UNIT-1

INTRODUCTION TO DATA COMMUNICATION

A computer network setup by connect two or more computer devices and other support hardware devices through communication channel is called computer network. A computer network is a set of devices connected through links. A node can be computer, printer, or any other device capable of sending or receiving the data. The links connecting the nodes are known as communication channels.

Uses of computer network:

- It allows you to share resources such as printers, scanners, etc.
- You can share expensive software and database among network users.
- It facilitates communications from one computer to another computer.
- It allows the exchange of data and information among users through a network.

CRITERIA OF COMPUTER NETWORK

Security: It provides limited interaction that a user can have with the entire system. For example, a bank allows the users to access their own accounts through an ATM without allowing them to access the bank's entire database.

Faster problem solving: Multiple computers can solve the problem faster than a single machine working alone.

Security through redundancy: Multiple computers running the same program at the same time can provide the security through redundancy. For example, if four computers run the same program and any computer has a hardware error, then other computers can override it.

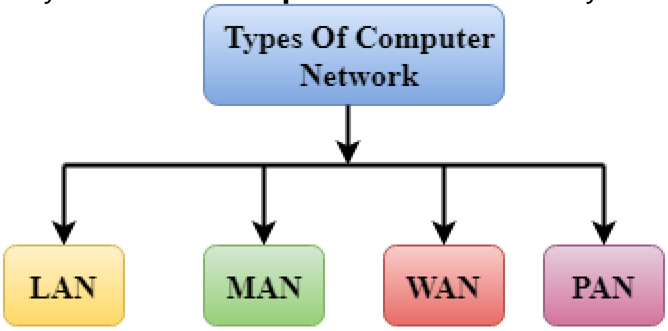
Performance: It can be measured in many ways, including transmit time and response time. Transit time is the amount of time required for a message to travel from one device to another. Response time is the elapsed time between an inquiry and a response. The performance of the network depends on a number of factors, including the number of users, the type of medium & Hardware

Reliability: In addition to accuracy is measured by frequency of failure, the time it takes a link to recover from failure, and the network's robustness in catastrophe.

In-Security: Network security issues include protecting data from unauthorized access, protecting data from damage and development, and implementing policies and procedures for recovery from breaches and data loss.

TYPES OF COMPUTERS NETWOK

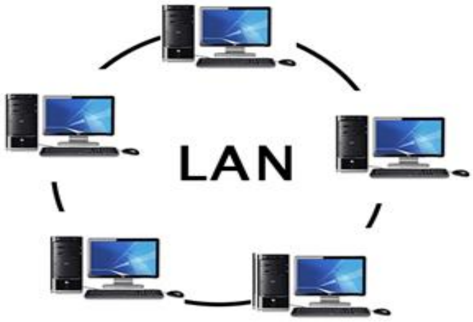
A computer network is a group of computers linked to each other that enables the computer to communicate with another computer and share their resources, data, and applications.A computer network can be categorized by their size. A **computer network** is mainly of **four types**:



- LAN(Local Area Network)
- PAN(Personal Area Network)
- MAN(Metropolitan Area Network)
- WAN(Wide Area Network)

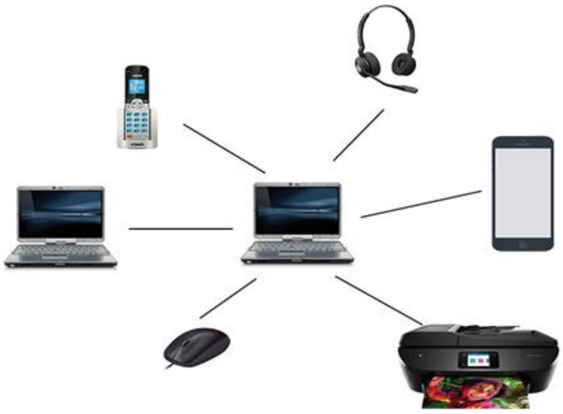
LAN(Local Area Network)

- Local Area Network is a group of computers connected to each other in a small area such as building, office.
- LAN is used for connecting two or more personal computers through a communication medium such as twisted pair, coaxial cable, etc.
- It is less costly as it is built with inexpensive hardware such as hubs, network adapters, and ethernet cables.
- The data is transferred at an extremely faster rate in Local Area Network.
- Local Area Network provides higher security.



PAN(Personal Area Network)

- Personal Area Network is a network arranged within an individual person, typically within a range of 10 meters.
- Personal Area Network is used for connecting the computer devices of personal use is known as Personal Area Network.
- **Thomas Zimmerman** was the first research scientist to bring the idea of the Personal Area Network.
- Personal Area Network covers an area of **30 feet**.
- Personal computer devices that are used to develop the personal area network are the laptop, mobile phones, media player and play stations.



There are two types of Personal Area Network:

- Wired Personal Area Network
- Wireless Personal Area Network

Wireless Personal Area Network: Wireless Personal Area Network is developed by simply using wireless technologies such as WiFi, Bluetooth. It is a low range.

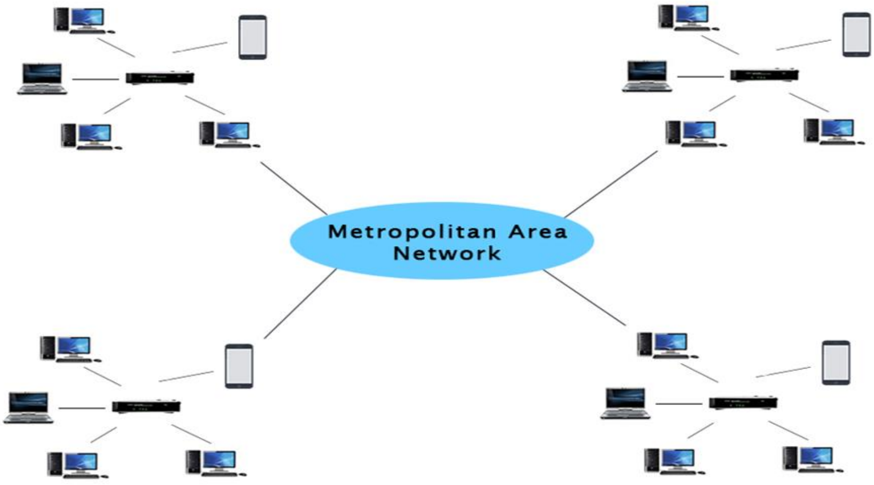
Wired Personal Area Network: Wired Personal Area Network is created by using the USB.

Examples Of Personal Area Network:

- **Body Area Network:** Body Area Network is a network that moves with a person. **For example**, a mobile network moves with a person. Suppose a person establishes a network connection and then creates a connection with another device to share the information.
- **Offline Network:** An offline network can be created inside the home, so it is also known as a **home network**. A home network is designed to integrate the devices such as printers, computer, television but they are not connected to the internet.
- **Small Home Office:** It is used to connect a variety of devices to the internet and to a corporate network using a VPN

MAN(Metropolitan Area Network)

- 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).

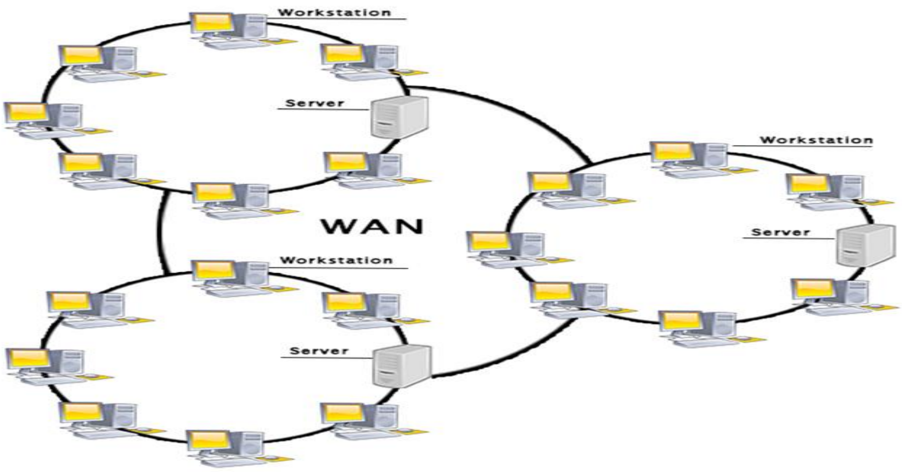


Uses Of Metropolitan Area Network:

- 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.

WAN(Wide Area Network)

- 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.
- **Last mile:** A telecom company is used to provide the internet services to the customers in hundreds of cities by connecting their home with fiber.
- **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.

Advantages Of Wide Area Network:

Following are the advantages of the Wide Area Network:

- **Geographical area:** A Wide Area Network provides a large geographical area. Suppose if the branch of our office is in a different city then we can connect with them through WAN. The internet provides a leased line through which we can connect with another branch.
- **Centralized data:** In case of WAN network, data is centralized. Therefore, we do not need to buy the emails, files or back up servers.
- **Get updated files:** Software companies work on the live server. Therefore, the programmers get the updated files within seconds.
- **Exchange messages:** In a WAN network, messages are transmitted fast. The web application like Facebook, Whatsapp, Skype allows you to communicate with friends.
- **Sharing of software and resources:** In WAN network, we can share the software and other resources like a hard drive, RAM.
- **Global business:** We can do the business over the internet globally.
- **High bandwidth:** If we use the leased lines for our company then this gives the high bandwidth. The high bandwidth increases the data transfer rate which in turn increases the productivity of our company.

P2P & MULTIPOINT CONNECTION

A network is two or more devices connected through a link. A link is a communication pathway that transfers data from one device to another. Devices can be a computer, printer, or any other device that is capable to send and receive data. For visualization purposes, imagine any link as a line drawn between two points.

For communication to occur, two devices must be connected in some way to the same link at the same time. There are two possible types of connections:

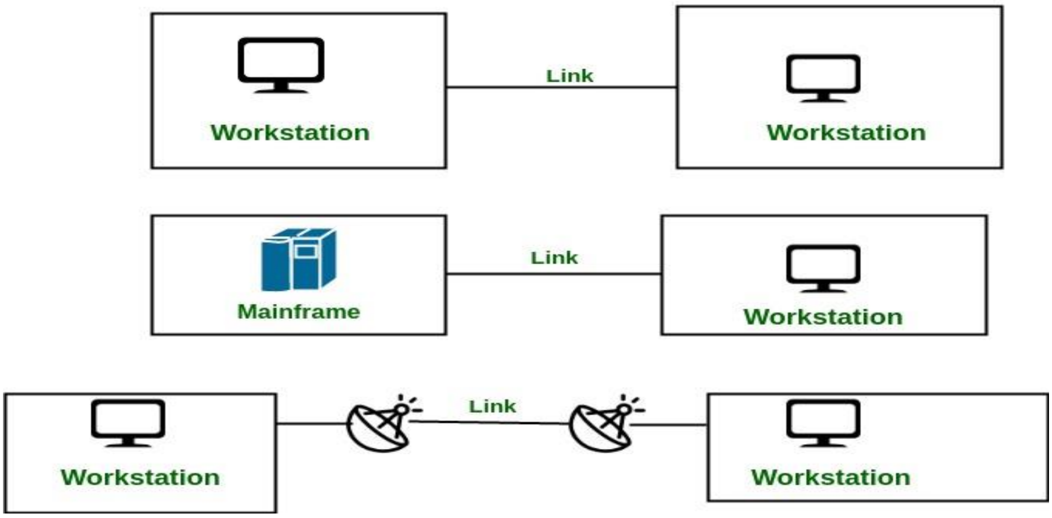
1. **Point-to-Point Connection**
2. **Multipoint Connection**

Point-to-Point Connection:

1. A point-to-point connection provides a dedicated link between two devices.
2. The entire capacity of the link is reserved for transmission between those two devices.

3. Most point-to-point connections use an actual length of wire or cable to connect the two ends, but other options such as microwave or satellite links are also possible.
4. Point to point network topology is considered to be one of the easiest and most conventional networks topologies.
5. It is also the simplest to establish and understand.

Example: Point-to-Point connection between the remote control and Television for changing the channels.



Advantages of Point-to-Point Connection:

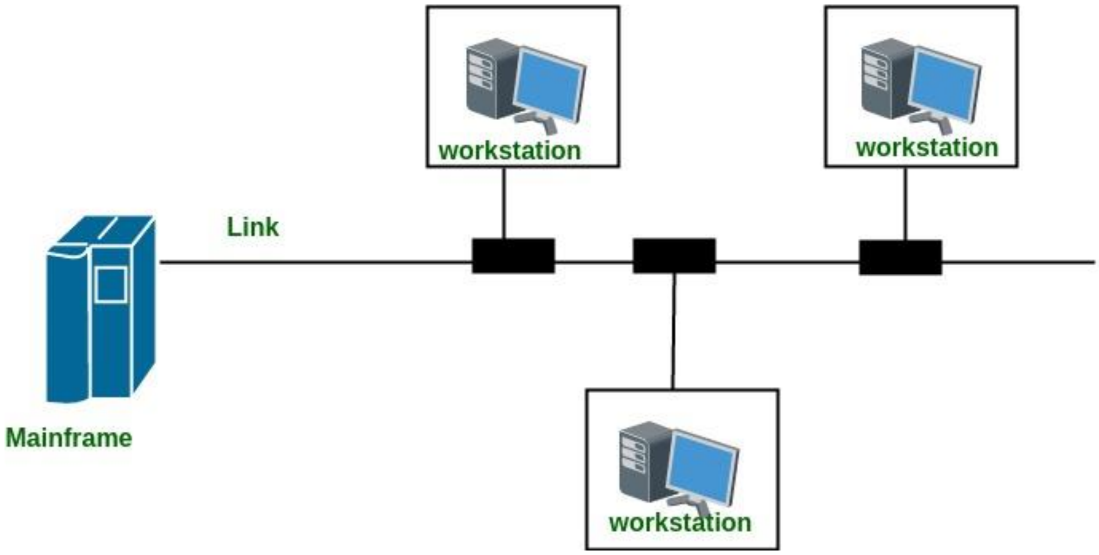
1. **High Bandwidth:** A point-to-point connection provides a dedicated link between two devices, which means that the entire capacity of the link is reserved for the two devices. As a result, point-to-point connections usually offer high bandwidth, which makes them suitable for transferring large amounts of data quickly.
2. **Security:** Point-to-point connections are more secure than multipoint connections because the link is dedicated to only two devices. There is no risk of other devices eavesdropping on the communication or interfering with it in any way.
3. **Reliability:** Because a point-to-point connection provides a dedicated link between two devices, it is usually more reliable than a shared link. If there is a problem with the link, it is easier to troubleshoot and fix because there are only two devices involved.
4. **Increased Control:** Point-to-point connections provide greater control over network traffic and bandwidth allocation. This allows for more efficient use of network resources and can help to prevent issues such as network congestion and bottlenecks.
5. **Easy to Manage:** Point-to-point connections are easy to manage because there are only two devices involved. This reduces the complexity of network administration and makes it easier to troubleshoot problems if they arise.

Multipoint Connection :

1. It is also called Multidrop configuration. In this connection, two or more devices share a single link.
2. If more than two devices share the link then the channel is considered a 'shared channel'. With shared capacity, there can be two possibilities in a Multipoint Line configuration:

Spatial Sharing: If several devices can share the link simultaneously, it's called Spatially shared line configuration.

Temporal (Time) Sharing: If users must take turns using the link, then it's called Temporally shared or Time Shared Line configuration.



Advantages of Multipoint Connection:

1. **Cost-Effective:** Multipoint connections are usually less expensive than point-to-point connections because they allow multiple devices to share the same resources, such as cables, routers, and switches.
2. **Scalability:** Multipoint connections are more scalable than point-to-point connections because they allow multiple devices to be connected to the same link. This makes them suitable for large networks that require many devices to be connected.
3. **Flexibility:** Multipoint connections are more flexible than point-to-point connections because they allow multiple devices to communicate with each other over the same link. This makes them suitable for applications that require collaboration or coordination between multiple devices.
4. **Increased Efficiency:** Multipoint connections can improve network efficiency by allowing multiple devices to transmit data simultaneously. This reduces the chances of network congestion and improves overall network performance.

Here are some features of different line configurations in computer networks:

Point-to-Point:

- Uses a dedicated link to connect two devices
- Simple and easy to set up
- Limited to two devices only
- Does not require a network interface card (NIC) or a hub/switch
- Can become complex and difficult to manage as the network grows

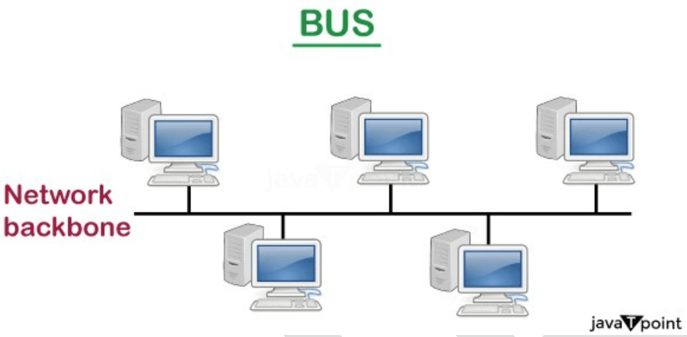
Multipoint:

- Uses a single link to connect three or more devices
- More complex than point-to-point configuration
- Can be more efficient and cost-effective for larger networks
- Devices share the same link, which can lead to collisions and lower performance
- Commonly used in LANs and MANs

PHYSICAL TOPOLOGY (or) NETWORK TOPOLOGY

Physical topology is the geometric representation of all the nodes in a network. There are six types of network topology which are Bus Topology, Ring Topology, Tree Topology, Star Topology, Mesh Topology, and Hybrid Topology.

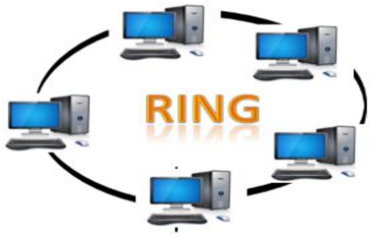
1) Bus Topology



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).

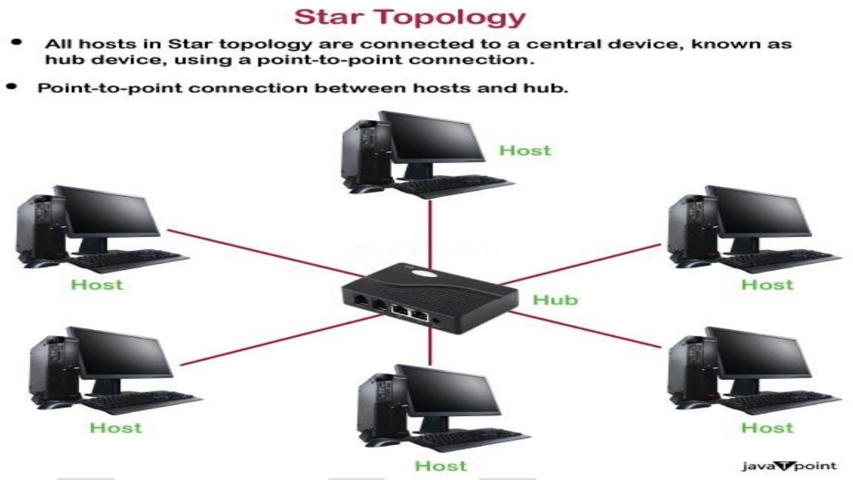
2) Ring Topology



- 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**.

3) Star Topology

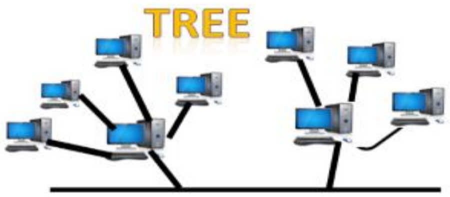


Star Topology

- All hosts in Star topology are connected to a central device, known as hub device, using a point-to-point connection.
- Point-to-point connection between hosts and hub.

- 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.

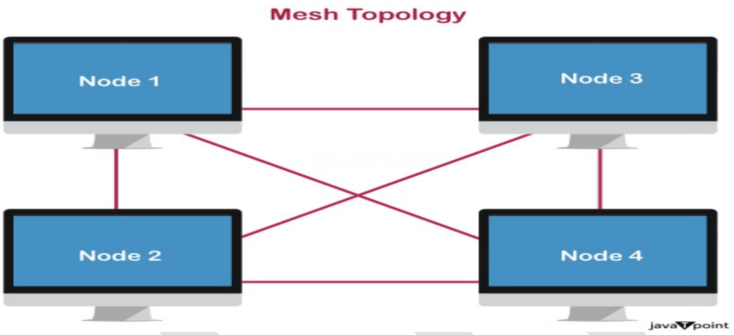
4) Tree topology



- 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.

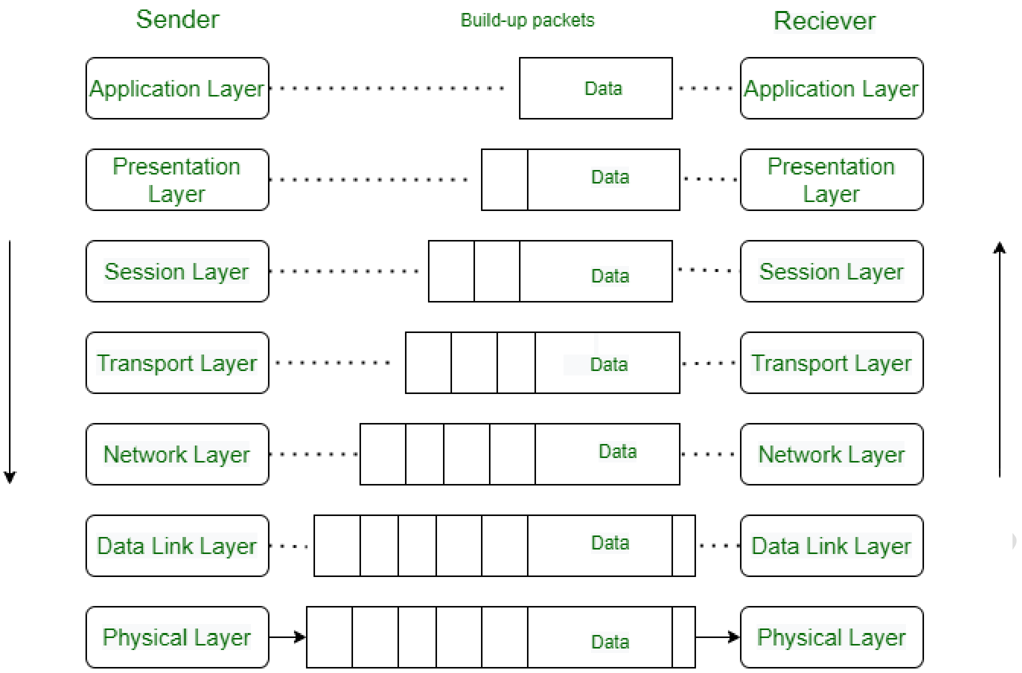
5) Mesh topology



- 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.

OSI REFERENCE MODEL

The OSI model, created in 1984 by ISO, is a reference framework that explains the process of transmitting data between computers. It is divided into seven layers that work together to carry out specialised network functions, allowing for a more systematic approach to networking.



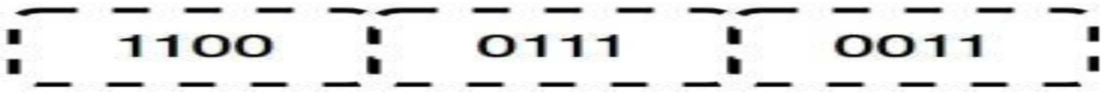
The OSI model consists of seven abstraction layers arranged in a top-down order:

1. Physical Layer
2. Data Link Layer
3. Network Layer
4. Transport Layer
5. Session Layer
6. Presentation Layer
7. Application Layer

Physical Layer – Layer 1 :

The lowest layer of the OSI reference model is the physical layer. It is responsible for the actual physical connection between the devices. The physical layer contains information in the form of **bits.** It is responsible for transmitting individual bits from one node to the next. When receiving data, this layer will get the signal received and convert it into 0s and 1s and send them to the Data Link layer, which will put the frame back together.

Hub, Repeater, Modem, and Cables are Physical Layer devices.



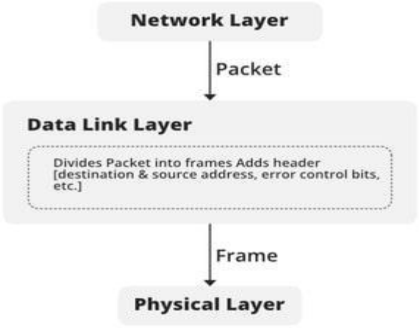
Datalink Layer – Layer 2:

The data link layer is responsible for the node-to-node delivery of the message. The main function of this layer is to make sure data transfer is error-free from one node to another, over the physical layer. When a packet arrives in a network, it is the responsibility of the DLL to transmit it to the Host using its MAC address.
The Data Link Layer is divided into two sublayers:

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

The packet received from the Network layer is further divided into frames depending on the frame size of the NIC(Network Interface Card). DLL also encapsulates Sender and Receiver's MAC address in the header.

- *Packet in the Data Link layer is referred to as **Frame.***
- *Data Link layer is handled by the NIC (Network Interface Card) and device drivers of host machines.*
- *Switch & Bridge are Data Link Layer devices*


Network Layer
Packet
Data Link Layer
Divides Packet into frames Adds header [destination & source address, error control bits, etc.]
Frame
Physical Layer

Network Layer - Layer 3 :

The network layer works for the transmission of data from one host to the other located in different networks. It also takes care of packet routing i.e. selection of the shortest path to transmit the packet, from the number of routes available. The sender & receiver's IP addresses are placed in the header by the network layer.

- *Segment in the Network layer is referred to as **Packet**.*
- *Network layer is implemented by networking devices such as routers and switches.*

Transport Layer – Layer 4:

It is responsible for reliable message delivered from process to process. The transport layer provides services to the application layer and takes services from the network layer. The data in the transport layer is referred to as *Segments*. It is responsible for the End to End Delivery of the complete message. The transport layer also provides the acknowledgment of the successful data transmission and re-transmits the data if an error is found.

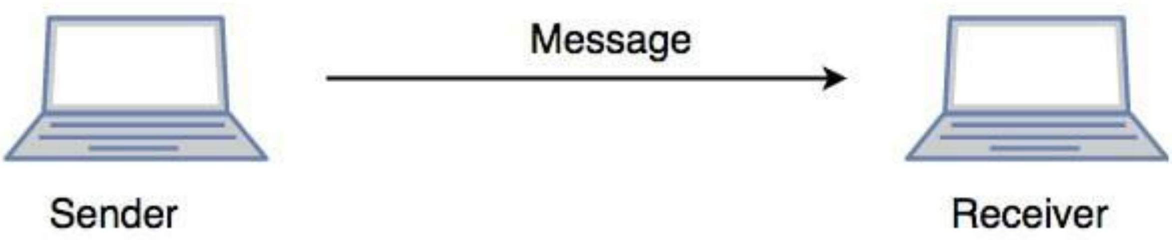
1. *Data in the Transport Layer is called **Segments**.*
2. *Transport layer is operated by the Operating System. It is a part of the OS and communicates with the Application Layer by making system calls.*
3. *The transport layer is called as **Heart of the OSI** model.*
4. ***Protocol Use :** TCP, UDP NetBIOS, PPTP*

Session Layer – Layer 5

This layer is responsible for the establishment of connection, maintenance of sessions, and authentication, terminate the session and also ensures security.

for Example:-

Let us consider a scenario where a user wants to send a message through some Messenger application running in his browser. The "Messenger" here acts as the application layer which provides the user with an interface to create the data. This message or so-called Data is compressed, encrypted (if any secure data), and converted into bits (0's and 1's) so that it can be transmitted.



Presentation Layer – Layer 6

The presentation layer is also called the **Translation layer**. The data from the application layer is extracted here and manipulated as per the required format to transmit over the network.

- **Translation:** For example, ASCII to EBCDIC.
- **Encryption/ Decryption:** Data encryption translates the data into another form or code. The encrypted data is known as the ciphertext and the decrypted data is known as plain text. A key value is used for encrypting as well as decrypting data.
- **Compression:** Reduces the number of bits that need to be transmitted on the network. **Device or Protocol Use :** JPEG, MPEG, GIF,MP3,ASCII

Application Layer – Layer 7

It is provide service to the user and At the very top of the OSI Reference Model stack of layers, we find the Application layer which is implemented by the network applications. These applications produce the data, which has to be transferred over the network. This layer also serves as a window for the application services to access the network and for displaying the received information to the user.

Example: Application – Browsers, Skype Messenger, etc.

1. *The application Layer is also called Desktop Layer.*
2. ***Device or Protocol Use :*** *SMTP, HTTP,HTTPS,FTP*

PROTOCOLS AND STANDARDS

A protocol is a set of rules that governs transmission of data. Many other protocols exist. Some of the more common protocols are:

- **TCP/IP** - Transmission Control Protocol/Internet Protocol - enables communication over the internet.
- **HTTP and HTTPS** - Hypertext Transfer Protocol - governs communication between a webserver and a client. HTTPS (secure) includes secure encryption to allow transactions to be made over the internet.
- **FTP** - File Transfer Protocol - governs the transmission of files across a network and the internet.

- **SMTP** - Simple Mail Transfer Protocol - governs the sending of email over a network to a mail server.
- **POP and IMAP** - Post Office Protocol and Internet Message Access Protocol - govern retrieving emails from email servers. POP is an older implementation, largely replaced by IMAP.

ADDRESSING

In Computer Network, an addressing or a network address is a unique address that is used to uniquely identify each computer (host) connected in a network.

- *Internet Protocol (IP)*adressing
- *media access control (MAC)* addressing

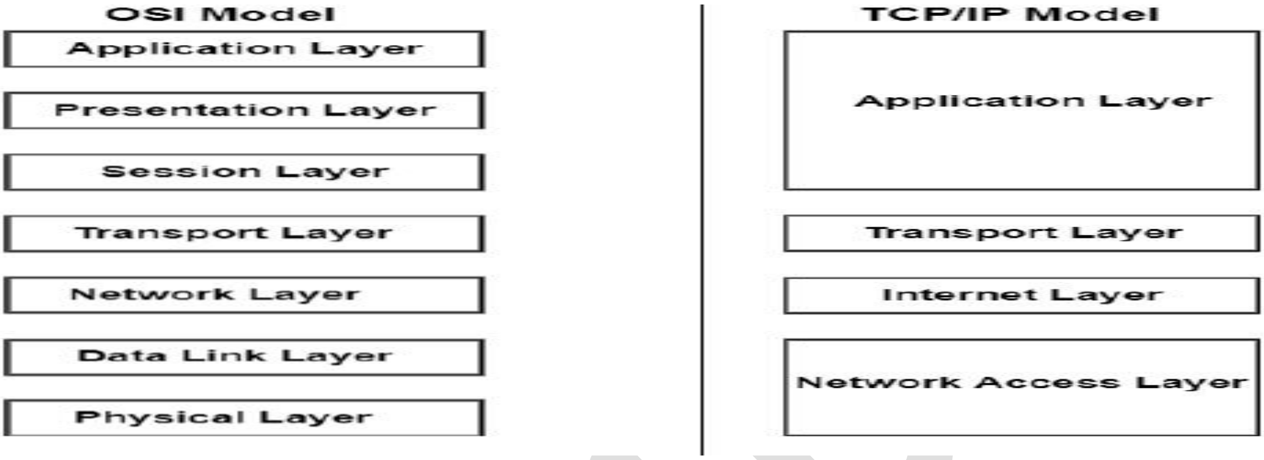
S.NO	MAC Address	IP Address
2.	MAC Address is a six byte hexadecimal address.	IP Address is either a four-byte (IPv4) or a sixteen-byte (IPv6) address.
3.	A device attached with MAC Address can retrieve by ARP protocol.	A device attached with IP Address can retrieve by RARP protocol.
4.	NIC Card's Manufacturer provides the MAC Address.	Internet Service Provider provides IP Address.
5.	MAC Address is used to ensure the physical address of a computer.	IP Address is the logical address of the computer.
6.	MAC Address operates in the data link layer.	IP Address operates in the network layer.
7.	MAC Address helps in simply identifying the device.	IP Address identifies the connection of the device on the network.
8.	MAC Address of computer cannot be changed with time and environment.	IP Address modifies with the time and environment.

S.NO	MAC Address	IP Address
9.	MAC Addresses can't be found easily by a third party.	IP Addresses can be found by a third party.
10.	It is a 48-bit address that contains 6 groups of 2 hexadecimal digits, separated by either hyphens (-) or colons(.). Example: 00:FF:FF:AB:BB:AA or 00-FF-FF-AB-BB-AA	IPv4 uses 32-bit addresses in dotted notations, whereas IPv6 uses 128-bit addresses in hexadecimal notations. Example: IPv4 192.168.1.1 IPv6 FFFF:F200:3204:0B00
11.	No classes are used for MAC addressing.	IPv4 uses A, B, C, D, and E classes for IP addressing.
12.	MAC Address sharing is not allowed.	In IP address multiple client devices can share the IP address.
13.	MAC address help to solve IP address issue.	IP addresses never able to solve MAC address issues.
14.	MAC addresses can be used for broadcasting.	The IP address can be used for broadcasting or multicasting.
15.	MAC address is hardware oriented.	IP address is software oriented.
16.	While communication, Switch needs MAC address to forward data.	While communication, Router need IP address to forward data.

DIFFERENCE BETWEEN OSI AND TCP/IP MODEL

Difference between TCP/IP and OSI Model	
TCP/IP	**OSI Model**
The full form of TCP/IP is Transmission Control Protocol/ Internet Protocol.	The full form of OSI is Open Systems Interconnection.
It is a communication protocol that is based on standard protocols and allows the connection of hosts over a network.	It is a structured model which deals which the functioning of a network.
In 1982, the TCP/IP model became the standard language of ARPANET.	In 1984, the OSI model was introduced by the International Organisation of Standardization (ISO).
It comprises of four layers: • Network Interface • Internet • Transport • Application	It comprises seven layers: • Physical • Data Link • Network • Transport • Session • Presentation • Application
It follows a horizontal approach.	It follows a vertical approach.
The TCP/IP is the implementation of the OSI Model.	An OSI Model is a reference model, based on which a network is created.
It is protocol dependent.	It is protocol independent.

The smallest size of the OSI header is 5 bytes.	The smallest size of the **TCP/IP header** is 20 bytes.



Parameters	**OSI Model**	**TCP/IP Model**
Full Form	OSI stands for Open Systems Interconnection.	TCP/IP stands for Transmission Control Protocol/Internet Protocol.
Layers	It has 7 layers.	It has 4 layers.
Usage	It is low in usage.	It is mostly used.
Approach	It is vertically approached.	It is horizontally approached.
Delivery	Delivery of the package is guaranteed in OSI Model.	Delivery of the package is not guaranteed in TCP/IP Model.
Replacement	Replacement of tools and changes can easily be done in this model.	Replacing the tools is not easy as it is in OSI Model.
Reliability	It is less reliable than TCP/IP Model.	It is more reliable than OSI Model.