SHORT QUESTIONS :

1. What are components of Network?

➢ **Components of a computer network**

Following are some of the important components of a computer network.

1. Two or more computers.
2. Cables (coaxial, twisted pair or fiber optic) as links between the computers.
3. A network interfacing card on each computer and switches.
4. A software called network operating system.

2. Define multicast and broadcast.

➢ **Broadcast::**

Broadcast transfer (one-to-all) techniques and can be classified into two types : Limited Broadcasting, Direct Broadcasting. In broadcasting mode, transmission happens from one host to all the other hosts connected on the LAN. The devices such as bridge uses this. The protocol like ARP implement this, in order to know MAC address for the corresponding IP address of the host machine. ARP does ip address to mac address translation. RARP does the reverse.

Multicast:

Multicasting has one/more senders and one/more recipients participate in data transfer traffic. In multicasting traffic recline between the boundaries of unicast and broadcast. It server's direct single copies of data streams and that are then simulated and routed to hosts that request it. IP multicast requires support of some other protocols such as IGMP (Internet Group Management Protocol), Multicast routing for its working. And also in Classful IP addressing Class D is reserved for multicast groups.

3. Define Intranet.

➢

- It is a worldwide/global system of interconnected computer networks. It uses the standard Internet Protocol (TCP/IP). Every computer in Internet is identified by a unique IP address. IP Address is a unique set of numbers (such as 110.22.33.114) which identifies a computer's location.
- A special computer DNS (Domain Name Server) is used to provide a name to the IP Address so that the user can locate a computer by a name.

4. **Define Internet** .

➢

- Intranet is the system in which multiple PCs are connected to each other. PCs in intranet are not available to the world outside the intranet. Usually each organization has its own Intranet network and members/employees of that organization can access the computers in their intranet

- Each computer in Intranet is also identified by an IP Address which is unique among the computers in that Intranet

5. What is Active and Passive Hub?

- **Active Hub**:- These are the hubs that have their own power supply and can clean, boost, and relay the signal along with the network. It serves both as a repeater as well as a wiring center. These are used to extend the maximum distance between nodes.

  Passive Hub :- These are the hubs that collect wiring from nodes and power supply from the active hub.
  These hubs relay signals onto the network without cleaning and boosting them and can't be used to extend the distance between nodes.

6. Define Gateways.

- A gateway is an internetworking capable of joining together two networks that use different base protocols.
  A network gateway can be implemented completely in software, hardware, or a combination of both,
  depending on the types of protocols they support.
  A network gateway can operate at any level of the OSI model. A broadband router typically serves as the
  network gateway, although ordinary computers can also be configured to perform equivalent functions.
  A gateway is a router or proxy server that routes between networks.
  A gateway belongs to the same subnet to which the PC belongs.

7. What is Access Point?

- While an access point (AP) can technically involve either a wired or wireless connection, it commonly means a wireless device. An AP works at the second OSI layer, the Data Link layer, and it can operate either as a bridge connecting a standard wired network to wireless devices or as a router passing data transmissions from one access point to another.
  - Wireless access points (WAPs) consist of a transmitter and receiver (transceiver) device used to create a wireless LAN (WLAN). Access points typically are separate network devices with a built-in antenna,transmitter and adapter.
  - APs use the wireless infrastructure network mode to provide a connection point between WLANs and a wired Ethernet LAN. They also have several ports, giving you a way to expand the network to support additional clients. Depending on the size of the network, one or more APs might be required to provide full coverage. Additional APs are used to allow access to more wireless clients and to expand the range of the wireless network.

- Each AP is limited by its transmission range — the distance a client can be from an AP and still obtain a usable signal and data process speed.
- The actual distance depends on the wireless standard, the obstructions and environmental conditions between the client and the AP.
- Higher end APs have high-powered antennas, enabling them to extend how far the wireless signal can travel.

8. What is Router?

➢ Routers are small physical devices that operate at the network layer to join multiple networks together.

- A router is a device like a switch that routes data packets based on their IP addresses.
- Routers normally connect LANs and WANs and have a dynamically updating routing table based on

which they make decisions on routing the data packets.

- A Router divides the broadcast domains of hosts connected through it.
- Routers perform the traffic directing functions on the Internet. A data packet is typically forwarded from one router to another through the networks that constitute the internetwork until it reaches its destination code.
- Routers may also be used to connect two or more logical groups of computer devices known as subnets, each with a different sub network address. The subnet addresses recorded in a router do not necessarily map directly to the physical interface connections.

Two types of routers –

- Static routers – Static routers are configured manually and route data packets based on the information in a router table.
- Dynamic routers – Dynamic routers use adaptive routing which is a process where a router can forward data by a different route.

9. What is MODEM?

➢ Modems (modulators-demodulators) are used to transmit digital signals over analog telephone lines.

- Thus, digital signals are converted by the modem into analog signals of different frequencies and transmitted to a modem at the receiving location.
- The receiving modem performs the reverse transformation and provides a digital output to a device connected to a modem, usually a computer.
- The digital data is usually transferred to or from the modem over a serial line through an industry standard interface, RS-232.
- Many telephone companies offer DSL services, and many cable operators use modems as end terminals for identification and recognition of home and personal users.
- Modems work on both the Physical and Data Link layers.

10. What is topology? Define the types of topologies

- **Topology** :- The arrangement of a network which comprises of nodes and connecting lines via sender 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

- Network topology is the way a network is arranged, including the physical or logical description of how links and nodes are set up to relate to eachother. There are numerous ways a network can be arranged, all with different pros and cons, and some are more useful in certain circumstances than others.
  Adminshave a range of options when it comes to choosing a network topology, and thisdecision must account for the size and scale of their business, its goals, andbudget.
  Several tasks go into effective network topology management, includingconfiguration management, visual mapping, and general performancemonitoring.
  The key is to understand your objectives and requirements to create and manage the network topology in the right way for your business.

12) Define Baud rate.

- Baud rate is the rate at which the number of signal elements or changes to the signal occurs per second when it passes through a transmission medium.

13) Define Nyquist bit rate.

- 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.

- Client:
  - A client is a device or software application that initiates requests for services, resources, or information from a server.
  - Clients can be personal computers, smartphones, tablets, IoT devices, or any device capable of connecting to a network.
  - Client devices use software programs (often called "client software") to communicate with servers.

- Clients send requests to servers, such as web browsers requesting web pages from web servers, email clients retrieving emails from mail servers, or gaming clients connecting to game servers.

➢ Server:

- A server is a powerful computer or software application designed to provide services, resources, or information to clients over a network.
- Servers are typically optimized for high availability, reliability, and performance.
- Different types of servers serve various purposes, including web servers (for hosting websites), mail servers (for handling emails), file servers (for file storage and sharing), and database servers (for managing data).
- Servers listen for incoming client requests, process those requests, and send back responses accordingly.

15) Define HTTP and HTTPS.

➢

➢ HTTP (Hypertext Transfer Protocol):

- HTTP is the foundation of data communication on the World Wide Web.
- It is an application layer protocol that facilitates the exchange of text, images, videos, and other multimedia content between a web server and a web browser or client.
- HTTP operates over TCP/IP (Transmission Control Protocol/Internet Protocol) and uses a request-response model.
- It is stateless, meaning each request-response cycle is independent and does not retain information from previous interactions.
- Data transmitted via plain HTTP is not encrypted, making it susceptible to interception or eavesdropping.

- HTTPS (Hypertext Transfer Protocol Secure):
  - HTTPS is an extension of HTTP that adds a layer of security to data transmission over the internet.
  - It uses a combination of HTTP and the SSL/TLS (Secure Sockets Layer/Transport Layer Security) protocols to encrypt data exchanged between the client and the server.
  - The encryption ensures that data remains confidential and cannot be easily intercepted or tampered with by malicious actors.
  - To enable HTTPS, a website needs an SSL/TLS certificate, which is issued by a trusted Certificate Authority (CA). This certificate verifies the authenticity of the website, providing assurance to users that they are connecting to the intended server.

16) Define Telnet and FTP.

➢ **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?

➢

1. Unshielded Twisted Pair (UTP):

This type of cable has the ability to block interference and does not depend on a physical shield for this purpose. It is used for telephonic applications.

Advantages:

- Least expensive
- Easy to install
- High speed capacity
- Susceptible to external interference
- Lower capacity and performance in comparison to STP
- Short distance transmission due to attenuation

2. Shielded Twisted Pair (STP):

This type of cable consists of a special jacket to block external interference. It is used in fast-data-rate Ethernet and in voice and data channels of telephone lines.

Advantages:

- Better performance at a higher data rate in comparison to UTP
- Eliminates crosstalk
- Comparitively faster
- Comparitively difficult to install and manufacture
- More expensive

- Bulky

18) What is Co-axial?

➢

- 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?

➢ 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.

➢ **UDP :-**

- UDP stands for User Datagram Protocol.
- UDP is a simple protocol and it provides non sequenced transport functionality. o UDP is a connectionless protocol.
- This type of protocol is used when reliability and security are less important than speed and size.
- 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.
- The packet produced by the UDP protocol is known as a user datagram

TCP :-

- TCP stands for Transmission Control Protocol.
- It provides full transport layer services to applications.
- 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?

➢ 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?

- 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?

- 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?

- 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?

- 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?

- **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?

- **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?

- **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?

- 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.

- HTTP (hypertext transfer), ICMP, IP, IPX, UDP, and TIPC.

31) List out the connection oriented protocol.

- telnet, rlogin, and ftp.

32) Give the full form of SMTP, DNS and POP with their port number.

- 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.

- 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?

-
  - 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?

- Presentation layer

36) What is the purpose of Presentation layer?

- 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?

- **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?

- **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?

-
    - Segmentation and reassembly of data.
    - End-to-end communication establishment and termination.
    - Port addressing for directing data to specific applications.
    - Multiplexing and demultiplexing of data streams.
    - Flow control to prevent congestion and ensure efficient data transfer.
    - Error detection and, in some cases, correction.
    - Reliability through acknowledgment and retransmission of data.
    - Support for both connection-oriented (e.g., TCP) and connectionless (e.g., UDP) communication.
    - Congestion control to manage network traffic.
    - Quality of Service (QoS) prioritization for critical data.
    - Ensuring data reaches the correct destination on the network.

40) Which protocols are used in Application Layer?

- 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?

- 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 withouthaving 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.

- 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.

- **The transmission modes are of three major types:**
  - Simplex Transmission Mode.
  - Half Duplex Transmission Mode.
  - Full Duplex Transmission Mode.

44) What is Absolute URL?

- 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?

- 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. What is computer Network? Explain Advantages & Disadvantages of computer network.

- A network consists of two or more computers that are linked in order to share resources (such as printers and CDs), exchange files, or allow electronic communications. The computers on a network may be linked through cables, telephone lines, radio waves, satellites, or infrared light beams.
- A **computer network** is a set of connected computers. Computers on a network are called **nodes**. The connection between computers can be done via cabling. Connected computers can share resources, like access to the Internet, printers, file servers. A network is a multipurpose connection, which allows a single computer to do more.

Advantages of computer network

1. Increased speed.

- Network provides a very fast means for sharing and transfer of files.
- If the computer networks would not have been there, then we would have to copy the files on floppy discs and send them to the other computers.

2. Reduced cost.

- Many popular versions of networkable software are now available at a considerably reduced costs as compared to individual licensed copies.
- In addition to this it is also possible to share a program on a network. It is also possible to upgrade the program

3. Improved security.

- It is possible to produce to protect the programs and files from illegal copying.
- By allotting password the access can be restricted to authorized users only.

4. Centralized software managements.

- Due to the use of computer networks, all the software can be loaded on one computer.
- All the other computers can make use of this centralized software. It is not necessary to waste time and energy in installing updates and tracking files on independent computers.

5. Electronic – mail.

- The computer network makes the hardware available which is necessary to install an e-mail system.
- The person to person communication is improved due to a presence of e-mail system.

6. Flexible access.

• It is possible for the authorized users to access their files from any computer connected on the network. This provides tremendous flexibility in accessing.

<u>Disadvantages of network</u>

1. High cost of installation

- use of a computer network is high. This is due to the cost of cables, network cards, computer, printers and various software that are required to be installed.

- The cost of services of technicians may also get added.

2. Requires time for administration

- Computer networks need proper and careful administration and maintenance. This is a time consuming job.

3. Failure of server

- If the file servers “goes down” then the entire network comes to a standstill.
- If this happens then the entire organization can lose access to the necessary program and files.

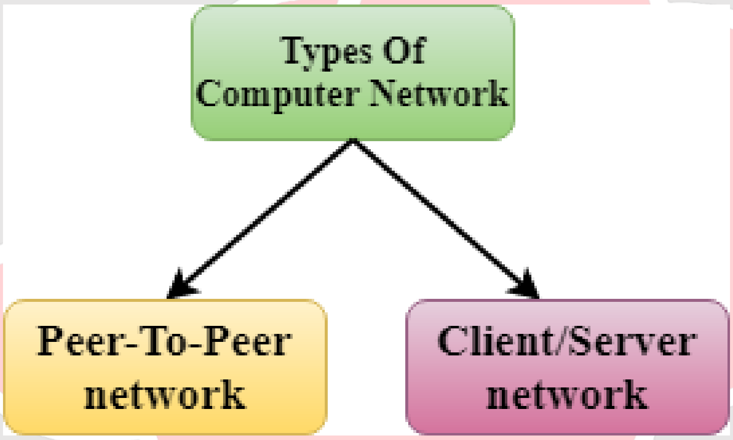
4. Cable fault

- The computers in a network are interconnected with the help of connecting cables.

2. Explain the Architecture of Computer Network ?

- Computer Network Architecture is defined as the physical and logical design of the software, hardware, protocols, and media of the transmission of data. Simply we can say that how computers are organized and how tasks are allocated to the computer.

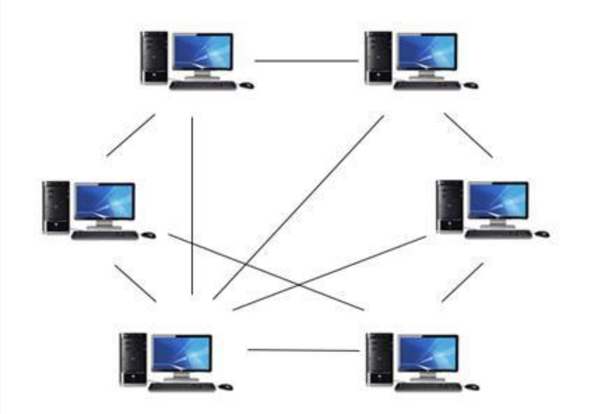
  The two types of network architectures are used :



- Peer To Peer Network
- Client/Server Network

<u>Peer-To-Peer network</u>

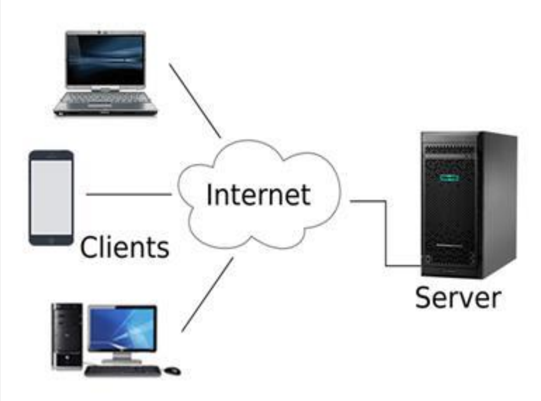
- Peer-To-Peer network is a network in which all the computers are linked together with equal privilege and responsibilities for processing the data.
- Peer-To-Peer network is useful for small environments, usually up to 10 computers.
- Peer-To-Peer network has no dedicated server.
- Special permissions are assigned to each computer for sharing the resources, but this can lead to a problem if the computer with the resource is down.



(peer to peer)

Client/Server Network

- Client/Server network is a network model designed for the end users called clients, to access the resources such as songs, video, etc. from a central computer known as Server.
- The central controller is known as a **server** while all other computers in the network are called **clients**.
- A server performs all the major operations such as security and network management.
- A server is responsible for managing all the resources such as files, directories, printer, etc.
- All the clients communicate with each other through a server. For example, if client1 wants to send some data to client 2, then it first sends the request to the server for the permission. The server sends the response to the client 1 to initiate its communication with the client 2.



(client & server)

1. Explain types of networks in detail .

- ➢ There are Three Types of Computer Networks:
- Local Area Network (LAN)
- Metropolitan Area Network (MAN)

- Wide Area Network (WAN)

Local Area Network

- A **local area network**, or **LAN**, consists of a computer network at a single site, typically an individual office building. A LAN is very useful for sharing resources, such as data storage and printers. LANs can be built with relatively inexpensive hardware, such as hubs, network adapters and Ethernet cables.
- The smallest LAN may only use two computers, while larger LANs can accommodate thousands of computers. A LAN typically relies mostly on wired connections for increased speed and security, but wireless connections can also be part of a LAN. High speed and relatively low cost are the defining characteristics of LANs.
- LANs are typically used for single sites where people need to share resources among themselves but not with the rest of the outside world. Think of an office building where everybody should be able to access files on a central server or be able to print a document to one or more central printers. Those tasks should be easy for everybody working in the same office, but you would not want somebody just walking outside to be able to send a document to the printer from their cell phone! If a local area network, or LAN, is entirely wireless, it is referred to as a wireless local area network, or WLAN.

Metropolitan Area Network

- A **metropolitan area network**, or **MAN**, consists of a computer network across an entire city, college campus or small region. A MAN is larger than a LAN, which is typically limited to a single building or site.

Depending on the configuration, this type of network can cover an area from several miles to tens of miles. A MAN is often used to connect several LANs together to form a bigger network.

When this type of network is specifically designed for a college campus, it is sometimes referred to as a campus area network, or CAN.

A metropolitan area network is a network that covers a larger geographic area by interconnecting a different LAN to form a larger network.

Government agencies use MAN to connect to the citizens and private industries.

In MAN, various LANs are connected to each other through a telephone exchange line.

The most widely used protocols in MAN are RS-232, Frame Relay, ATM, ISDN, OC-3, ADSL, etc.

It has a higher range than Local Area Network(LAN).

Uses Of Metropolitan Area Network:

- MAN is used in communication between the banks in a city.
- It can be used in an Airline Reservation.

- It can be used in a college within a city.
- It can also be used for communication in the military.

Wide Area Network

- A **wide area network**, or **WAN**, occupies a very large area, such as an entire country or the entire world. A WAN can contain multiple smaller networks, such as LANs or MANs. The Internet is the best-known example of a public WAN.
- A Wide Area Network is a network that extends over a large geographical area such as states or countries.
- A Wide Area Network is quite bigger network than the LAN.
- A Wide Area Network is not limited to a single location, but it spans over a large geographical area through a telephone line, fibre optic cable or satellite links.
- The internet is one of the biggest WAN in the world.
- A Wide Area Network is widely used in the field of Business, government, and education.

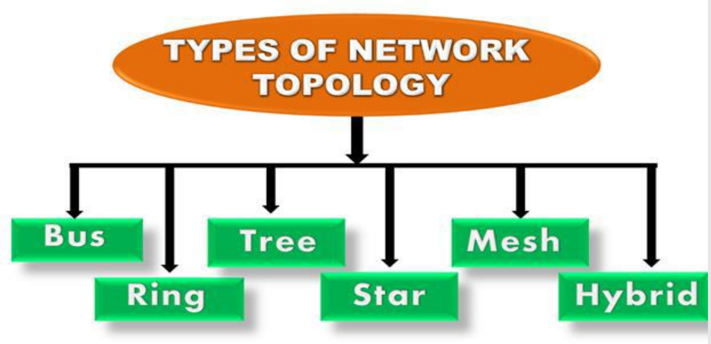
Examples Of Wide Area Network:

- **Mobile Broadband:** A 4G network is widely used across a region or country.
- **Private network:** A bank provides a private network that connects the 44 offices. This network is made by using the telephone leased line provided by the telecom company.

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

- Topology defines the structure of the network of how all the components are interconnected to each other. There are two types of topology: physical and logical topology.

  Physical topology is the geometric representation of all the nodes in a network



1. Bus Topology

- The bus topology is designed in such a way that all the stations are connected through a single cable known as a backbone cable.
- Each node is either connected to the backbone cable by drop cable or directly connected to the backbone cable.

- When a node wants to send a message over the network, it puts a message over the network. All the stations available in the network will receive the message whether it has been addressed or not.
- The bus topology is mainly used in 802.3 (ethernet) and 802.4 standard networks.
- The configuration of a bus topology is quite simpler as compared to other topologies.
- The backbone cable is considered as a **"single lane"** through which the message is broadcast to all the stations.
- The most common access method of the bus topologies is **CSMA** (Carrier Sense Multiple Access).

CSMA: It is a media access control used to control the data flow so that data integrity is maintained, i.e., the packets do not get lost. There are two alternative ways of handling the problems that occur when two nodes send the messages simultaneously.

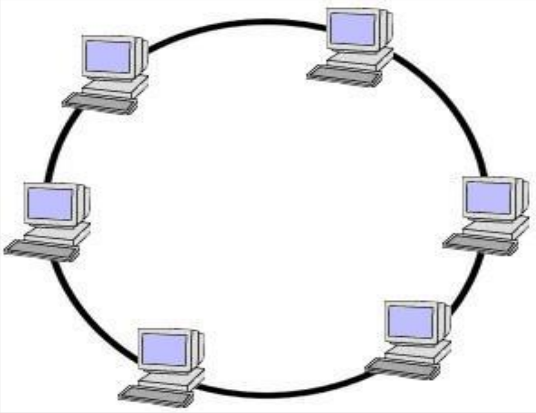
Advantages of Bus topology:

- **Low-cost cable:** In bus topology, nodes are directly connected to the cable without passing through a hub. Therefore, the initial cost of installation is low.
- **Moderate data speeds:** Coaxial or twisted pair cables are mainly used in bus-based networks that support upto 10 Mbps.
- **Familiar technology:** Bus topology is a familiar technology as the installation and troubleshooting techniques are well known, and hardware components are easily available.
- **Limited failure:** A failure in one node will not have any effect on other nodes.

Disadvantages of Bus topology:

- **Extensive cabling:** A bus topology is quite simpler, but still it requires a lot of cabling.
- **Difficult troubleshooting:** It requires specialized test equipment to determine the cable faults. If any fault occurs in the cable, then it would disrupt the communication for all the nodes.
- **Signal interference:** If two nodes send the messages simultaneously, then the signals of both the nodes collide with each other.
- **Reconfiguration difficult:** Adding new devices to the network would slow down the network.
- **Attenuation:** Attenuation is a loss of signal leads to communication issues. Repeaters are used to regenerate the signal.

2. Ring Topology



- Ring topology is like a bus topology, but with connected ends.
- The node that receives the message from the previous computer will retransmit to the next node.
- The data flows in one direction, i.e., it is unidirectional.
- The data flows in a single loop continuously known as an endless loop.
- It has no terminated ends, i.e., each node is connected to other node and having no termination point.
- The data in a ring topology flow in a clockwise direction.
- The most common access method of the ring topology is **token passing**.
- **Token passing:** It is a network access method in which token is passed from one node to another node.
- **Token:** It is a frame that circulates around the network.

Working of Token passing

- A token moves around the network, and it is passed from computer to computer until it reaches the destination.
- The sender modifies the token by putting the address along with the data.
- The data is passed from one device to another device until the destination address matches. Once the token received by the destination device, then it sends the acknowledgment to the sender.
- In a ring topology, a token is used as a carrier.

Advantages of Ring topology:

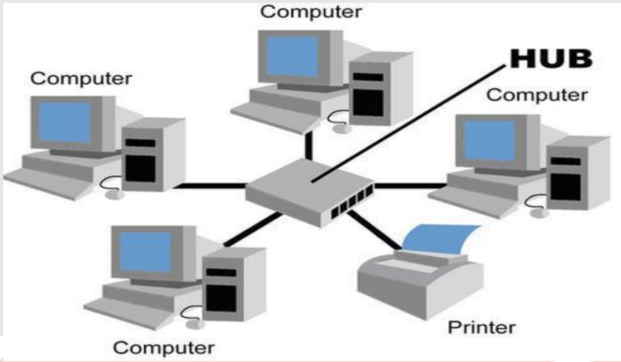
- **Network Management:** Faulty devices can be removed from the network without bringing the network down.
- **Product availability:** Many hardware and software tools for network operation and monitoring are available.
- **Cost:** Twisted pair cabling is inexpensive and easily available. Therefore, the installation cost is very low.

- **Reliable:** It is a more reliable network because the communication system is not dependent on the single host computer.

Disadvantages of Ring topology:

- **Difficult troubleshooting:** It requires specialized test equipment to determine the cable faults. If any fault occurs in the cable, then it would disrupt the communication for all the nodes.
- **Failure:** The breakdown in one station leads to the failure of the overall network.
- **Reconfiguration difficult:** Adding new devices to the network would slow down the network.
- **Delay:** Communication delay is directly proportional to the number of nodes. Adding new devices increases the communication delay.

3. Star Topology



- Star topology is an arrangement of the network in which every node is connected to the central hub, switch or a central computer.
- The central computer is known as a **server**, and the peripheral devices attached to the server are known as **clients**.
- Coaxial 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**.
- Star topology is the most popular topology in network implementation.

Advantages of Star topology

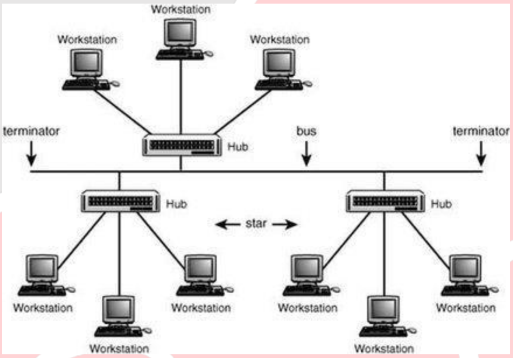
- **Efficient troubleshooting:** Troubleshooting is quite efficient in a star topology as compared to bus topology. In a bus topology, the manager has to inspect the kilometers of cable. In a star topology, all the stations are connected to the centralized network. Therefore, the network administrator has to go to the single station to troubleshoot the problem.
- **Network control:** Complex network control features 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.

- **Familiar technology:** Star topology is a familiar technology as its tools are cost-effective.
- **Easily expandable:** It is easily expandable as new stations can be added to the open ports on the hub.
- **Cost effective:** Star topology networks are cost-effective as it uses inexpensive coaxial cable.
- **High data speeds:** It supports a bandwidth of approx 100Mbps. Ethernet 100BaseT is one of the most popular Star topology networks.

Disadvantages of Star topology

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

4. Tree topology



Tree topology combines the characteristics of bus topology and star topology.

- A tree topology is a type of structure in which all the computers are connected with each other in hierarchical fashion.
- The top-most node in tree topology is known as a root node, and all other nodes are the descendants of the root node.
- There is only one path exists between two nodes for the data transmission. Thus, it forms a parent-child hierarchy.

Advantages of Tree topology

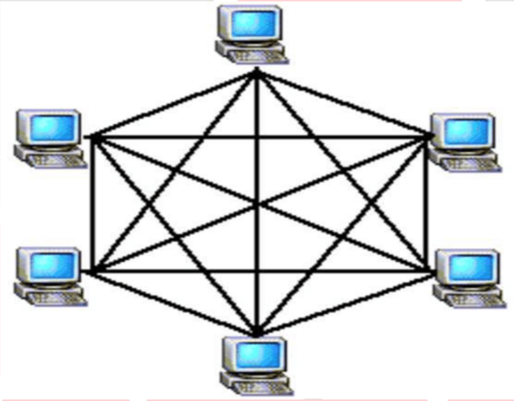
- **Support for broadband transmission:** Tree topology is mainly used to provide broadband transmission, i.e., signals are sent over long distances without being attenuated.
- **Easily expandable:** We can add the new device to the existing network. Therefore, we can say that tree topology is easily expandable.
- **Easily manageable:** In tree topology, the whole network is divided into segments known as star networks which can be easily managed and maintained.

- **Error detection:** Error detection and error correction are very easy in a tree topology.
- **Limited failure:** The breakdown in one station does not affect the entire network.
- **Point-to-point wiring:** It has point-to-point wiring for individual segments.

Disadvantages of Tree topology

- **Difficult troubleshooting:** If any fault occurs in the node, then it becomes difficult to troubleshoot the problem.
- **High cost:** Devices required for broadband transmission are very costly.
- **Failure:** A tree topology mainly relies on main bus cable and failure in main bus cable will damage the overall network.
- **Reconfiguration difficult:** If new devices are added, then it becomes difficult to reconfigure

5. Mesh topology.



- Mesh technology is an arrangement of the network in which computers are interconnected with each other through various redundant connections.
- There are multiple paths from one computer to another computer.
- It does not contain the switch, hub or any central computer which acts as a central point of communication.
- The Internet is an example of the mesh topology.
- Mesh topology is mainly used for WAN implementations where communication failures are a critical concern.
- Mesh topology is mainly used for wireless networks.
- Mesh topology can be formed by using the formula: **Number of cables = (n*(n-1))/2;**

Where n is the number of nodes that represents the network.

Mesh topology is divided into two categories:

- Fully connected mesh topology
- Partially connected mesh topology

- **Full Mesh Topology:** In a full mesh topology, each computer is connected to all the computers available in the network.
- **Partial Mesh Topology:** In a partial mesh topology, not all but certain computers are connected to those computers with which they communicate frequently.

Advantages of Mesh topology:

- **Reliable:** The mesh topology networks are very reliable as if any link breakdown will not affect the communication between connected computers.
- **Fast Communication:** Communication is very fast between the nodes.
- **Easier Reconfiguration:** Adding new devices would not disrupt the communication between other devices.

Disadvantages of Mesh topology

- **Cost:** A mesh topology contains a large number of connected devices such as a router and more transmission media than other topologies.
- **Management:** Mesh topology networks are very large and very difficult to maintain and manage. If the network is not monitored carefully, then the communication link failure goes undetected.
- **Efficiency:** In this topology, redundant connections are high that reduces the efficiency of the network.

6) Write a short note on Unicast, Multicast and Broadcast.

- **Broadcast**

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

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

- Definition - A communication where a message is sent from one sender to all receivers.
- Transmission - Data is sent to all recipients in a network
- Addressing - Uses a special broadcast address
- Delivery - Not all devices may be interested in the data
- Network Traffic - Generates the most amount of network traffic
- Security - Less secure because data is sent to all devices in the network
- Examples - DHCP requests, ARP requests
- Destination - All receivers

Multicast

In multicasting, one/more senders and one/more recipients participate in data transfer traffic. In this method traffic recline between the boundaries of unicast (one-to-one) and broadcast (one-to-all). Multicast lets servers direct single copies of data streams that are then simulated and routed to hosts that request it. IP multicast requires the support of some other protocols like **IGMP (Internet Group Management Protocol), Multicast routing** for its work. Also in Classful IP addressing **Class D** is reserved for multicast groups.

- Definition - A communication where a message is sent from one sender to a group of receivers
- Transmission - Data is sent to a group of recipients
- Addressing - Uses a special multicast address
- Delivery - Not all devices may be interested in the data
- Network Traffic - Generates moderate network traffic
- Security - Moderately secure because data is sent to a specific group of devices
- Examples - Video streaming, online gaming
- Destination - Group of receivers

7) Explain working of Internet and its architecture.

- **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. 1.Application layer
  2. 2.transfer control protocol
  3. 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.

- **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.

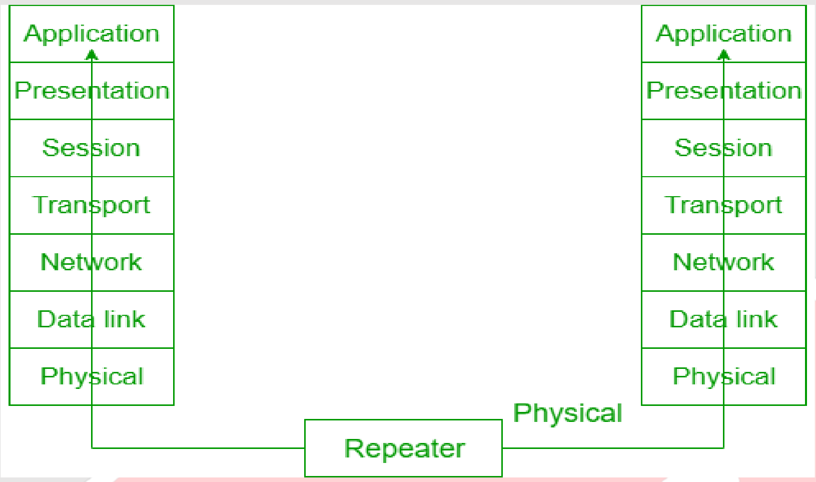
Here in this diagram, a company or an organization has created its private network or intranet for its work(intranet network is under the circle). The company or organization has many employees(in this diagram, we have considered 3). So, for their access, they have PC 1, PC 2, and PC 3(In the real world 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.

- **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

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.

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.

2.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.

- 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.

- **Fiber-Optic Cable**

A fiber-optic cable is made of glass or plastic and transmits signals in the form of light. Light travels in a straight line as long as it is moving through a single uniform substance. If a ray of light traveling through one substance suddenly enters another substance(of a different density), the ray changes direction**.**

Advantages and Disadvantages of Optical Fiber

utilization over fiber-optic cable are limited not by the medium but by the signal generation and reception technology available.

- Less signal attenuation : Fiber-optic transmission distance is significantly greater than that of other guided media. A signal can run for 50 km without requiring regeneration. We need repeaters every 5 km for coaxial or twisted-pair cable.
- Immunity to electromagnetic interference: Electromagnetic noise cannot affect fiber-optic cables.
- Resistance to corrosive materials : Glass is more resistant to corrosive materials than copper.
- Light weight. Fiber-optic cables are much lighter than copper cables.

- Greater immunity to tapping : Fiber-optic cables are more immune to tapping than copper cables.
- Copper cables create antenna effects that can easily be tapped.

Disadvantages

There are some disadvantages in the use of optical fiber.

- Installation and maintenance: Fiber-optic cable is a relatively new technology. Its installation and maintenance require expertise that is not yet available everywhere.
- Unidirectional light propagation: Propagation of light is unidirectional. If we need bidirectional communication, two fibers are needed.
- Cost: The cable and the interfaces are relatively more expensive than those of other guided media.

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

- **Guided Media:**

It is also referred to as Wired or Bounded transmission media. Signals being transmitted are directed and confined in a narrow pathway by using physical links.

Features:

- High Speed
- Secure
- Used for comparatively shorter distances

There are 3 major types of Guided Media:

(i) Twisted Pair Cable –

It consists of 2 separately insulated conductor wires wound about each other. Generally, several such pairs are bundled together in a protective sheath. They are the most widely used Transmission Media. Twisted Pair is of two types:

1. Unshielded Twisted Pair (UTP):

This type of cable has the ability to block interference and does not depend on a physical shield for this purpose. It is used for telephonic applications.

Advantages:

- Least expensive
- Easy to install
- High speed capacity
- Susceptible to external interference
- Lower capacity and performance in comparison to STP
- Short distance transmission due to attenuation

2. Shielded Twisted Pair (STP):

This type of cable consists of a special jacket to block external interference. It is used in fast-data-rate Ethernet and in voice and data channels of telephone lines.

Advantages:

- Better performance at a higher data rate in comparison to UTP
- Eliminates crosstalk
- Comparitively faster
- Comparitively difficult to install and manufacture
- More expensive
- Bulky

(ii) Coaxial Cable –

It has an outer plastic covering containing 2 parallel conductors each having a separate insulated protection cover. Coaxial cable transmits information in two modes: Baseband mode(dedicated cable bandwidth) and Broadband mode(cable bandwidth is split into separate ranges). Cable TVs and analog television networks widely use Coaxial cables.

Advantages:

- High Bandwidth
- Better noise Immunity
- Easy to install and expand
- Inexpensive

Disadvantages:

- Single cable failure can disrupt the entire network

(iii) Optical Fibre Cable –

It uses the concept of reflection of light through a core made up of glass or plastic. The core is surrounded by a less dense glass or plastic covering called the cladding. It is used for transmission of large volumes of data.

The cable can be unidirectional or bidirectional. The WDM (Wavelength Division Multiplexer) supports two modes, namely unidirectional and bi

Advantages:

- Increased capacity and bandwidth
- Light weight
- Less signal attenuation
- Immunity to electromagnetic interference
- Resistance to corrosive materials
- Disadvantages:
- Difficult to install and maintain
- High cost
- Fragile

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

2. 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:

- Signal is broadcasted through air
- Less Secure
- Used for larger distances

There are 3 major types of Unguided Media:

(i) Radiowaves –

These are easy to generate and can penetrate through buildings. The sending and receiving antennas need not be aligned. Frequency Range:3KHz

radios and cordless phones use Radiowaves

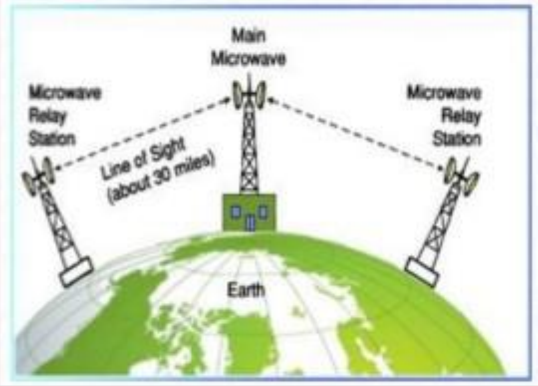
Further Categorized as (i) Terrestrial and (ii) Satellite.

bidirectional mode.

e – 1GHz. AM and FM

(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.



(iii) Infrared –

Infrared waves are used for very short distance communication. They cannot penetrate through obstacles. This prevents interference between systems.

Frequency Range:300GHz – 400THz. It is used in TV remotes, wireless mouse, keyboard, printer,etc.

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

- 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.

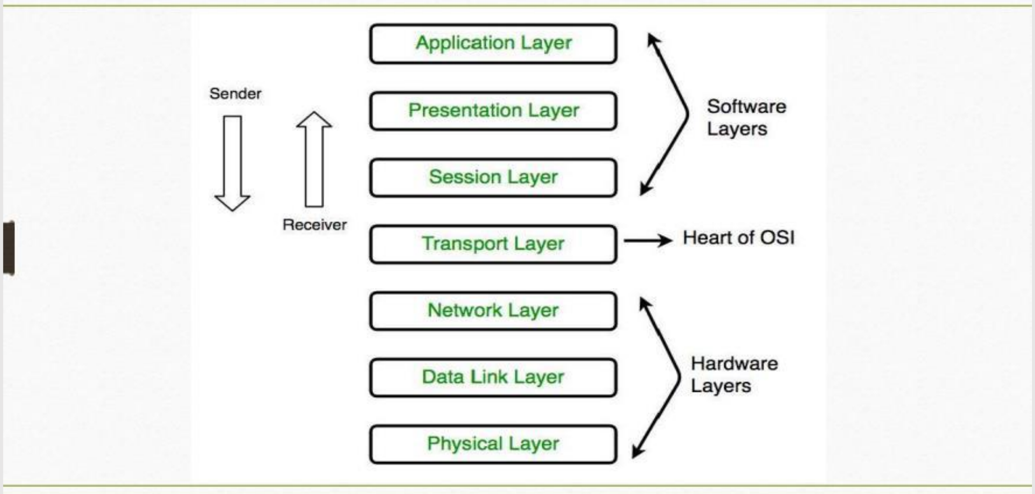
Disadvantages:

- 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.

➢ 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



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.

- 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

- 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 certain information. SNMP uses port numbers 161 (TCP) and 162 (UDP).

18) Write a short note on DNS.

➢ 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.

➢ **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.
- Secure Sockets Layer (SSL) is a standard technique for transmitting documents securely across a network. SSL technology, created by Netscape, establishes a secure connection between a Web server and a browser, ensuring private and secure data transmission. SSL communicates using the Transport Control Protocol (TCP).28-Oct-2021

20) Explain IP Subnetting in detail.

➢ IP subnetting is a fundamental concept in computer networking that allows you to divide an IP address space into smaller, more manageable subnetworks or subnets. Subnetting is essential for efficient IP address allocation and routing. Let's break down IP subnetting in detail:

1. IP Addresses:

   IP addresses are numerical labels assigned to devices on a network to identify and locate them.

   In IPv4, addresses are 32 bits long, typically written as four decimal numbers separated by dots (e.g., 192.168.1.1).

   IPv6 uses 128-bit addresses, represented as a series of hexadecimal numbers (e.g., 2001:0db8:85a3:0000:0000:8a2e:0370:7334).

2. Network and Host Portion:

   An IP address consists of two parts: the network portion and the host portion.

   The network portion identifies the specific network, while the host portion identifies the individual device on that network.

3. Subnet Mask:

   A subnet mask is used to divide the IP address into network and host parts.

   It is a 32-bit value composed of consecutive 1s (network bits) followed by consecutive 0s (host bits).

   For example, in the subnet mask 255.255.255.0 (or /24 in CIDR notation), the first 24 bits are network bits.

4. CIDR Notation:

   Classless Inter-Domain Routing (CIDR) notation is a compact way to represent IP addresses and subnet masks.

   It's expressed as IP_address/mask_bits (e.g., 192.168.1.0/24).

5. Subnetting Benefits:

   Efficient IP address allocation: Subnetting helps minimize IP address wastage.

   Improved network organization: Subnets simplify network management and troubleshooting.

   Enhanced security: Subnets can be used to isolate parts of a network for security purposes.

   Efficient routing: Smaller subnets reduce the size of routing tables, improving network performance.

6. Subnetting Process:

   Determine the required number of subnets and hosts per subnet.Calculate the number of bits required for each: Subnet bits and Host bits.

   Modify the subnet mask accordingly.

   Assign IP addresses to each subnet.

7. Subnetting Example:

   Let's say you have the IP address 192.168.1.0 with a subnet mask of 255.255.255.0 (/24). You want to create four subnets:

   - Determine the subnet bits needed: 2 bits for 4 subnets (2^2 = 4).
   - Calculate host bits: 8 bits (original) - 2 bits (subnet) = 6 bits for hosts.
   - New subnet mask: /26 (32 - 2 - 6 = 24).

   Your subnets would be:

   - Subnet 1: 192.168.1.0/26
   - Subnet 2: 192.168.1.64/26
   - Subnet 3: 192.168.1.128/26
   - Subnet 4: 192.168.1.192/26

   This is a basic overview of IP subnetting. In practice, subnetting can become more complex with variable-length subnet masks and VLSM (Variable Length Subnet Masking) to optimize address allocation for different network segments.

21) Difference between http and https.

➢ 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.

➢ **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.

➢ **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 apage 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.

1. Introduction

Email services have revolutionized communication since their inception. They have become an integral part of both personal and professional communication, enabling individuals and organizations to send and receive messages, documents, and multimedia content efficiently. This case study explores the inner workings of email services, their evolution over the years, and the various components that make them function seamlessly.

2. Background

Email, short for electronic mail, emerged as a means of sending digital messages between users over computer networks in the 1960s and 1970s. Since then, it has evolved from simple text-based messages to support multimedia content, advanced security features, and real-time collaboration. Email services are made possible through a combination of hardware, software, and internet protocols.

3. Key Components of Email Services

- User Interface

  Email services typically provide users with a web-based interface (e.g., Gmail, Outlook) or support for third-party email clients (e.g., Thunderbird, Microsoft Outlook).

  The user interface allows users to compose, send, receive, and organize emails

- Mail Servers

  Mail servers are the backbone of email services. They are responsible for storing and forwarding emails.

- Two primary types of mail servers exist: SMTP (Simple Mail Transfer Protocol) servers for sending emails and POP3 (Post Office Protocol) or IMAP (Internet Message Access Protocol) servers for receiving and storing emails.

- Protocols

- SMTP is used for sending emails, while POP3 and IMAP are used for receiving emails.
- These protocols define the rules for communication between email clients and servers.

- Spam Filters
  - Email services employ spam filters to identify and filter out unwanted or potentially harmful emails.
  - These filters use algorithms and heuristics to assess the content of incoming emails.
- Security
  - Secure Sockets Layer (SSL) and Transport Layer Security (TLS) are encryption protocols used to secure email communication between clients and servers.
  - Authentication mechanisms such as DKIM (DomainKeys Identified Mail) and SPF (Sender Policy Framework) help verify the authenticity of senders.

- Storage
  - Email services provide storage space for users' emails. The amount of storage varies depending on the service provider and subscription plan.
  - Users can typically archive, delete, or organize their emails within their allocated storage.

4. Evolution of Email Services

- Multimedia Support
  - Early email systems were limited to text-based messages. However, modern email services support attachments, images, videos, and rich formatting options.
- Collaboration Features
  - Email services have evolved to offer real-time collaboration tools, such as shared calendars, document collaboration, and video conferencing integrations.
- Mobile Accessibility
  - The proliferation of smartphones has led to the development of mobile email apps, making it possible to access email on the go.
- Cloud Integration
  - Many email services now offer cloud storage integration, enabling users to store email attachments in cloud services like Google Drive or Dropbox.

5. Conclusion

Email services have come a long way since their inception, evolving to meet the changing needs of users and organizations. From basic text-based communication to multimedia-rich collaboration platforms, email services continue to play a crucial role in modern communication. Understanding the key components and the evolution of email services is essential for both users and technology professionals to make the most of this ubiquitous communication tool. As technology continues to advance, it is likely that email services will continue to evolve to meet the ever-expanding demands of the digital age.

25) Explain URL and types of URL in detail.

➢ 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.