguration and trouble-shooting.
➔ Changes to the network are as simple as plugging another segment intothe hub and a break in the LAN is easy to isolate and doesn't affect the rest of the network.



A star topology having four systems connected to single point of connection i.e. hub

Advantages:

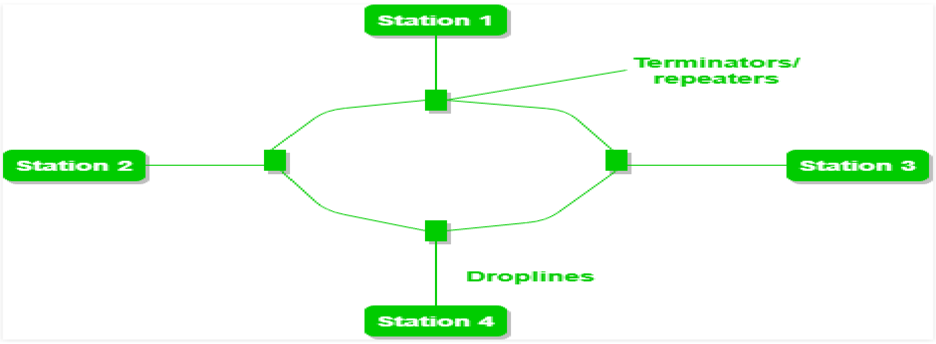
Relatively easy to configure. If N devices are connected to each other in startopology, then the number of cables required to connect them is N. So, it is easy to set up.
Easy to troubleshoot
Media faults are automatically isolated to the fail segment.
Each device requires only 1 port i.e. to connect to the hub.
Used in big network
Easily add and remove devices

Disadvantages

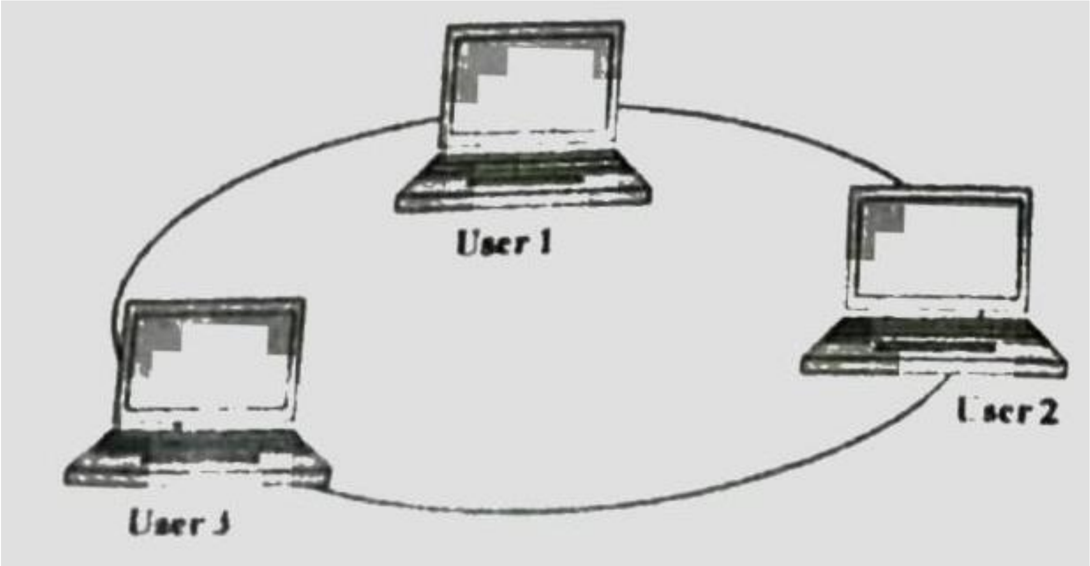
If the concentrator (hub) on which the whole topology relies fails, the wholesystem will crash down.
Cost of installation is high.
Performance is based on the single concentrator i.e. hub.

- Ring Topology:

➔ The physical ring Network Topology is a circular loop of point-to-point links.
➔ In this topology, it forms a ring connecting a devices with its exactly twoneighbouring devices.
➔ Each device connects directly to the ring or indirectly through an interface device or drop cable.
➔ Message travel around the ring from node to node in a very organized manner.
➔ Each workstation checks the message for a matching destination address.
➔ If the address doesn't match the node simply regenerates the message and sends it on its way.
➔ If the address matches, the node accepts the message and sends a replyto the originating sender.
➔ The following operations takes place in ring topology are :
➔ One station is known as **monitor** station which takes all the responsibilityto perform the operations.
➔ To transmit the data, station has to hold the token. After the transmissionis done, the token is to be released for other stations to use.
➔ When no station is transmitting the data, then the token will circulate inthe ring.



A ring topology comprises of 4 stations connected with eachforming a ring



Advantages:

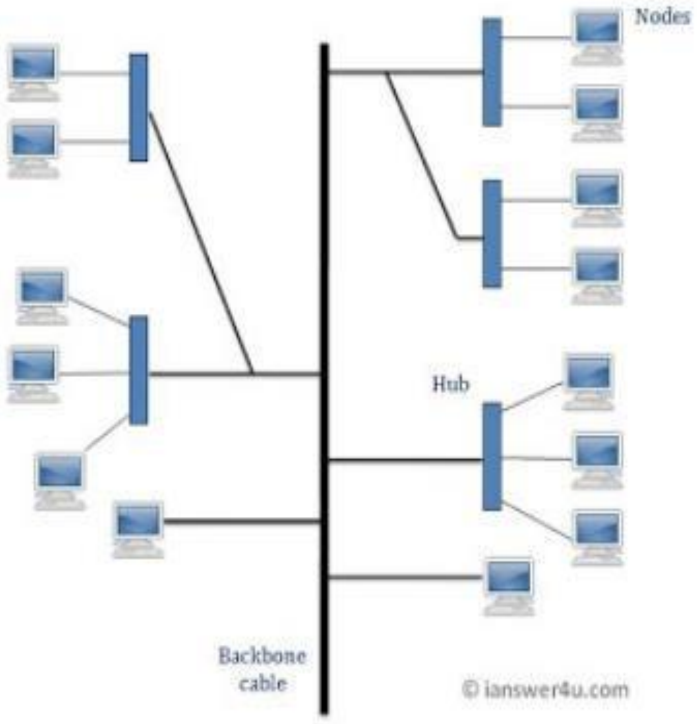
They are very easy to troubleshoot because each device incorporates a repeater.
A special internal feature called beaconing allows troubled workstations to identify themselves quickly.The possibility of collision is minimum in this type of topology.

Disadvantages:

It is considerably difficult to install and reconfigure ring Network Topology
Media failure on unidirectional or single loop causes complete network failure.
Addition of stations in between or removal of stations can disturb the wholetopology.

- Tree Topology:

➔ Tree Topology integrates the characteristics of Star and Bus Topology.
➔ In Tree Topology, the number of Star networks is connected using Bus.
➔ This main cable seems like a main stem of a tree, and other star networks asthe branches.
➔ It is also called **Expanded Star Topology**.



Tree Topology

Advantages

It is an extension of Star and bus Topologies, so in networks where these topologies can't be implemented individually for reasons related to scalability,tree topology is the best alternative.

Expansion of Network is possible and easy.

Here, we divide the whole network into segments (star networks), which canbe easily managed and maintained.

Error detection and correction is easy.

Each segment is provided with dedicated point-to-point wiring to the centralhub.

If one segment is damaged, other segments are not affected.

Disadvantages

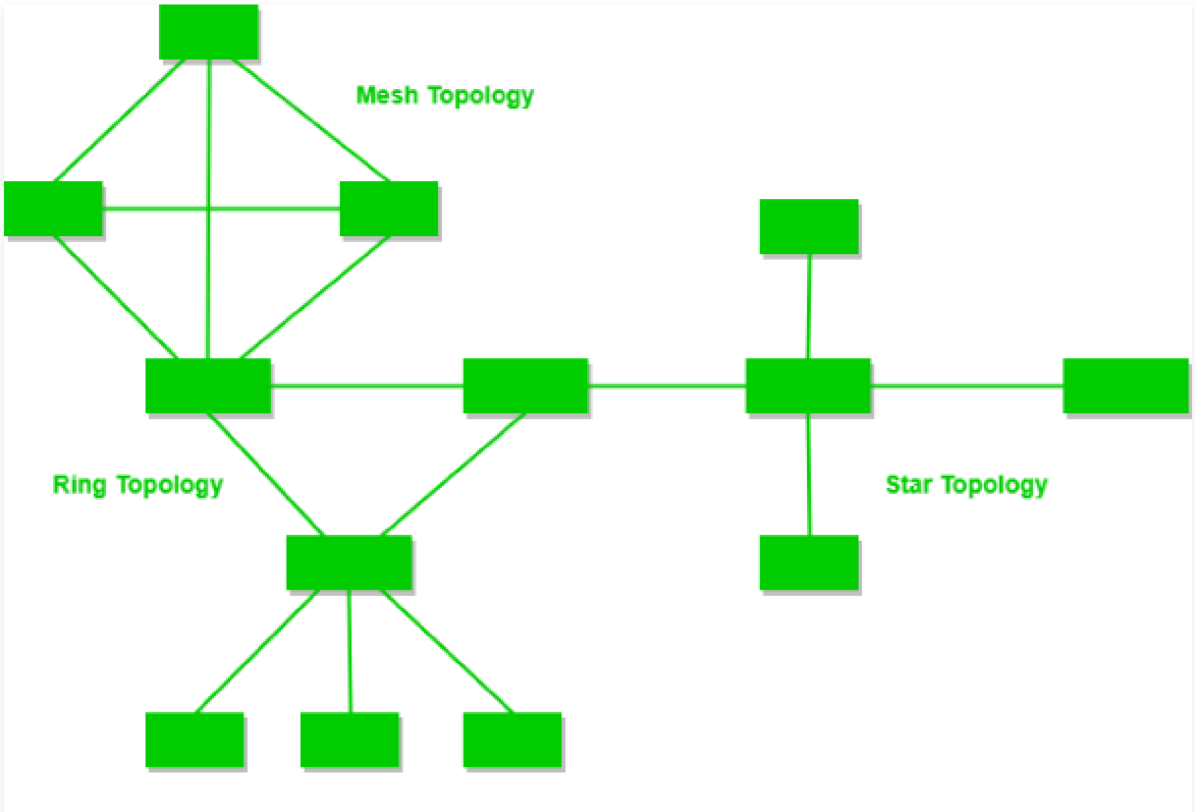
Because of its basic structure, tree topology, relies heavily on the main buscable, if it breaks whole network is crippled.

As more and more nodes and segments are added, the maintenance becomes difficult.

- Hybrid Topology:

➔ The hybrid Network topology is a type of network that is composed of oneor more interconnection of two or more networks that are based upon

different physical topologies.
➔ This topology is a collection of two or more topologies which are describedabove. This is a scalable topology which can be expanded easily. It is reliable one but at the same it is a costly topology.



3)Explain Ring topology with Merits and Demerits
Ans : - IN que 3

4)Explain Mesh topology with Merits and Demerits.
Ans :- In que 3

5)Explain Tree topology with Merits and Demerits
Ans:- In que 3

6)Write a short note on Unicast, Multicast and Broadcast.
Ans:-
Casting in computer networks means transmitting data (stream of packets) over a network. Following are the different types of casting used in networking –
Unicast transmission
Broadcast transmission
Multicast transmission

Unicast Transmission (One-to-One)

In Unicast transmission, the data is transferred from a single sender (or a single source host) to a single receiver (or a single destination host).

The network switches hear the MAC addresses of the devices on the networks to which they are connected. They can then forward packets only onto those networks containing devices with the connected MAC addresses. Unicast gradually becomes less efficient as more receivers need to see identical data.

Example

In the following figure, Host A sends the IP address 11.1.2.2 data to the Host B IP address 20.12.4.3.

Source Address = IP address of host A is 11.1.2.2

Destination Address = IP address of host B is 20.12.4.3

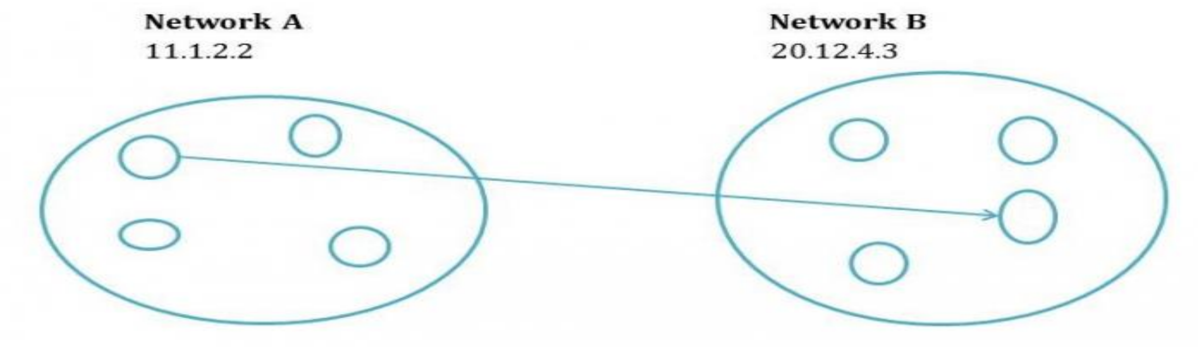


Figure: Unicast

Broadcast Transmission (One-to-All)

In Broadcast transmission, the data is transmitted from one or more senders to all the receivers within the same network or in other networks. This type of transmission is useful in network management packets such as ARP (Address Resolution Protocol) and RIP (Routing Information Protocol) where all the devices must see the data.

There are two types of broadcast transmission –

Directed Broadcast, and

Limited Broadcast

Directed Broadcast

Directed Broadcast transmits data from one source host to all the other hosts that exist in some other network. It is used in two scenarios –

When the hosts are responsible for parsing data from broadcast packets.

When all the hosts require the same data.

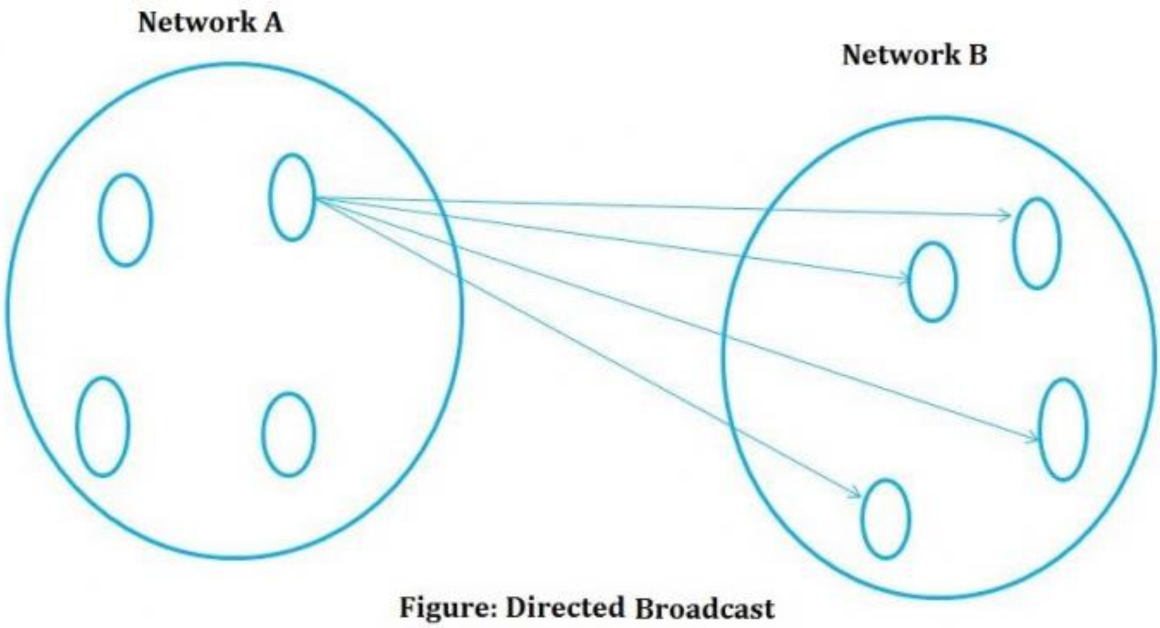


Figure: Directed Broadcast

Multicast Transmission (One-to-Many)

When the data is transmitted from a single source host to a specific group of hosts having the interest to receive the data, it is known as multicast transmission. Multicast can be more efficient than unicast when different groups of receivers need to see the same data.

Example – Multicast is the technique used in Internet streaming of video or audio teleconference, sending an email to a particular group of people, etc.

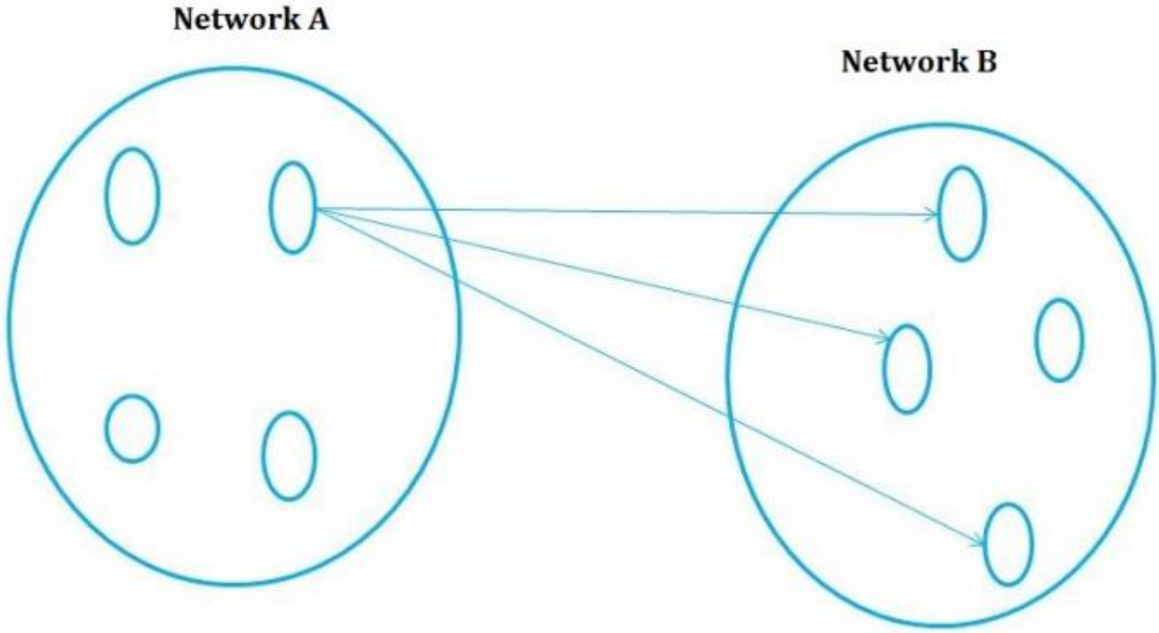


Figure: Multicast

7)Explain working of Internet and its architecture.
Ans :-
Internet : -
Internet is a global network that connects billions of computers across the world with each other and to the World Wide Web. It uses standard internet protocol suite (TCP/IP) to connect billions of computer users worldwide. It is set up by using cables such as optical fibers and other wireless and networking technologies. At present, internet is the fastest mean of sending or exchanging information and data between computers across the world. It is believed that the internet was developed by "Defense Advanced Projects Agency" (DARPA) department of the United States. And, it was first connected in 1969.

Internet Architecture:-
Internet architecture is a meta-network, which refers to a congregation of thousands of distinct networks interacting with a common protocol. In simple terms, it is referred as an internetwork that is connected using protocols. Protocol used is TCP/IP. This protocol connects any two networks that differ in hardware, software and design.

Process:-

TCP/IP provides end to end transmission, i.e., each and every node on one network has the ability to communicate with any other node on the network.

Layers of Internet Architecture:-
Internet architecture consists of three layers –

1.Application layer
2.transfer control protocol
3.internet protocol

IP:-

In order to communicate, we need our data to be encapsulated as Internet Protocol (IP) packets. These IP packets travel across number of hosts in a network through routing to reach the destination. However IP does not support error detection and error recovery, and is incapable of detecting loss of packets.

TCP:-

TCP stands for "Transmission Control Protocol". It provides end to end transmission of data, i.e., from source to destination. It is a very complex protocol as it supports recovery of lost packets.

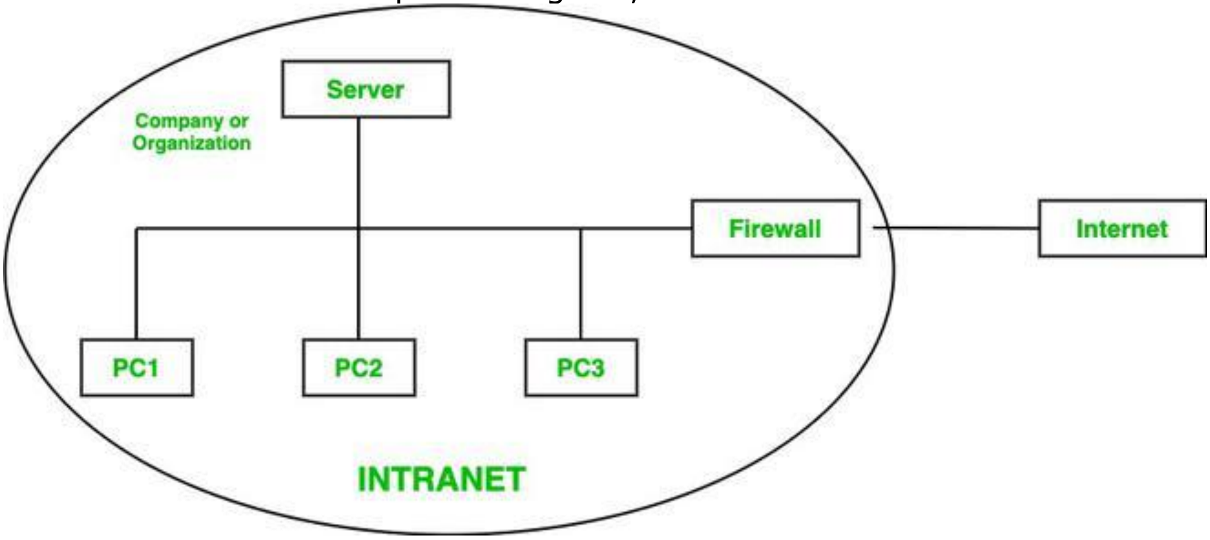
Application Protocol:-

Third layer in internet architecture is the application layer which has different protocols on which the internet services are built. Some of the examples of internet services include email (SMTP facilitates email feature), file transfer (FTP facilitates file transfer feature), etc.

8)Explain working of intranet and its architecture.
Ans :-

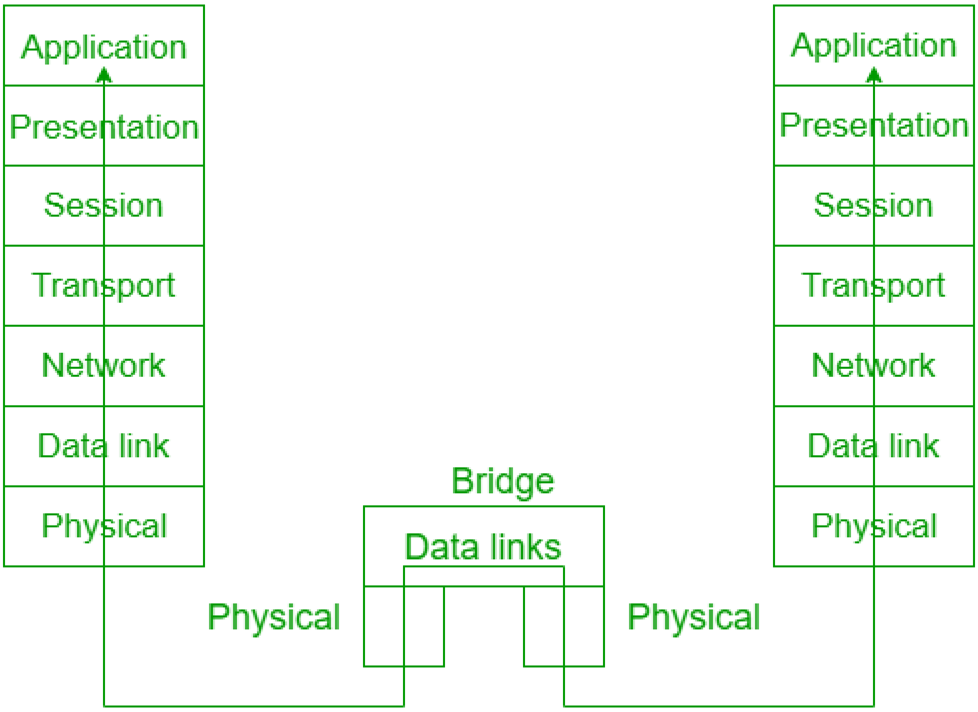
What is Intranet?
An intranet is a kind of private network. For example, an intranet is used by different organizations and only members/staff of that organization have access to this. It is a system in which multiple computers of an organization (or the computers you want to connect) are connected through an intranet. As this is a private network, so no one from the outside world can access this network. So many organizations and companies have their intranet network and only its members and staff have access to this network. This is also used to protect your data and provide data security to a particular organization, as it is a private network and does not leak data to the outside world.

Working of Intranet
An intranet is a network confined to a company, school, or organization that works like the Internet. Let us understand more about the working of the intranet with the help of a diagram, as shown below:



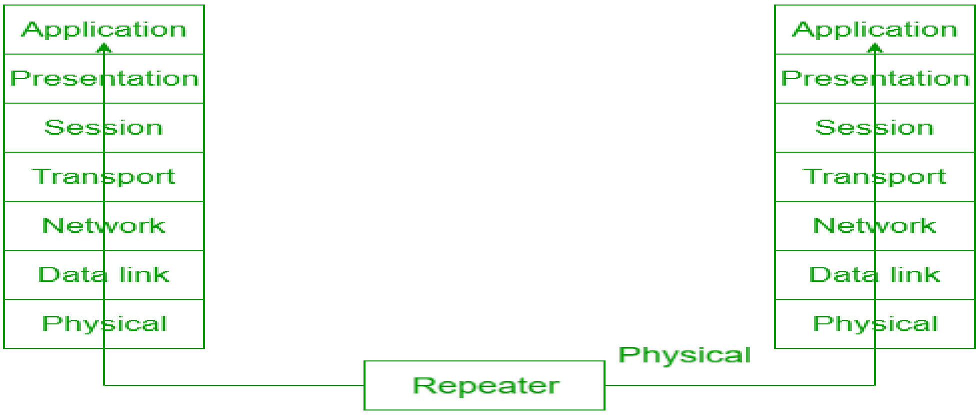
Here in this diagram, a company or an organization has created its private network or intranet for its work(intranet network is under the circle). The company or organization has many employees(in this diagram, we have considered 3). So, for their access, they have PC 1, PC 2, and PC 3(In the real world there are many employees as per the requirements of an organization). Also, they have their server for files or data to store, and to protect this private network, there is a Firewall. This firewall protects and gives security to the intranet server and its data from getting leaked to any unwanted user. So, a user who has access to the intranet can only access this network. So, no one from the outside world can access this network. Also, an intranet user can access the internet but a person using the internet cannot access the intranet network.

9)Write a short note on Repeater and Bridge.
Ans :-
Bridge: Bridge operates at the second layer i.e. data link layer of the ISO-OSI model. It connects the two networks together that uses the same protocol. Bridges are relatively easy to configure and focuses on MAC addresses.

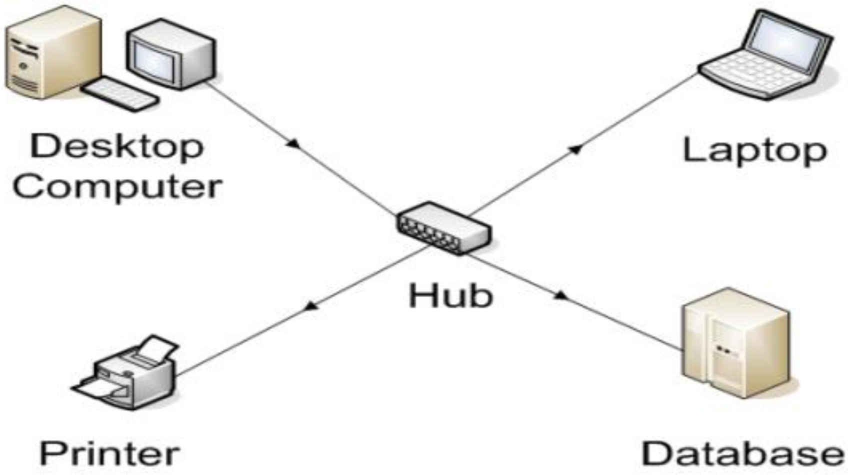


Bridge with OSI Layer

Repeater: Repeater is an electronic device. It is a hardware device used to extend a local area network. Repeater operates only on the physical layer i.e. first layer of the OSI model. It regenerates the weak signal and increases the range of the network. Functionality of the network remains unchanged by the use of repeater. Switch can be used as a repeater but hub cannot be used as a repeater.

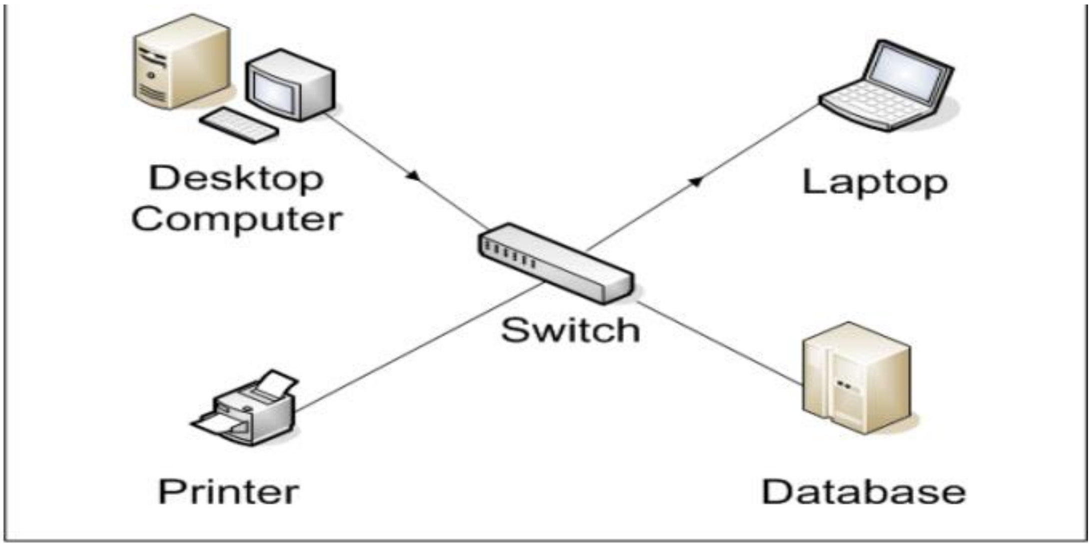


10)Write a short note on Switch and Hub.
Ans :-
1. Network Hub: The hub or network hub connects computers and devices and sends messages and data from any one device to all the others. If the desktop computer wants to send data to the laptop and it sends a message to the laptop through the hub, the message will get sent by the hub to all the computers and devices on the network. They need to do work to figure out that the message is not for them. Hub does not store any address of devices which are connected through it. Max 8 to 10 pc connected through hub However, because of its working mechanism, a hub is not so secure and safe. Moreover, copying the data on all the ports makes it slower and more congested which led to the use of network switch.



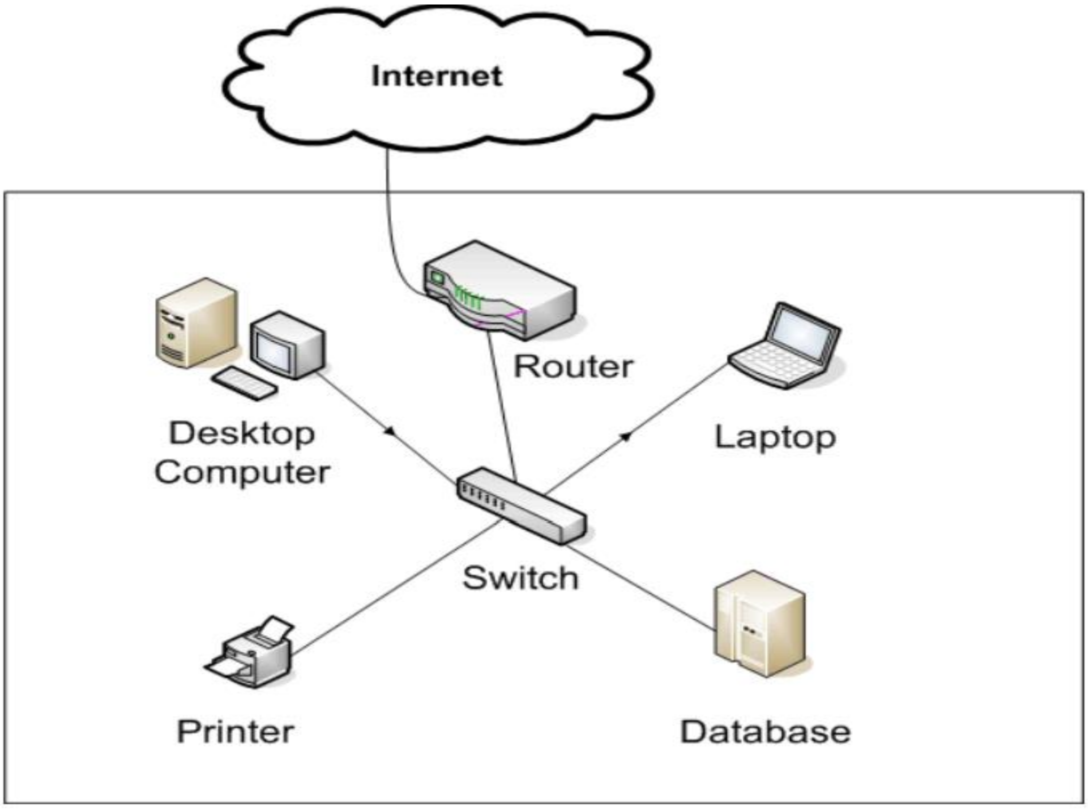
Network Switch:
Like a hub, a switch also works at the layer of LAN (Local Area Network) but you can say that a switch is more intelligent than a hub. While hub just does the work of data forwarding, a switch does 'filter and

forwarding' which is a more intelligent way of dealing with the data.
The switch connects the computer network components but it is smart about it. It knows the address of each item and so when the desktop computer wants to talk to tie laptop, it only sends the message to the laptop and nothing else.
Switch maintains a CAM (Content Addressable Memory) table and has its own system configuration and memory. CAM table is also called as forwarding table or forwarding information base (FIB).
In order to have a small home network that just connects the local equipment all that is really needed is a switch and network cable or the switch can transmit wireless information
Switch is a multiport bridge which can connect 48 ports.

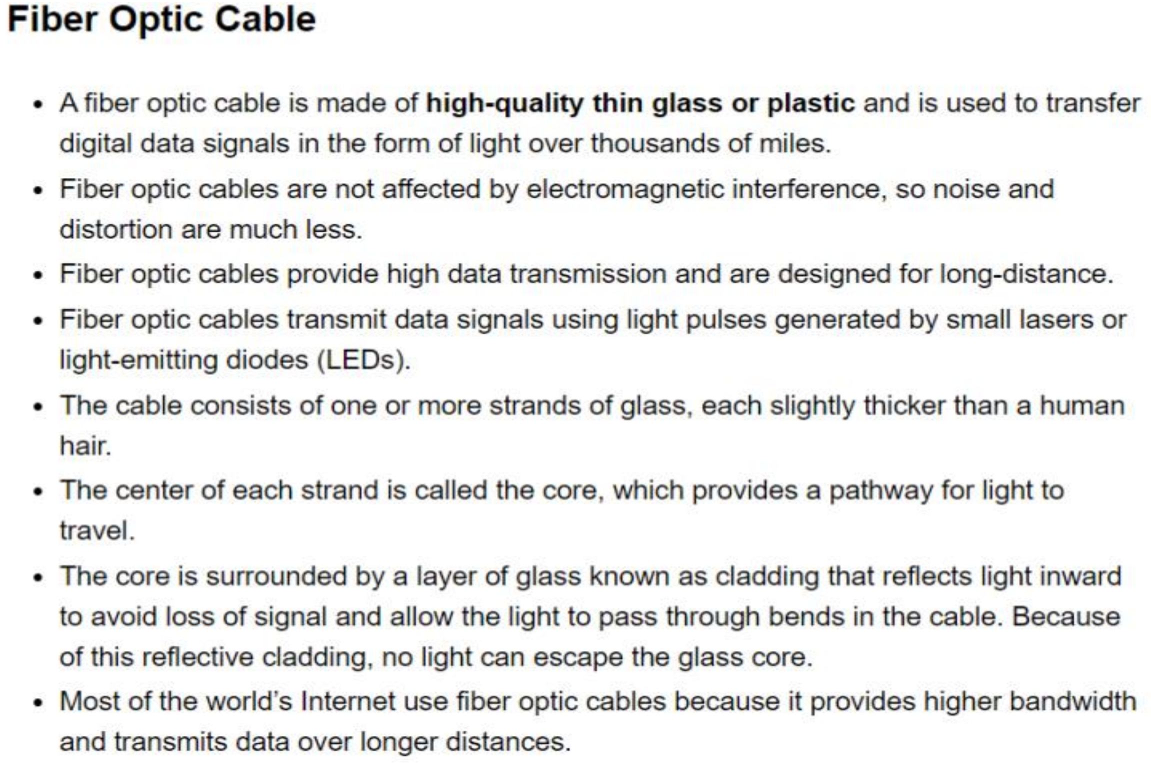


11) Explain Routers in detail.
Ans :-
A router is a network (internetworking) device which is responsible for routing traffic from one to another network.
These two networks could be a private company network to a public network.
You can think of a router as a traffic police who directs different network traffic to different directions.
A router is device that connects two networks. If you happened to have 2 LANs (local area networks) in your home or office and wanted to connect them, the router is the device that you would need.
The network that most home network connect to is the world’s biggest WAN (wide area network) the INTERNET
Router maintains Routing table.
Router cannot connect directly to pc first, pc connect through switch and switch connects to router
Router used in wan mostly because its costly but you can used it in LAN

too if you want. Router has 4 to 8 port

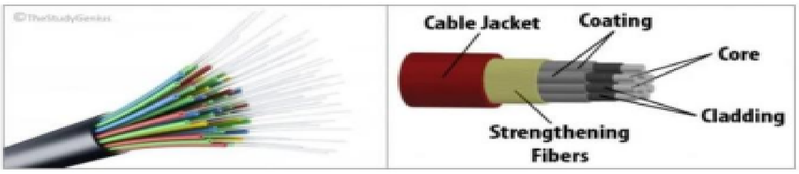


12) Explain Fiber optic cable in detail.
Ans :-

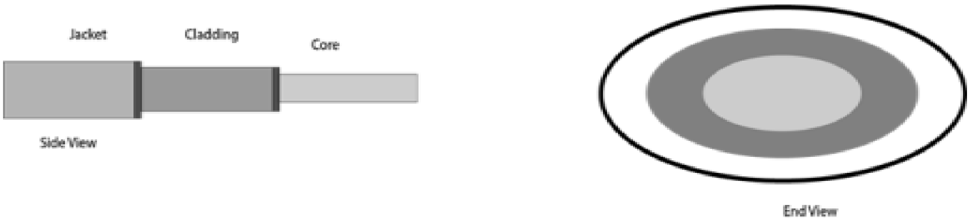


Fiber Optic Cable

- A fiber optic cable is made of **high-quality thin glass or plastic** and is used to transfer digital data signals in the form of light over thousands of miles.
- Fiber optic cables are not affected by electromagnetic interference, so noise and distortion are much less.
- Fiber optic cables provide high data transmission and are designed for long-distance.
- Fiber optic cables transmit data signals using light pulses generated by small lasers or light-emitting diodes (LEDs).
- The cable consists of one or more strands of glass, each slightly thicker than a human hair.
- The center of each strand is called the core, which provides a pathway for light to travel.
- The core is surrounded by a layer of glass known as cladding that reflects light inward to avoid loss of signal and allow the light to pass through bends in the cable. Because of this reflective cladding, no light can escape the glass core.
- Most of the world's Internet use fiber optic cables because it provides higher bandwidth and transmits data over longer distances.



Diagrammatic representation of fibre optic cable:



Advantages of Optical Fibre

Optical fibre is fast replacing copper wires because of these advantages that it offers –

- High bandwidth
- Immune to electromagnetic interference
- Suitable for industrial and noisy areas
- Signals carrying data can travel long distances without weakening

Disadvantages of Optical Fibre

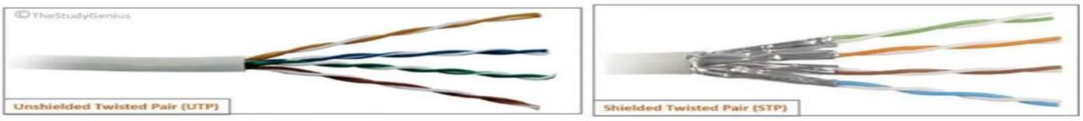
Despite long segment lengths and high bandwidth, using optical fibre may not be a viable option for every one due to these disadvantages –

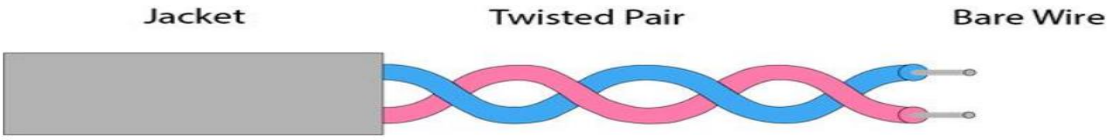
- Optical fibre cables are expensive
- Light waves are unidirectional, so two frequencies are required for full duplex transmission

13) Explain any two guided transmission Media with Advantages and Disadvantages.
Ans :-

Twisted Pair Cable

- Twisted-pair cabling is the most popular network cable for data transmission.
- It is lightweight, easy to install, inexpensive, and supports data speeds up to 100 Mbps.
- It is a pair of copper wires. Copper wires are the most common and widely used wire for transmitting signals due to their good performance at a low cost.
- A twisted pair cable consists of two conductors (normally copper), each pair of cables twisted together to form a single media with its own plastic insulation.
- Out of these two wires, one wire carries the actual signal and the other is used for ground reference.
- To identify each cable, these cables are color-coated.
- A twist between wires is helpful in reducing noise (electromagnetic interference) and crosstalk.
- This type of cable is mostly used to provide voice and data transmission in telephone networks.





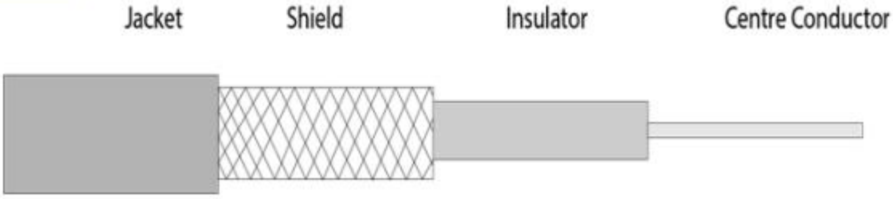
Coaxial Cable

- Coaxial cable has two wires of copper.
- The core/inner copper wire is in the center and is made of the solid conductor which is used for actual data transmission. It is enclosed in an insulating sheath.
- The second/external copper wire is wrapped around and used to protect against external electromagnetic interference (noise).
- This all is covered by plastic cover used to protect the inner layers from physical damage such as fire or water.

©TheStudyGenius

Coaxial cables are categorized by their Radio Government (RG) ratings. Each RG number denotes a unique set of physical specifications

Coaxial cable



Coaxial cable is of two types:

1. **Baseband transmission:** It is defined as the process of transmitting a single signal at high speed.
2. **Broadband transmission:** It is defined as the process of transmitting multiple signals simultaneously.

Advantages Of Coaxial cable:

- The data can be transmitted at high speed.
- It has better shielding as compared to twisted pair cable.
- It provides higher bandwidth.

Disadvantages Of Coaxial cable:

- It is more expensive as compared to twisted pair cable.
- If any fault occurs in the cable causes the failure in the entire network.

Common coaxial cable standards:

- **50-Ohm RG-7 or RG-11:** Used for thick Ethernet or “thicknet”.
- **50-Ohm RG-58:** Used for thin Ethernet, or “cheapernet”.
- **75-Ohm RG-59:** Used for cable television.
- **93-Ohm RG-62:** Used for ARCNET.

14) Explain any two unguided transmission Media with Advantages and Disadvantages.

Ans :-

Unguided Media:

It is also referred to as Wireless or Unbounded transmission media. No physical medium is required for the transmission of electromagnetic signals.

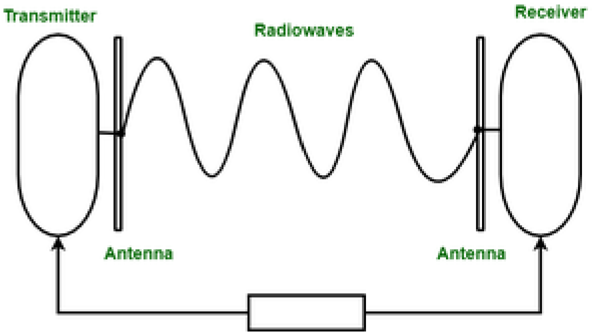
Features:

- The signal is broadcasted through air
- Less Secure
- Used for larger distances

There are 3 types of Signals transmitted through unguided media:

(i) Radio waves –

These are easy to generate and can penetrate through buildings. The sending and receiving antennas need not be aligned. Frequency Range:3KHz – 1GHz. AM and FM radios and cordless phones use Radio waves for transmission.



Further Categorized as (i) Terrestrial and (ii) Satellite.

(ii) Microwaves –

It is a line of sight transmission i.e. the sending and receiving antennas need to be properly aligned with each other. The distance covered by the signal is directly proportional to the height of the antenna. Frequency Range:1GHz – 300GHz. These are majorly used for mobile phone communication and television distribution.

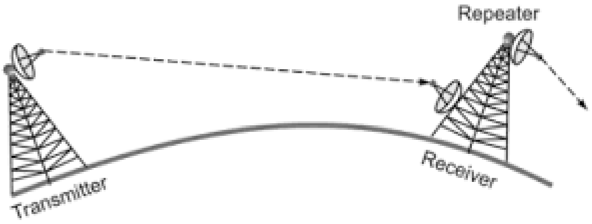


Fig: Microwave Transmission

15) What is MANET? Explain Smart phone Ad hoc Network in Detail.
Ans :-

- MANET stands for Mobile adhoc Network also called as wireless adhoc network or adhoc wireless network. They consist of a set of mobile nodes connected wirelessly in a self-configured, self-healing network without having a fixed infrastructure. MANET nodes are free to move randomly as the network topology changes frequently.

- Smart Phone Ad hoc Network (SPANC) –

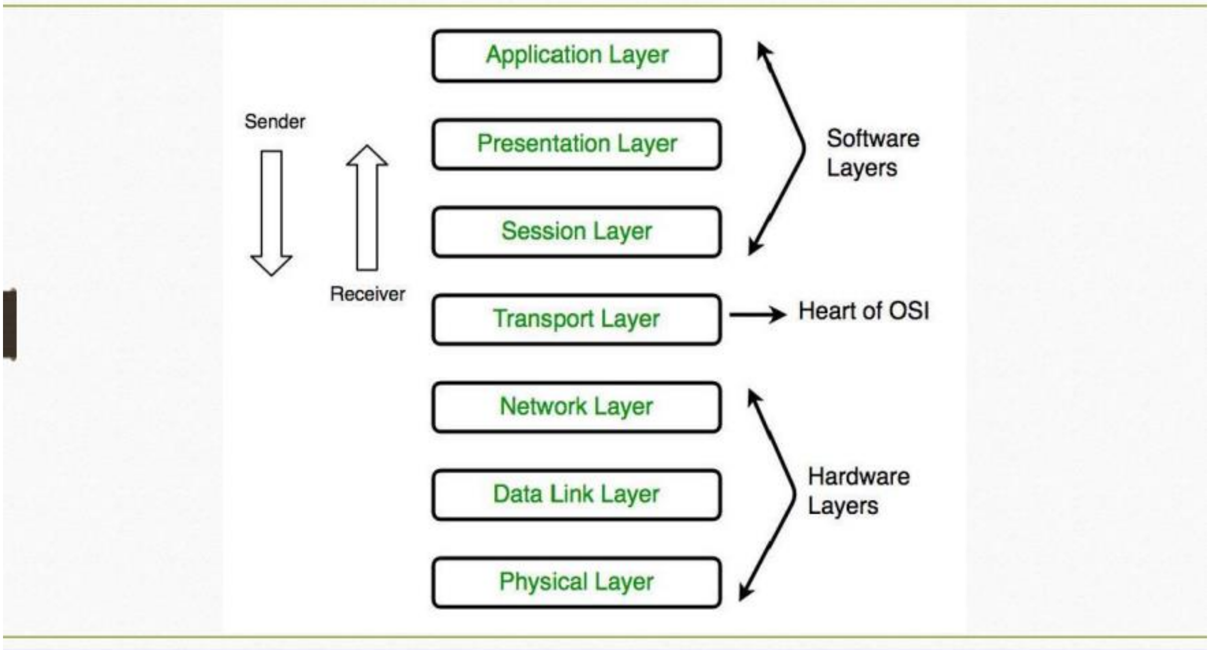
- To create peer-to-peer networks without relying on cellular carrier networks, wireless access points, or traditional network infrastructure. Here peers can join or leave the network without destroying it. ad-hoc network that utilizes smartphones as the primary nodes for communication. In SPANC, smartphones can act as both routers and hosts, creating a decentralized network without the need for a central infrastructure. This allows for increased flexibility and scalability in wireless communication, especially in emergency or disaster scenarios where traditional communication infrastructure may be unavailable. Some examples of SPANC applications include disaster response, search and rescue, and urban crowd management. Uses: Smart Phone Ad hoc Network (SPANC) can be used for a variety of applications, including:
- • Emergency communication: In the event of a natural disaster or other emergency, SPANCs can be used to establish a communication network quickly, allowing people to contact emergency services or stay in touch with loved ones.
- • Remote areas: SPANCs can be useful in remote areas where traditional wireless networks are not available, such as rural communities or wilderness areas.
- • Event networking: SPANCs can be used to create a temporary network for events or gatherings, allowing attendees to communicate and share information.
- • Military and emergency services: SPANCs can be used by military and emergency services to establish a quick and reliable communication network in the field.
- • Content sharing: SPANCs can be used to share various types of content such as pictures and videos, as well as other forms of multimedia.
- • Research and Development: SPANCs can be used in various research and development projects such as security, routing, and energy consumption.
- • Crowdsourcing: SPANCs can be used to gather data from a large group of people, such as in a survey or study.
- • Advertising and marketing: SPANCs can be used to deliver targeted advertising and marketing messages to a specific group of people.

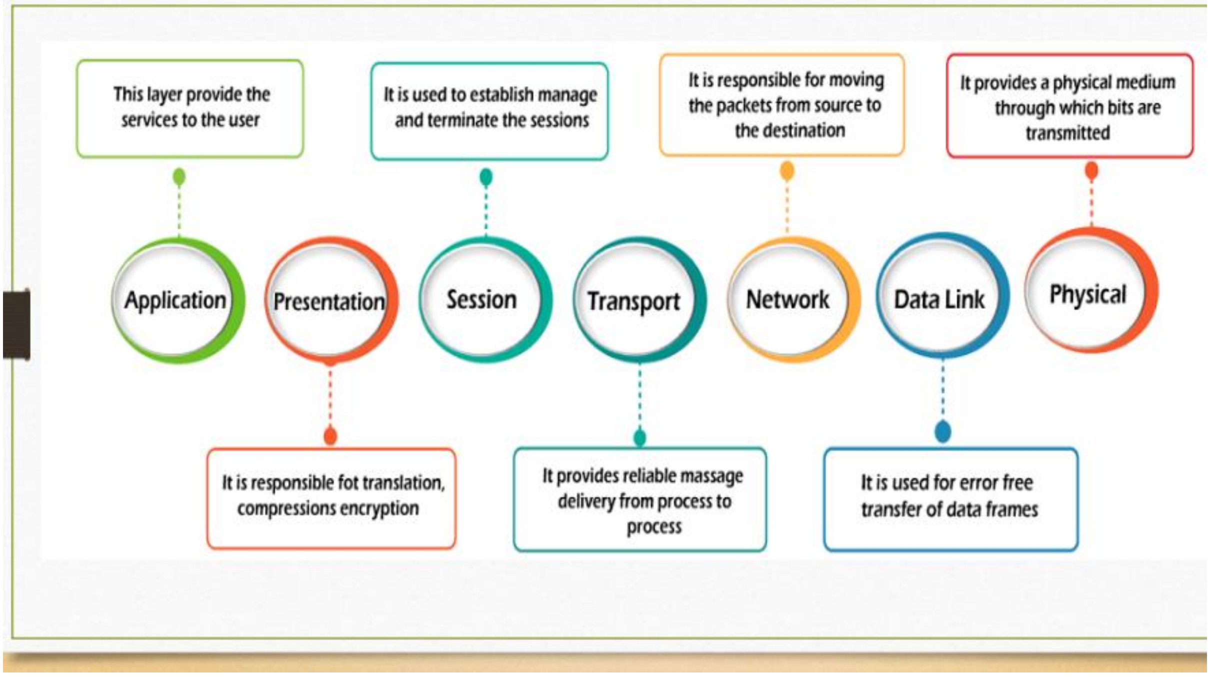
Advantages:
- Enables communication without relying on traditional network infrastructure or wireless access points.
- Provides a decentralized network without the need for a central infrastructure.
- Useful in emergency or disaster scenarios where traditional communication infrastructure may be unavailable.
- Can be used to establish a communication network quickly in the event of a natural disaster or other emergency.

Disadvantages:
- Limited coverage area, as SPANCs rely on the range of smartphone Wi-Fi capabilities.
- Requires a large number of smartphones to form an effective network.
- Vulnerable to attacks and security breaches

16) Discuss OSI model with functions of each layer
Ans :-

- OSI stands for Open System Interconnection 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 the International Organization for Standardization (ISO) in 1984, and it is now considered as an architectural model for the inter-computer communications.
- OSI model divides the whole task into seven smaller and manageable tasks. Each layer is assigned a particular task
- Each layer is self-contained, so that task assigned to each layer can be performed independently
- The OSI model is divided into two layers: upper layers and lower layers.
- The upper layer of the OSI model mainly deals with the application related issues, and they are implemented only in the software. The application layer is closest to the end user. Both the end user and the application layer interact with the software applications. An upper layer refers to the layer just above another layer.
- •The lower layer of the OSI model deals with the data transport issues. The data link layer and the physical layer are implemented in hardware and software. The physical layer is the lowest layer of the OSI model and is closest to the physical medium. The physical layer is mainly responsible for placing the information on the physical medium.




This layer provide the services to the user
It is used to establish manage and terminate the sessions
It is responsible for moving the packets from source to the destination
It provides a physical medium through which bits are transmitted
Application
Presentation
Session
Transport
Network
Data Link
Physical
It is responsible fot translation, compressions encryption
It provides reliable massage delivery from process to process
It is used for error free transfer of data frames

1. Physical Layer :-
    - Functions of a physical layer:-
        - Line Configuration: It defines the way how two or more devices can be connected physically
        - Data Transmission: It defines the transmission mode whether it is simplex, halfduplex or full-duplex mode between the two devices on the network.
        - Signals: It determines the type of the signal used for transmitting the information.

2. Data link layer :-

- Functions of data link layer :-
    - Framing: The data link layer translates the physical's raw bit stream into packets known as Frames. The Data link layer adds the header and trailer to the frame. The header which is added to the frame contains the hardware destination and source address.
    - Physical Addressing: The Data link layer adds a header to the frame that contains a destination address. The frame is transmitted to the destination address mentioned in the header.
    - Flow Control: Flow control is the main functionality of the Data-link layer. It is the technique through which the constant data rate is maintained on both the sides so that no data get corrupted. It ensures that the transmitting station such as a server with higher processing speed does not exceed the receiving station, with lower processing speed.
    - Error Control: Error control is achieved by adding a calculated value CRC (Cyclic Redundancy Check) that is placed to the Data link layer's trailer which is added to the message frame before it is sent to the physical layer. If any error seems to occur, then the receiver sends the acknowledgment for the retransmission of the corrupted frames.
    - Access Control: When two or more devices are connected to the same communication channel, then the data link layer protocols are used to determine which device has control over the link at a given time.

3. Network Layer :-

- Functions of Network Layer :-
    - Internetworking: An internetworking is the main responsibility of the network layer. It provides a logical connection between different devices.
    - Addressing: A Network layer adds the source and destination address to the header of the frame. Addressing is used to identify the device on the internet.
    - Routing: Routing is the major component of the network layer, and it determines the best optimal path out of the multiple paths from source to the destination.
    - Packetizing: A Network Layer receives the packets from the upper layer and converts them into packets. This process is known as Packetizing. It is achieved by internet protocol (IP).

4. Transport layer :-

- Functions of transport layer :-
    - Service-point addressing: Computers run several programs simultaneously due to this reason, the transmission of data from source to the destination not only from one computer to another computer but also from one process to another process. The transport layer adds the header that contains the address known as a service-point address or port address. The responsibility of the network layer is to transmit the data from one computer to another computer and the responsibility of the transport layer is to transmit the message to the correct process.

    - Segmentation and reassembly: When the transport layer receives the message from the upper layer, it divides the message into multiple segments, and each segment is assigned with a sequence number that uniquely identifies each segment. When the message has arrived at the destination, then the transport layer reassembles the message based on their sequence numbers.

    - Connection control: Transport layer provides two services Connection-oriented service and connectionless service. A connectionless service treats each segment as an individual packet, and they all travel in different routes to reach the destination. A connection-oriented service makes a connection with the transport layer at the destination machine before delivering the packets. In connection-oriented service, all the packets travel in the single route.

    - Flow control: The transport layer also responsible for flow control but it is performed end-toend rather than across a single link.

    - Error control: The transport layer is also responsible for Error control. Error control is performed end-to-end rather than across the single link. The sender transport layer ensures that message reach at the destination without any error.

5. Session layer :-

- Functions of session layer :-
    - Dialog control: Session layer acts as a dialog controller that creates a dialog between two processes or we can say that it allows the communication between two processes which can be either half-duplex or full-duplex.
    - Synchronization: Session layer adds some checkpoints when transmitting the data in a sequence. If some error occurs in the middle of the transmission of data, then the transmission will take place again from the checkpoint. This process is known as Synchronization and recovery

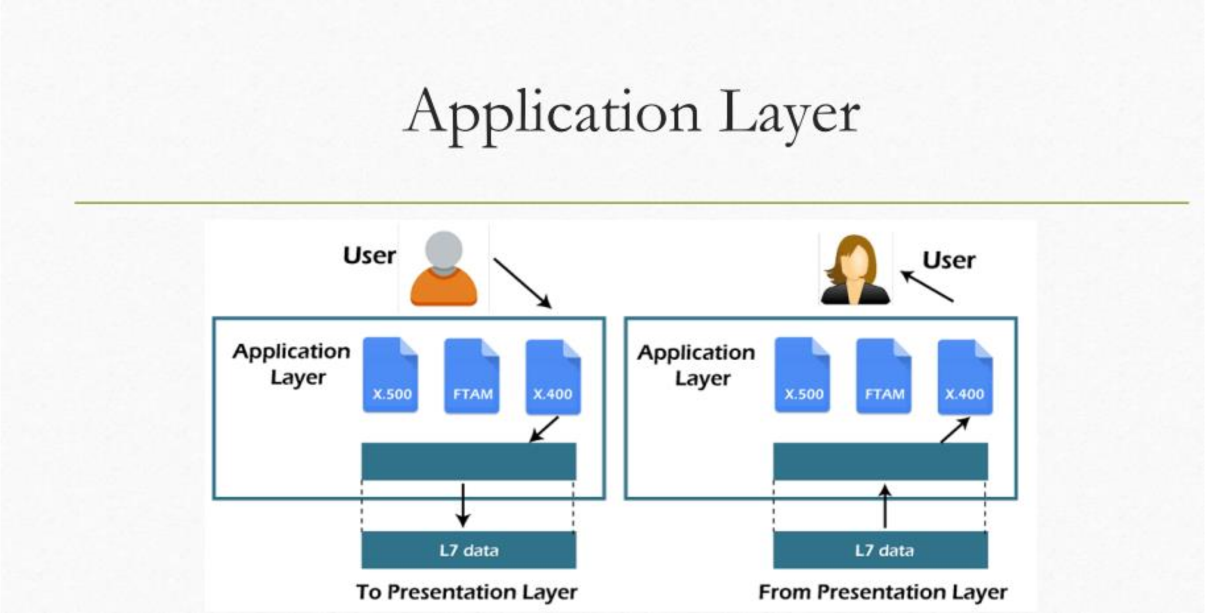
6. Presentation layer :-

- Functions of presentation layer :-
    - Translation: The processes in two systems exchange the information in the form of character strings, numbers and so on. Different computers use different encoding methods, the presentation layer handles the interoperability between the different encoding methods. It converts the data from sender-dependent format into a common format and changes the common format into receiver-dependent format at the receiving end.
    - Encryption: Encryption is needed to maintain privacy. Encryption is a process of converting the sender-transmitted information into another form and sends the resulting message over the network.
    - Compression: Data compression is a process of compressing the data, i.e., it reduces the number of bits to be transmitted. Data compression is very important in multimedia such as text, audio, video.

7. Application layer :-

- Functions of application layer :-
    - File transfer, access, and management (FTAM): An application layer 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: An application layer provides the facility for email forwarding and storage.
    - Directory services: An application provides the distributed database sources and is used to provide that global information about various objects.

17) Write a short note on Application Layer.
Ans :-



- An application layer serves as a window for users and application processes to access network service.
- It handles issues such as network transparency, resource allocation, etc.
- An application layer is not an application, but it performs the application layer functions.
- This layer provides the network services to the end-users. Application Layer is also called as Desktop Layer.
- Ex: Application – Browsers, Skype Messenger etc.

- Functions of application layer :-
  - File transfer, access, and management (FTAM): An application layer 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: An application layer provides the facility for email forwarding and storage.
  - Directory services: An application provides the distributed database sources and is used to provide that global information about various objects.

- Application Layer Protocols
  - The application layer provides several protocols which allow any software to easily send and receive information and present meaningful data to its users. The following are some of the protocols which are

provided by the application layer.

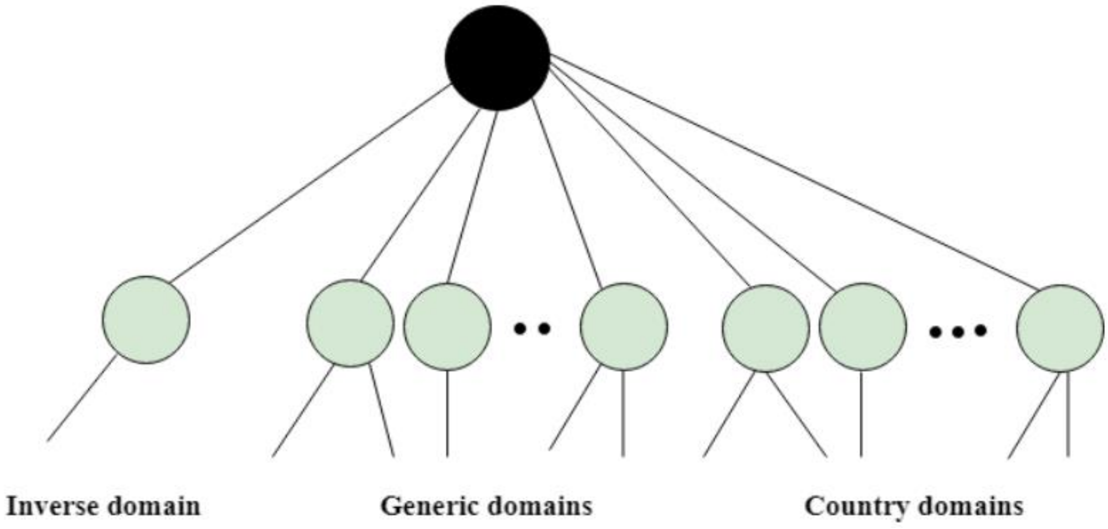
- TELNET: Telnet stands for Telecommunications Network. This protocol is used for managing files over the Internet. It allows the Telnet clients to access the resources of Telnet server. Telnet uses port number 23.
- DNS: DNS stands for Domain Name System. The DNS service translates the domain name (selected by user) into the corresponding IP address. For example- If you choose the domain name as www.flipcart.com, then DNS must translate it as 192.36.20.8 (random IP address written just for understanding purposes). DNS protocol uses the port number 53.
- DHCP: DHCP stands for Dynamic Host Configuration Protocol. It provides IP addresses to hosts. Whenever a host tries to register for an IP address with the DHCP server, DHCP server provides lots of information to the corresponding host. DHCP uses port numbers 67 and 68.
- FTP: FTP stands for File Transfer Protocol. This protocol helps to transfer different files from one device to another. FTP promotes sharing of files via remote computer devices with reliable, efficient data transfer. FTP uses port number 20 for data access and port number 21 for data control.
- SMTP: SMTP stands for Simple Mail Transfer Protocol. It is used to transfer electronic mail from one user to another user. SMTP is used by end users to send emails with ease. SMTP uses port numbers 25 and 587.
- HTTP: HTTP stands for Hyper Text Transfer Protocol. It is the foundation of the World Wide Web (WWW). HTTP works on the client server model. This protocol is used for transmitting hypermedia documents like HTML. This protocol was designed particularly for the communications between the web browsers and web servers, but this protocol can also be used for several other purposes. HTTP is a stateless protocol (network protocol in which a client sends requests to server and server responses back as per the given state), which means the server is not responsible for maintaining the previous client’s requests. HTTP uses port number 80.
- NFS: NFS stands for Network File System. This protocol allows remote hosts to mount files over a network and interact with those file systems as though they are mounted locally. NFS uses the port number 2049.
- SNMP: SNMP stands for Simple Network Management Protocol. This protocol gathers data by polling the devices from the network to the management station at

fixed or random intervals, requiring them to disclose certain information. SNMP uses port numbers 161 (TCP) and 162 (UDP).

18) Write a short note on DNS
Ans :-
❖DNS
An application layer protocol defines how the application processes running on different systems pass the messages to each other.

- DNS stands for Domain Name System.
- DNS is a directory service that provides a mapping between the name of a host on the network and its numerical address.
- DNS is required for the functioning of the internet.
- Each node in a tree has a domain name, and a full domain name is a sequence of symbols specified by dots.
- DNS is a service that translates the domain name into IP addresses. This allows the users of networks to utilize user-friendly names when looking for other hosts instead of remembering the IP addresses.
- For example, suppose the FTP site at EduSoft had an IP address of 132.147.165.50, most people would reach this site by specifying ftp.EduSoft.com. Therefore, the domain name is more reliable than the IP address

➔ DNS is a TCP/IP protocol used on different platforms. The domain name space is divided into three different sections: generic domains, country domains, and inverse domain



❖ Working of DNS

- DNS is a client/server network communication protocol. DNS clients send requestsT to the. server while DNS servers send responses to the client.
- Client requests contain a name which is converted into an IP address known as a forward DNS lookups while requests containing an IP address which is converted into a name known as reverse DNS lookups.
- DNS implements a distributed database to store the name of all the hosts available on the internet.
- If a client like a web browser sends a request containing a hostname, then a piece of software such as DNS resolver sends a request to the DNS server to obtain the IP address of a hostname. If DNS server does not contain the IP address associated with a hostname, then it forwards the request to another DNS server. If IP address has arrived at the resolver, which in turn completes the request over the internet protocol

19) Write a short note on SSL.
Ans :-
Secure Socket Layer(SSL):-

- Secure Socket Layer (SSL) provides security to the data that is transferred between web browser and server.
- SSL encrypts the link between a web server and a browser which ensures that all data passed between them remain private and free from attack.
- The Secure Sockets Layer (SSL) protocol was developed by Netscape Communications Corporation.

20) Explain IP Subnetting in detail.
Ans :-

21) Difference between http and https
Ans :-
★ Difference Between HTTP and HTTPS

- HTTP stands for HyperText Transfer Protocol and HTTPS stands for HyperText Transfer Protocol Secure.
- In HTTP, URL begins with “http://” whereas URL starts with “https://”
- HTTP uses port number 80 for communication and HTTPS uses 443
- HTTP is considered to be insecure and HTTPS is secure
- HTTP Works at Application Layer and HTTPS works at Transport Layer
- In HTTP, Encryption is absent and Encryption is present in HTTPS as discussed above

- HTTP does not require any certificates and HTTPS needs SSL Certificates
- HTTP speed is faster than HTTPS and HTTPS speed is slower than HTTP
- HTTP does not improve search ranking while HTTPS improves search ranking.
- HTTP does not use data hashtags to secure data, while HTTPS will have the data before sending it and return it to its original state on the receiver side.
- The S in HTTPS stands for "secure."
- HTTPS uses TLS or SSL to encrypt HTTP requests and responses. So basically, the only difference between the two protocols is that HTTPS uses TLS (SSL) to encrypt normal HTTP requests and responses.
- As a result, HTTPS is far more secure than HTTP. Because of that HTTPS can protect against eavesdropping and man-in-the-middle (MitM) attacks. A website that uses HTTP has "http://" in its URL, while a website that uses HTTPS has "https://"

22) Differentiate TCP and UDP.
Ans :-

- Transmission Control Protocol
  - ○ It is a standard protocol that allows the systems to communicate over the internet.
  - ○ It establishes and maintains a connection between hosts.
  - ○ When data is sent over the TCP connection, then the TCP protocol divides the data into smaller units known as segments. Each segment travels over the internet using multiple routes, and they arrive in different orders at the destination. The transmission control protocol reorders the packets in the correct order at the receiving end.9
- User Datagram Protocol
  - ○ User Datagram Protocol is a transport layer protocol.
  - ○ It is an unreliable transport protocol as in this case the receiver does not send any acknowledgment when the packet is received, the sender does not wait for any acknowledgment. Therefore, this makes a protocol unreliable.

23) Explain Search Engine in detail.
Ans :-
Search Engine:

A search engine is a service that allows Internet users to search for content via the World Wide Web (WWW). Search Engine refers to a huge database of internet resources such as web pages, newsgroups, programs, images etc. It helps to locate information on World Wide Web. A user enters keywords or key phrases into a search engine and receives a list of Web content results in the form of websites, images, videos or other online data that semantically match with the search query.

Search Engine Components:

Generally there are three basic components of a search engine as listed below:

1. Web Crawler
2. Database
3. Search Interfaces
4. Ranking algorithm

1.Web crawler:-

Crawling is the first stage in which a search engine uses web crawlers to find, visit, and download the web pages on the WWW (World Wide Web). Crawling is performed by software robots, known as "spiders" or "crawlers." So, Web Crawler is also known as a search engine bot, web robot, or web spider. These robots are used to review the website content. In short, it is a software component that traverses the web to gather information.

2.Database

All the information on the web is stored in database. It consists of huge web resources.

3.Search Interfaces

This component is an interface between user and the database. It helps the user to search through the database.

4.Ranking Algorithms

The ranking is the last stage of the search engine. It is used to provide a piece of content that will be the best answer based on the user's query. It displays the best content at the top rank of the website. The ranking algorithm is used by Google to rank web pages according to the Google search algorithm. There are the following ranking features that affect the search results –

- Location and frequency
- Link Analysis
- Click through measurement

-How do search engines work

Web crawler, database and the search interface are the major component of a search engine that actually makes search engine to work. Search engines make use of Boolean expression AND, OR, NOT to restrict and widen the results of a search.

Following are the steps that are performed by the search engine:

- The search engine looks for the keyword in the index for predefined database instead of going directly to the web to search for the keyword. Indexing is an online library of websites, which is used to sort, store, and organize the content that we found during the crawling. Once a page is indexed, it appears as a result of the most valuable and most relevant query.

- It then uses software to search for the information in the database. This software component is known as web crawler.
- Once web crawler finds the pages, the search engine then shows the relevant web pages as a result. These retrieved web pages generally include title of page, size of text portion, first several sentences etc.
- These search criteria may vary from one search engine to the other. The retrieved information is ranked according to various factors such as frequency of keywords, relevancy of information, links etc.
- User can click on any of the search results to open it.

24) Write a Case study on E-mail from sender to receiver with their functionality and use of different protocol.
Ans :-

25) Explain URL and types of URL in detail.
Ans :-

URL stands for Uniform Resource Locator. Any internet location available on server is called a web URL, web address or website. Each website or webpage has a unique address called URL.
A URL (Uniform Resource Locator) contains the information, which is as follows:

- The port number on the server, which is optional.
- It contains a protocol that is used to access the resource.
- The location of the server
- A fragment identifier
- In the directory structure of the server, it contains the location of the resource.

For e.g., the website of mywork website has an address or URL called https://www.mywork.org/
type://address/path -> basic structure of url

type: It specifies the type of the server in which the file is located.
address: It specifies the address or location of the internet server. path: It specifies the location of the file on the internet server.

Types of URL: URL gives the address of files created for webpages or other documents like an image, pdf for a doc file, etc.
There are two types of URL:
1. Absolute URL
2. Relative URL

1.Absolute URL:

This type of URL contains both the domain name and directory/page path. An absolute URL gives complete location information. It begins with a protocol like “http://” and continues, including every detail. An absolute URL typically comes with the following syntax.
protocol://domain/path

For web browsing, absolute URL’s are types in the address bar of a web browser. For example, if it is related to our project page link of “mywork” website, the URL should be mentioned as https://www.mywork.org/computer-science-projects/ This gives the complete information about the file location path.

Note: The protocol may be of following types. http://, https://, ftp://, gopher://, etc.

2.Relative URL:

This type of URL contains the path excluding the domain name. Relative means “in relation to”, and a relative URL tells a URL location on terms of the current location. Relative path is used for reference to a given link of a file that exist within the same domain. Let us assume a web developer setting up a webpage and want to link an image called “mywork.jpg”.

```
<img src="mywork.jpg">
```

It would internally be interpreted like the following.

```
<img src="./mywork.jpg">
```

The dot(.) before the “/” in the src attribute is a “special character”. It means the location should be started from the current directory to find the file location.