UNIT - 4

What is a Network?

- A **network** is a group of two or more computers or other electronic devices that are interconnected for the purpose of exchanging data and sharing resources.
- The computers on a network may be linked through wired or wireless medium.
- There are various terminologies related to network. Some of them are as follows-

- Internet, Intranet
- LAN, WAN
- WWW
- Download, Upload
- Servers, Clients
- Terminals
- Authentication
- Encryption, Decryption

1) INTERNET : The internet is a globally connected network system providing worldwide communication and access to data resources.

2) INTRANET : An intranet is a private network within an enterprise that is used to securely share company information among employees.

3) LAN : It stands for Local Area Network and covers a small area such as a small office or home. It physically connects all the computers located in the premises.

4) WAN : It stands for Wide Area Network and covers a wide area such as a city.

5) WORLD WIDE WEB (WWW) : It is the service that is used on Internet to view and search contents (in the form of web-pages).

6) DOWNLOAD : It is a process that saves data from Internet onto a personal computer.

7) UPLOAD : It is a process that transfers the saved data from a personal computer to Internet server.

8) SERVER : It is a system that provides services to other systems in its network.

9) CLIENT : A client is a computer hardware device or software that accesses a service made available by a server. The server is often (but not always) located on a separate physical computer.

10) TERMINAL : The terminal is the device you use to interact with your computer system.

11) AUTHENTICATION : Authentication is the process of verifying the identity of a user, process, or device to allow access to data in an information system.

12) ENCRYPTION : It is a method by which information is converted into secret code that hides the information's true meaning.

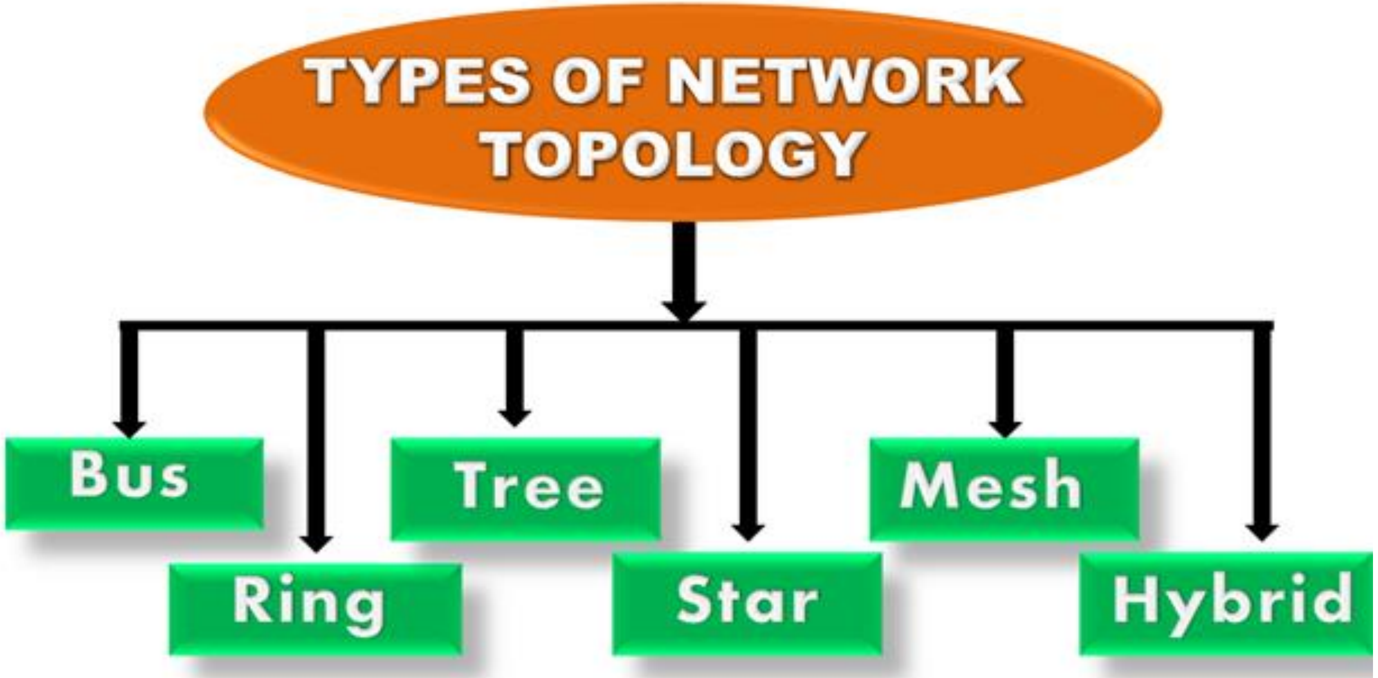
OR

ENCRYPTION : It is the process by which a readable message is converted to an unreadable form to prevent unauthorized parties from reading it.

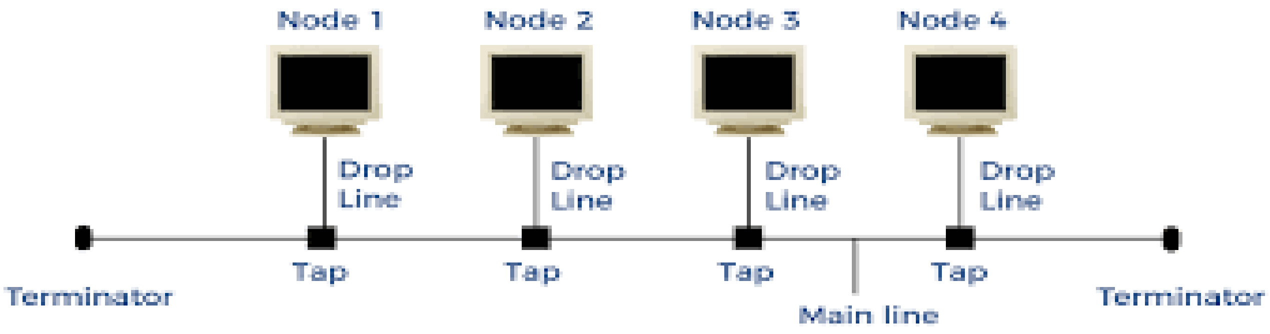
13) DECRYPTION : Decryption is the process of converting an encrypted message back to its original (readable) format. It is generally a reverse process of encryption.

What is Topology?

- Topology defines the structure of the network.
- It shows how all the components are interconnected to each other.



1) Linear or Bus Topology



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 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 stands for Carrier Sense Multiple Access. 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.

- ***CSMA CD:*** CSMA CD (**Collision detection**) is an access method used to detect the collision. Once the collision is detected, the sender will stop transmitting the data. Therefore, it works on "**recovery after the collision**".
- ***CSMA CA:*** CSMA CA **(Collision Avoidance)** is an access method used to avoid the collision by checking whether the transmission media is busy or not. If busy, then the sender waits until the media becomes idle. This technique effectively reduces the possibility of the collision. It does not work on "recovery after the collision".

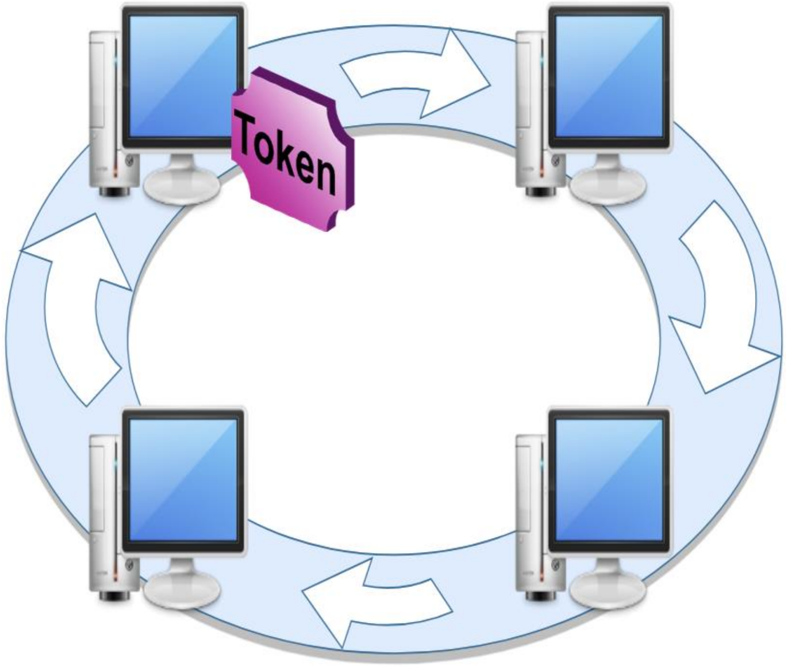
- Advantages of Bus topology:

- ***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 up to 10 Mbps.
- ***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.

2) Ring or Circular 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.

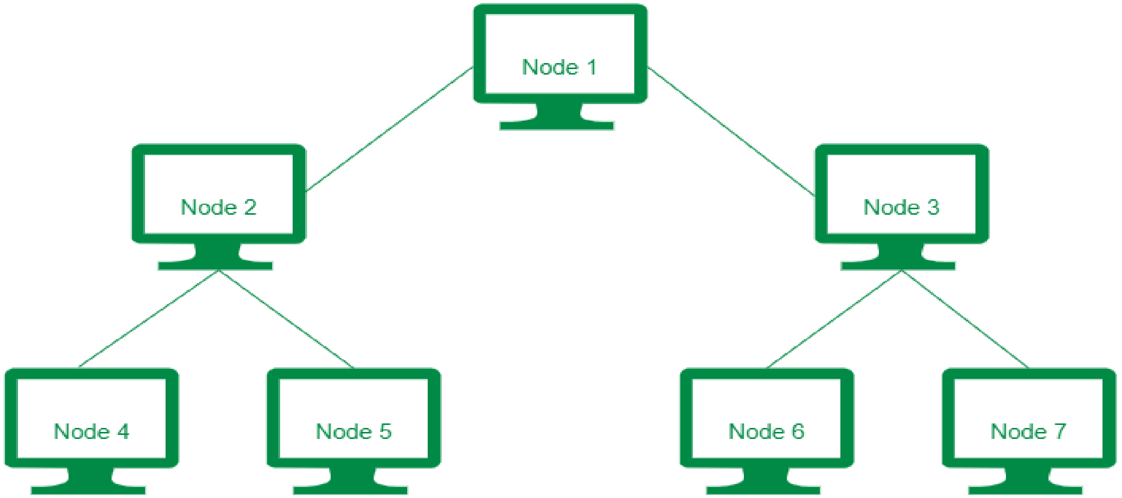
- Advantages of Ring topology:

- **Network Management:** Faulty devices can be removed from the network without bringing the network down.
- **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) Tree Topology



Tree 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 between two nodes for the data transmission.
- Thus, it forms a parent-child hierarchy.

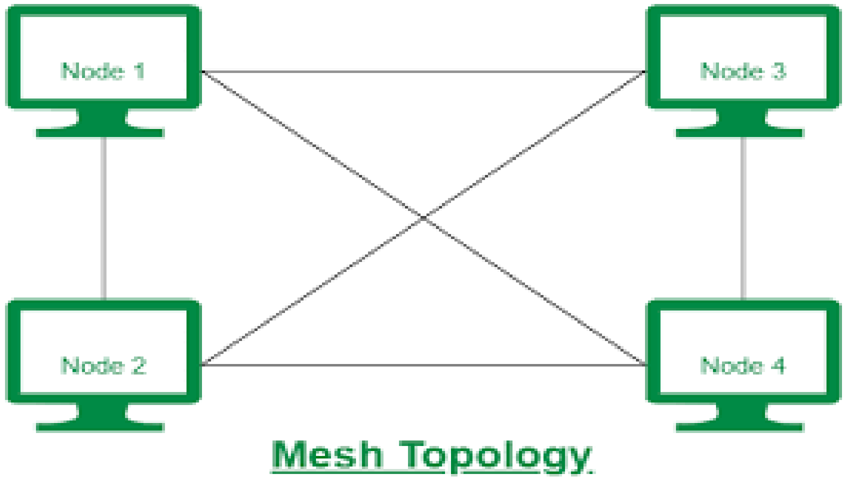
- Advantages of Tree topology

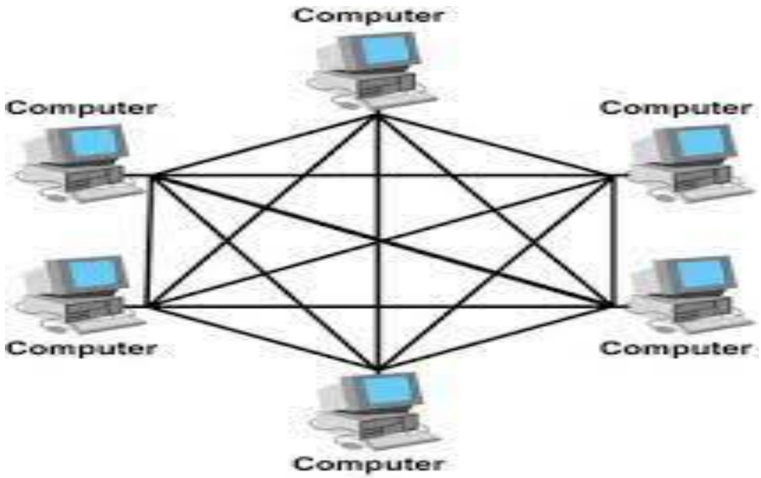
- **Supports broadband transmission:** Tree topology is mainly used to provide broadband transmission, i.e., signals are sent over long distances without being attenuated.
- **Easily expandable:** We can add the new device to the existing network. Therefore, we can say that tree topology is easily expandable.
- **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 is difficult:** If new devices are added, then it becomes difficult to reconfigure.

4) Mesh Topology

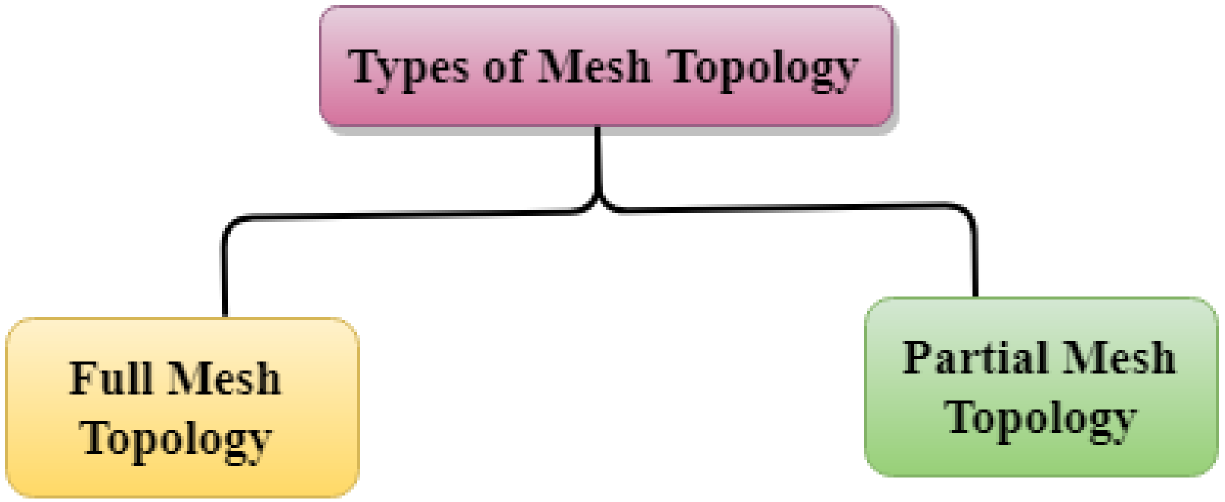




- Mesh technology is an arrangement of the network in which computers are interconnected with each other through various redundant connections.
- There are multiple paths from one computer to another computer.
- It does not contain the switch, hub or any central computer which acts as a central point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

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.

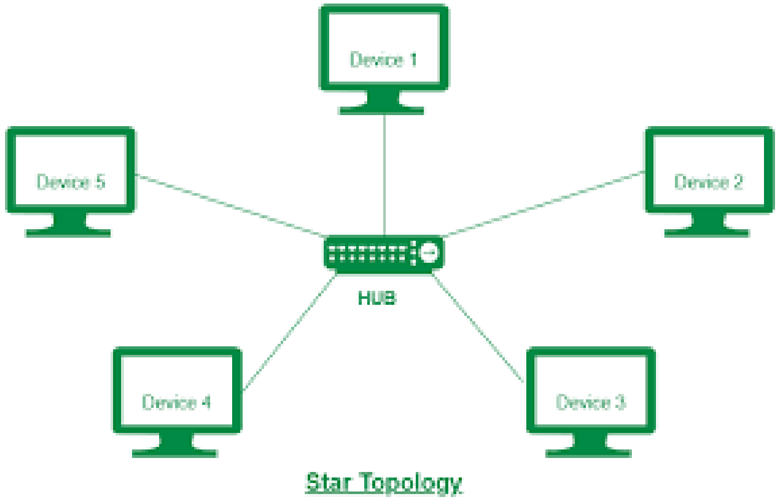
- Advantages of Mesh topology

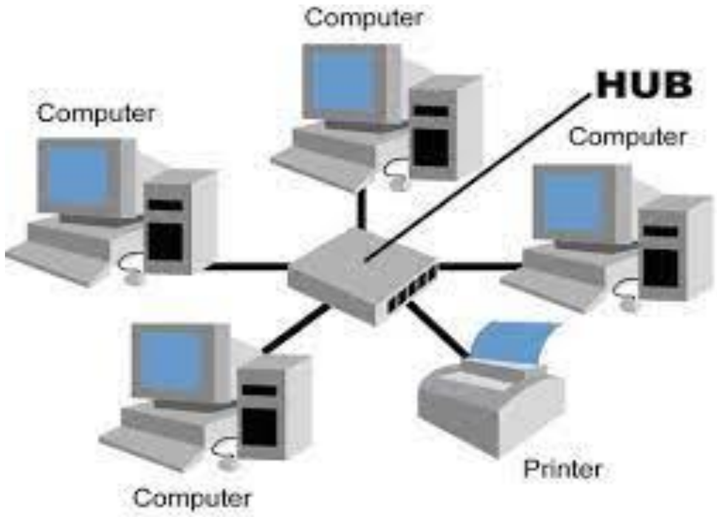
- **Reliable:** The mesh topology networks are very reliable as if any link breakdown will not affect the communication between connected computers.
- **Fast Communication:** Communication is very fast between the nodes.
- **Easier Reconfiguration:** Adding new devices would not disrupt the communication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

5) 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**.
- Hubs or Switches are mainly used as connection devices in a **physical star topology**.
- Star topology is the most popular topology in network implementation.

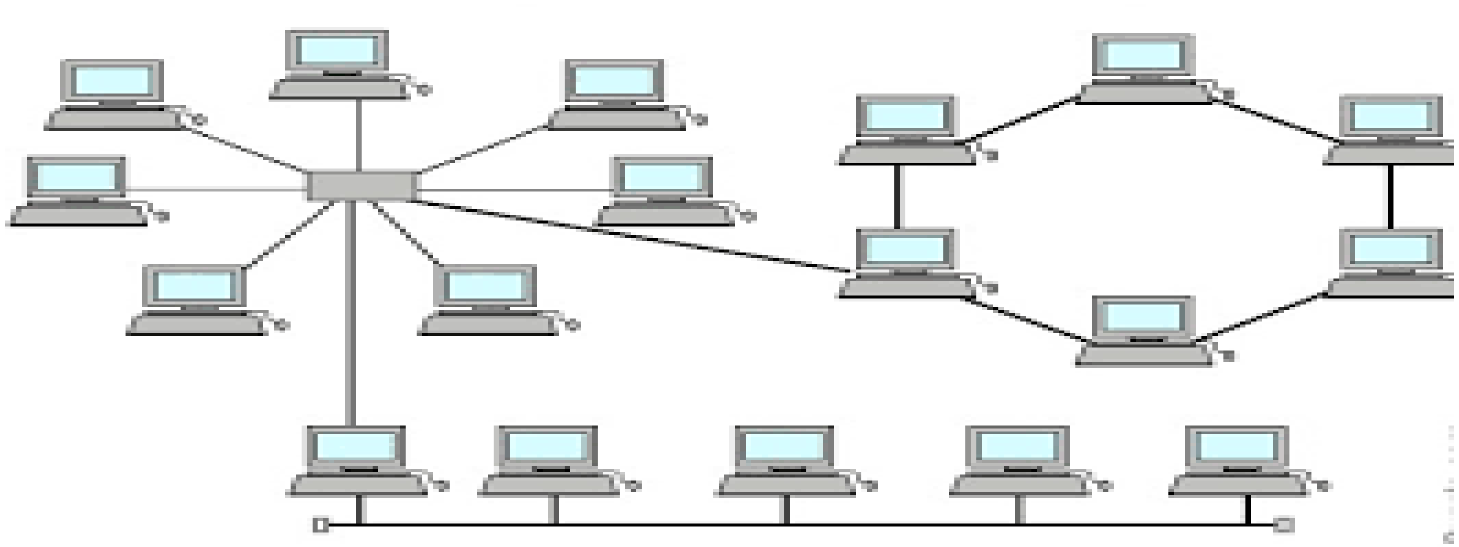
- Advantages of Star topology

- **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.

- 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.

6) Hybrid Topology



- The combination of various different topologies is known as **Hybrid topology**.
- A Hybrid topology is a connection between different links and nodes to transfer the data.
- When two or more different topologies are combined together is termed as Hybrid topology and if similar topologies are connected with each other will not result in Hybrid topology.

- Advantages of Hybrid Topology

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

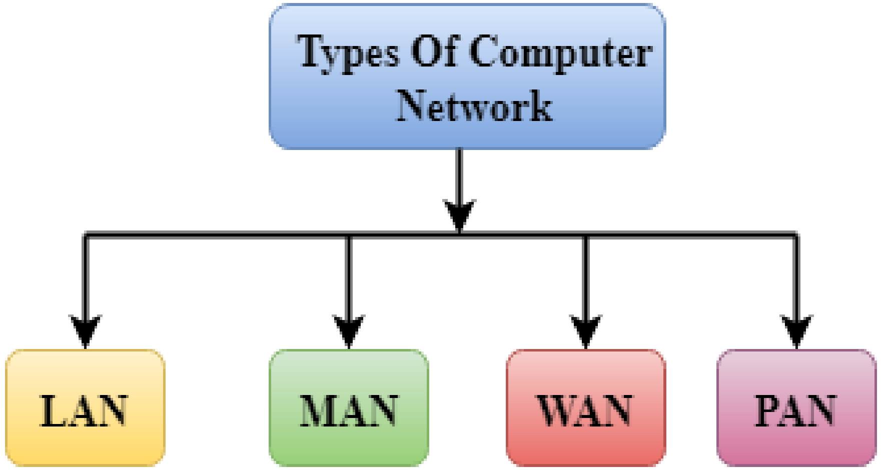
- Disadvantages of Hybrid topology

- **Complex design:** The major drawback of the Hybrid topology is the design of the Hybrid network. It is very difficult to design the architecture of the Hybrid network.
- **Costly Hub:** The Hubs used in the Hybrid topology are very expensive as these hubs are different from usual Hubs used in other topologies.
- **Costly infrastructure:** The infrastructure cost is very high as a hybrid network requires a lot of cabling, network devices, etc.

WHAT IS A COMPUTER NETWORK?

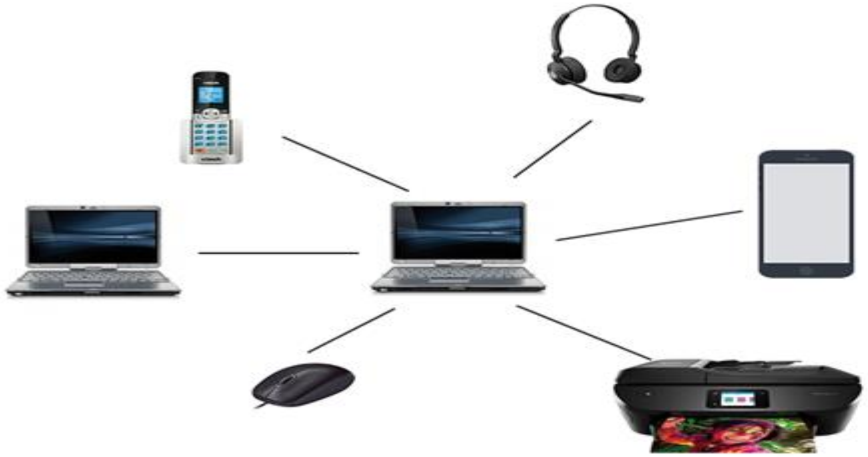
- A computer network is a group of computers linked to each other that enables the computer to communicate with another computer and share their resources, data, and applications.
- It is an interconnected system of devices, represented as network nodes, that share information, data and resources among each other.
- Network types can be defined on the basis of network size, their capabilities and the geographical regions they cover.
- A computer network is mainly of four types:

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

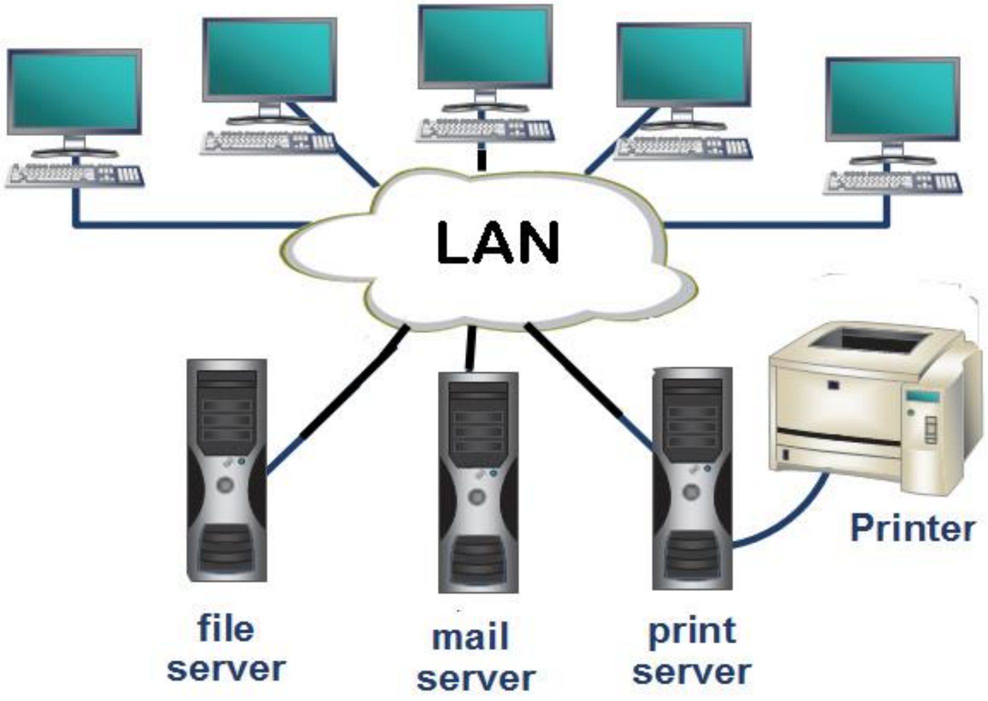


1. Personal Area Network

- A personal area network (PAN) is the smallest and simplest type of network.
- PANs connect devices within the range of about 10 meters (m).
- Because PANs operate in such limited areas of space, most are wireless and provide short-range connectivity with infrared technology.
- An example of a wireless PAN is when users connect Bluetooth devices, like wireless headsets, to a smartphone or laptop.
- Although most PANs are wireless, wired PAN options exist, including USB.

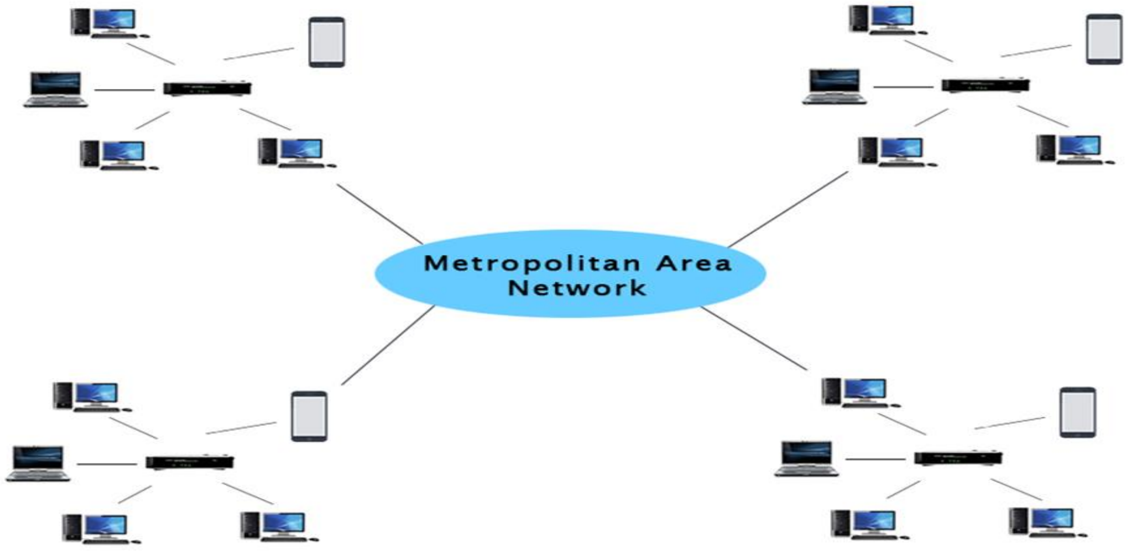


2. Local Area Network



- LAN is one of the simplest computer network.
- It covers a small geographical region in its network.
- Local area network can be established in an office building, schools, colleges, homes or in nearby buildings.
- LAN is very useful network of resource sharing like printers, scanners, data storage etc.
- A local area network can be wired or wireless.
- Typically wired LANs are used for more speed and security.
- If a LAN is entirely wireless it’s called WLAN.
- LAN is used for connecting two or more personal computers through a communication medium such as twisted pair, coaxial cable, etc.
- The data is transferred at an extremely faster rate in Local Area Network.
- Local Area Network provides higher security.
- A LAN can be composed of inexpensive routing and networking devices such as hubs and Ethernet cables.

3. Metropolitan Area Network

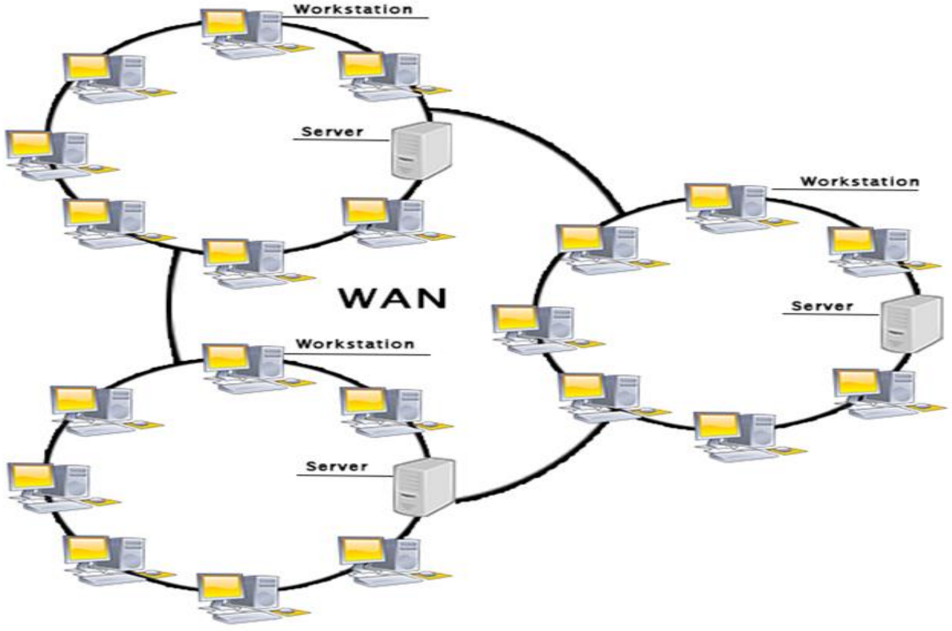


- MAN is relatively new computer network.
- It covers more geographical area in comparison of LAN.
- A Metropolitan Area Network is extended over a city and uses the similar technology as local area network.
- Its geographical area extends to approx. 100kilometers.
- This computer network includes different hardware and transmission media.
- It can be combination of different LANs into a large network for resource sharing or can be a single network like cable TV network.
- Security and standardization are two most important things in a MAN.
- **Security** is required for information sharing between dissimilar devices and **standardization** is required for ensuring reliable data communication.

4. Wide Area Network

- WAN is the most complicated computer network.
- It allows the computing devices to communicate together

  over a large geographical region even when they are quite far.
- A Wide Area Network is not limited to a single location, but it spans over a large geographical area such as states or countries through a telephone line, fiber optic cable or satellite links.



- The internet is one of the biggest WAN in the world.
- The Internet is the most common example of wide area network that connects the computers from all over the world.
- A Wide Area Network is widely used in the field of Business, government, and education.
- This type of computer network uses routers to transmit data securely and quickly.
- LANs are connected to WAN via routers that maintains IP addresses.
- Wide area networks are more complex and owned and managed by collective or distributed ownership and management.

Difference Between LAN, MAN, and WAN

Parameter	LAN	MAN	WAN
Full Form	LAN is an acronym for Local Area Network.	MAN is an acronym for Metropolitan Area Network.	WAN is an acronym for Wide Area Network.
Definition and Meaning	LAN is a network that usually connects a small group of computers in a given geographical area.	MAN is a comparatively wider network that covers large regions- like towns, cities, etc.	The WAN network spans to an even larger locality. It has the capacity to connect various countries together. For example, the Internet is a WAN.
Network Ownership	The LAN is private. Hospitals, homes, schools, offices, etc., may own it.	The MAN can be both private or public. Many organizations and telecom operators may own them.	The WAN can also be both private or public.
Maintenance and Designing	Very easy to design and maintain.	Comparatively difficult to design and maintain.	Very difficult to design and maintain.

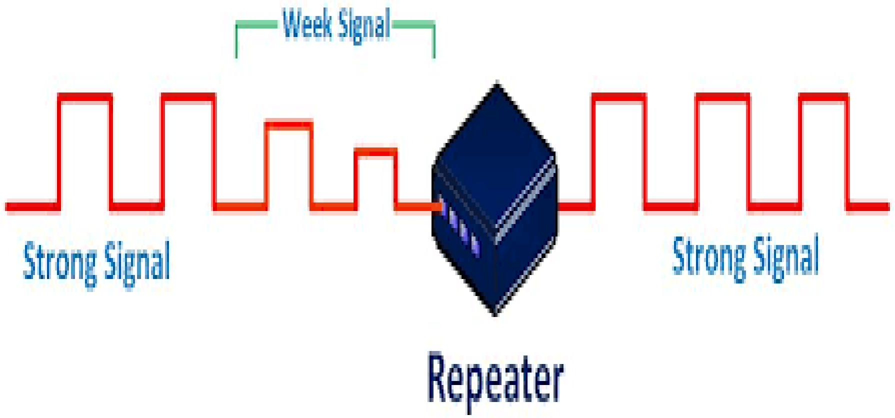
Parameter	LAN	MAN	WAN
Speed	LAN offers a very high Internet speed.	MAN offers a moderate Internet speed.	WAN offers a low Internet speed.
Delay in Propagation	It faces a very short propagation delay.	It faces a moderate propagation delay.	It faces a high propagation delay.
Fault Tolerance	The LAN exhibits a better fault tolerance than the rest of the networks.	The MAN exhibits a lesser fault tolerance.	The WAN also exhibits a lesser fault tolerance.
Bandwidth	The bandwidth of LAN is high.	The bandwidth of MAN is less.	The bandwidth of WAN is relatively low.
Uses	Schools, homes, colleges, hospitals, offices, etc., can privately use it.	It basically covers a city, a small town, or any given area with a bigger radius than the LAN.	It covers an entire country, a subcontinent, or an equivalent area.

NETWORK DEVICES

Network devices, also known as networking hardware, are physical devices that allow hardware on a computer network to communicate and interact with one another. For example Repeater, Hub, Bridge, Switch, Routers, Gateway, etc.

1) Repeater

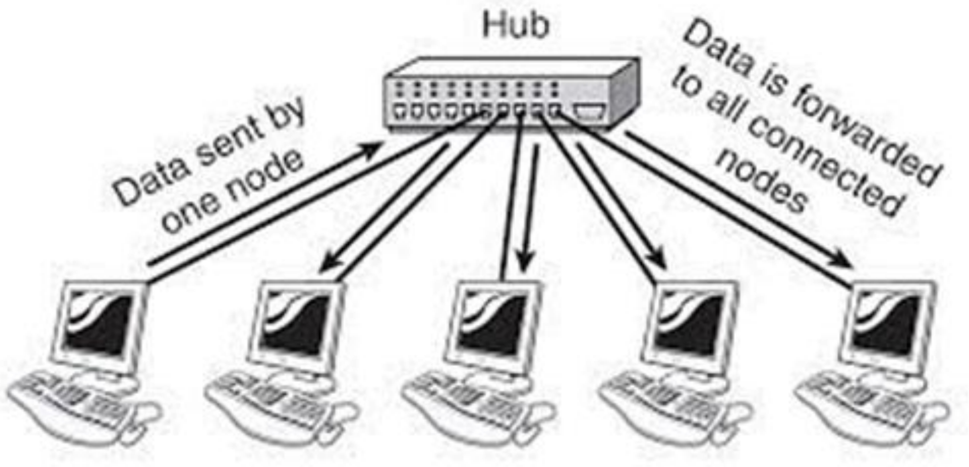
- A repeater is a network device used to reproduce the signals when they transmit over a greater distance so that the signal's strength remains equal.
- The signals get weaker as they transit to greater distances.
- The repeater provides the stability of the signals.



- Repeaters are used in the networking components to enhance the coverage area so these are termed signal boosters.
- When there is the transmission of an electrical signal across the channel, it gets attenuated based on the channel’s behavior and technology.
- This creates a restriction on the length of the LAN connection or expansion of area of the networks.
- This issue can be eliminated by the installation of repeaters at periodic intervals.
- These repeaters are cost-effective and easy to use.
- The repeaters do not influence network performance.
- These repeaters can retransmit the information and strengthen the weak signals.
- While amplifying the signals, the repeaters also amplify the level of noise in those signals.
- If we enhance the extent of the web by only using the repeaters. In that case, the signal propagation time will grow to a considerable level, and the network’s performance will collapse.

2) Hub

- A hub is a common connection point, also known as a network hub, which is used for connection of devices in a network.
- A network hub is a node that broadcasts data to every computer or device connected to it.



- A network hub has no routing tables or intelligence (unlike a network switch or router), which is used to send information.
- Thus, it broadcasts all network data across each and every connection.
- Network hubs are sometimes referred to as "dumb switches.“

- Network hubs are best suited for small, simple local area network (LAN) environments.
- They connect multiple computers together, transmitting data received at one port to all of its other ports without restriction.
- Hubs operate in half-duplex.
- This model raises security and privacy concerns, because traffic could not be safeguarded.
- It also presents a practical issue in terms of traffic management.
- Devices on a hub share one collision domain.

Types of network hubs

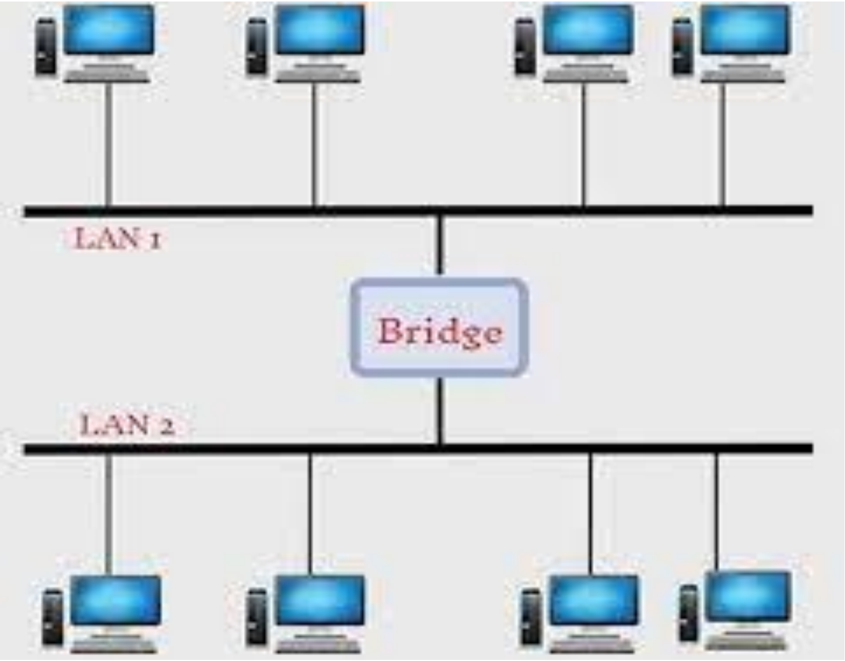
- There are two types of network hubs: active and passive.

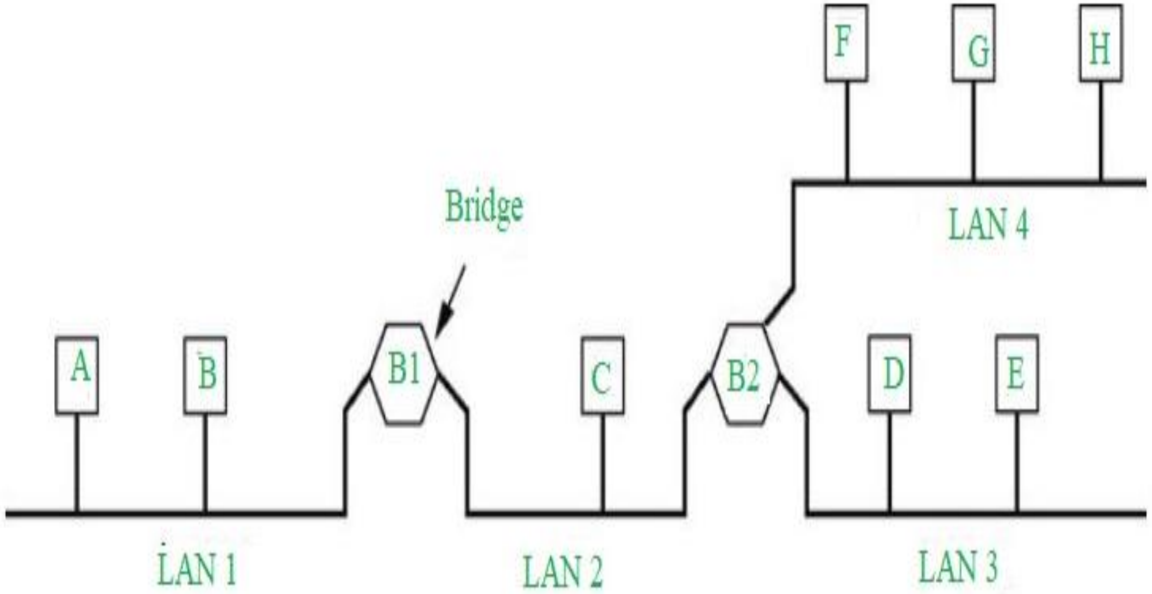
- **Active hubs** repeat and strengthen incoming transmissions. They are also sometimes referred to as repeaters.

- **Passive hubs** simply serves as a point of connectivity, without any additional capabilities.

3) Bridge

- A bridge in a computer network is a device used to connect multiple LANs together with a larger Local Area Network (LAN).
- The mechanism of network aggregation is known as bridging.





- The primary responsibility of a switch is to examine the incoming traffic and determine whether to filter or forward it.
- Here bridge is used to improve network performance.
- Bridges can be used as a network extension like they can connect two network topologies together.
- It has a separate collision domain.

Types of Bridges:

- There are three types of bridges in computer networks, which are as follows:

- Transparent bridge
- Source routing bridge
- **Transparent Bridge:**

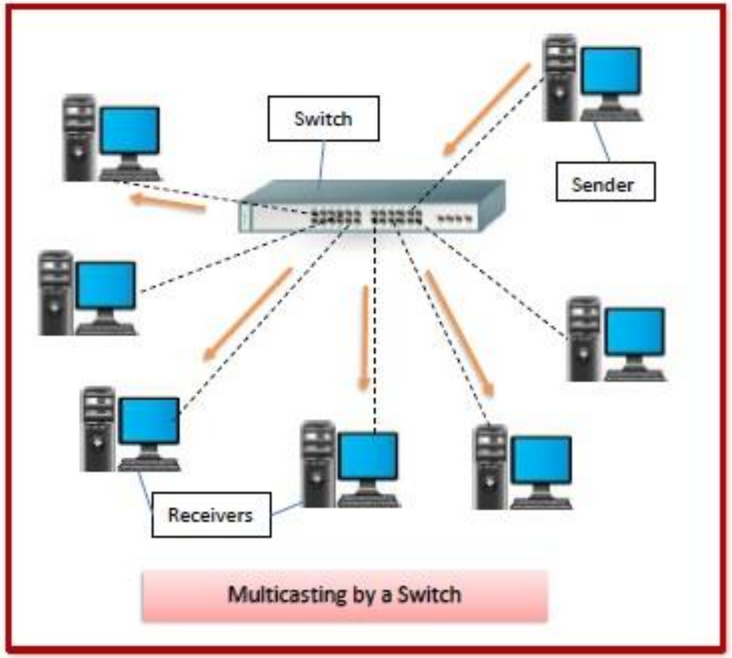
- Transparent bridges are invisible to other devices on the network. This bridge doesn’t reconfigure the network on the addition or deletion of any station.

- **Source Routing Bridge:**

- The frame’s entire route is embedded with the data frames by the source station to perform the routing operation so that once the frame is forwarded it must follow a specific defined path/route.

4) Switch

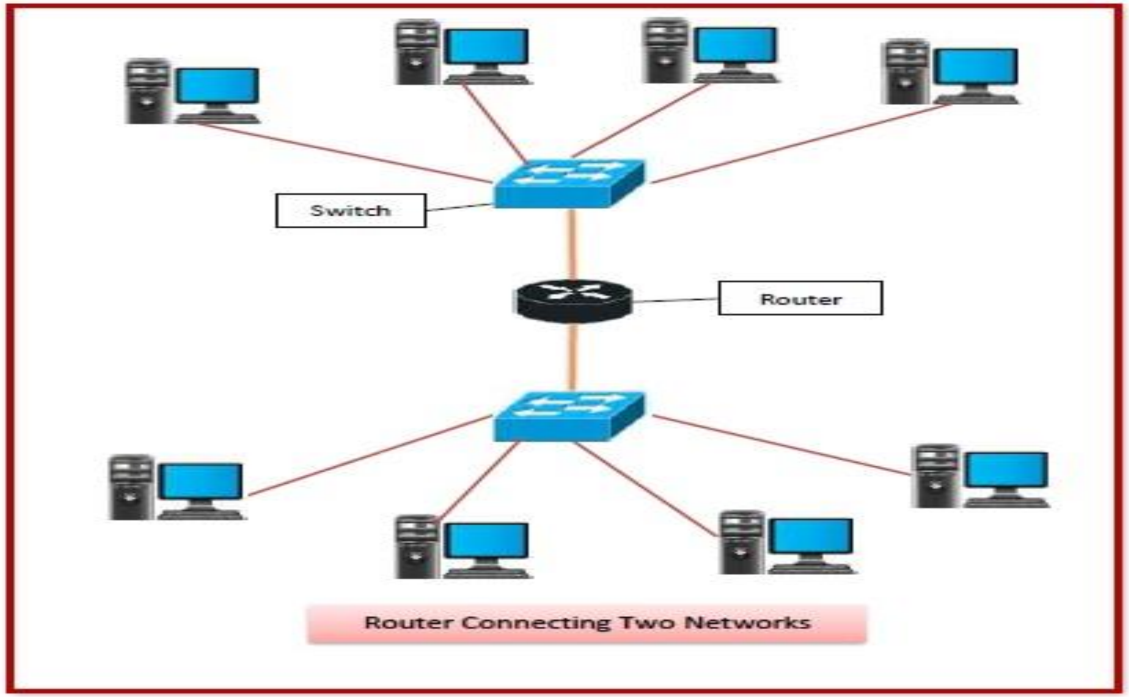
- Switches are networking devices that connect devices in a network to send, receive or forward data packets or data frames over the network.
- A switch has many ports, to which computers are plugged in.
- When a data frame arrives at any port of a network switch, it examines the destination address, performs necessary checks and sends the frame to the corresponding device(s).



- It is an intelligent network device.
- It is a multiport network bridge.
- It uses MAC addresses to send data packets to selected destination ports.
- It uses packet switching technique to receive and forward data packets from the source to the destination device.
- It is supports unicast (one-to-one), multicast (one-to-many) and broadcast (one-to-all) communications.
- Switches can perform some error checking before forwarding data to the destined port.

5) Router

- Routers are responsible for receiving, analyzing, and forwarding data packets among the connected computer networks.
- When a data packet arrives, the router inspects the destination address, consults its routing tables to decide the optimal route and then transfers the packet along this route.



- It connects different networks together and sends data packets from one network to another.
- A router can be used both in LANs (Local Area Networks) and WANs (Wide Area Networks).
- It transfers data in the form of IP packets.
- In order to transmit data, it uses IP address mentioned in the destination field of the IP packet.
- Routers have a routing table in it that is refreshed periodically according to the changes in the network.
- In order to transmit data packets, it consults the table and uses a routing protocol.
- In order to prepare or refresh the routing table, routers share information among each other.
- The functioning of a router depends largely upon the routing table stored in it.
- The routing table stores the available routes for all destinations.
- The router consults the routing table to determine the optimal route through which the data packets can be sent.
- Routers are more expensive than other networking devices like hubs, bridges and switches.
- It is fast and supports speed of up to 10 Gbps.

6) Brouters –

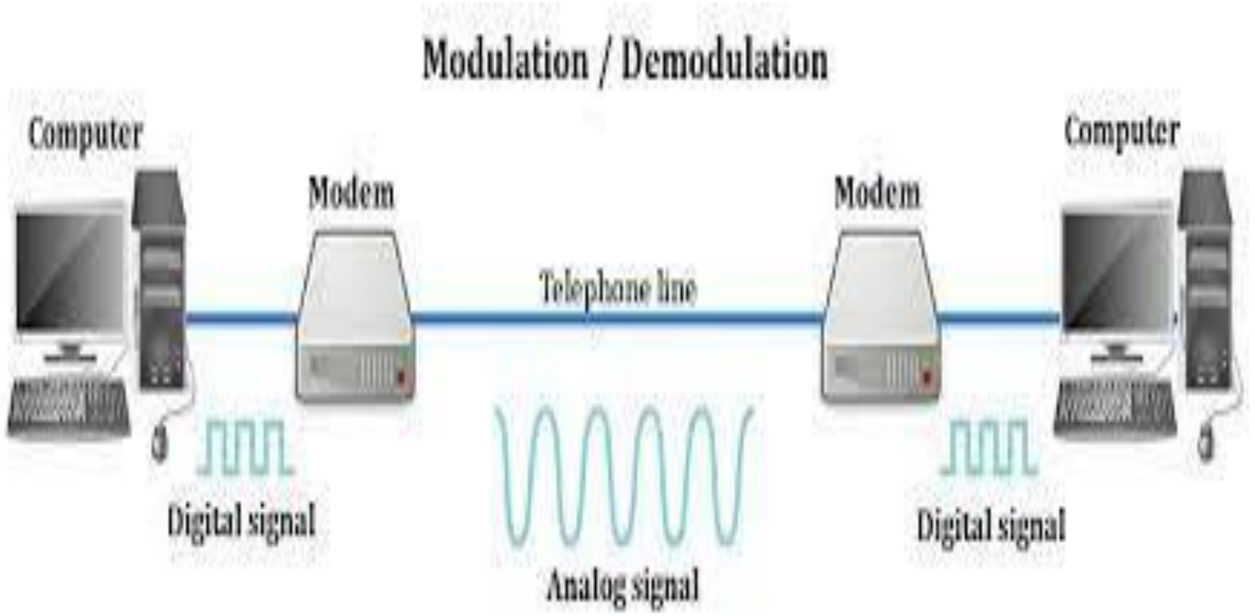
- Brouters are specialized routers that can provide the functionalities of bridges as well.
- It is also known as the bridging router is a device that combines features of both bridge and router.
- Like a bridge, Brouters help to transfer data between networks.
- They route the data within the devices of a network.

7) Gateway

- A gateway, as the name suggests, is a passage to connect two networks together that may work upon different networking models.
- They basically work as the messenger agents that take data from one system, interpret it, and transfer it to another system.
- Gateways are also called protocol converters and can operate at any network layer.
- Gateways are generally more complex than switches or routers.
- Gateway is also called a protocol converter.

Modem

- It stands for Modulation and Demodulation.
- It converts digital signals to analog signals.
- Digital symbols cannot be passed on analog lines therefore digital symbols (1 and 0) are converted into analog signals.
- This process is called modulation.
- The same way, analog signals can't be sent on digital mediums, therefore analog signals are turned into digital signals.
- This process is called De-modulation.
- There is a device to perform both the process- Modulation and Demodulation which is called Modem.
- Modem is the short form of Modulation and Demodulation.
- Modem is useful even when signals are weak because modem enhances speed of data signals for data transmission at distant places.
- It increases the speed before transmission of data signals.
- Today, fiber optic modem are also available which can convert digital signals into optical signals which can make data communication in Fiber Optic Cables possible.



- Modems are available in different transmission speeds, which are measured in bps (bits per second).
- Standard modems speeds are 9600 bps, 14400 bps, 28000 bps, 33600 bps, 56800 bps.

Functions of a modem -

a) <u>Data Compression</u>:

- To decrease the amount of time when it try to send data and for cutting down on the percentages of errors in the all flowing of signals, then modem required the data compression mechanism.
- So, this data compression method helps to reduce the size of signals, which are required for sending data.

b) <u>Error Correction</u>:

- In the error correction techniques, all devices monitor all information while receiving is undamaged.
- It splits all information into small units that is called the “**Frames**“.
- In this process, it tags all frames along with checksums, but it is done before sending information.
- Checksum is a special technique that helps to check redundancy in the presented data in the computer.
- If, this information matches with checksums then device grabs the verified information that is sent by error-correcting modem.
- But, if it gets to fail in matching with checksum then information is moved back.

c) **Modulate Signals**:

- The main function of modem is to transmit and decode all signals which allow sending digital data from one node to other nodes.

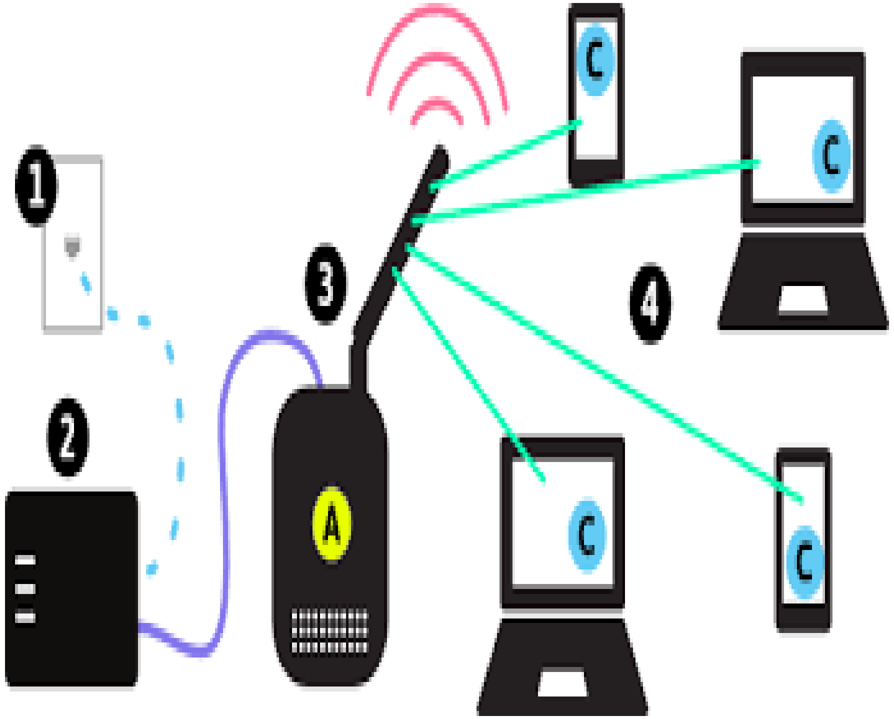
d) **Flow Control**:

- Each modem has different speed of sending signals.
- This can generate issues during receiving the signals if any one of the device’s speed is slow.
- So, in the flow control technique, faster signals are paused, by sending a ‘character’.
- If, slow device will send a character to faster modem, then this character would be a signal to the faster modem for pausing the information transfer until the slow modem gets caught up.

WIFI NETWORK

- Wi-Fi is a wireless technology used to connect computers, tablets, smartphones and other devices to the internet.
- Wi-Fi is the radio signal sent from a wireless router to a nearby device, which translates the signal into data you can see and use.
- The device transmits a radio signal back to the router, which connects to the internet by wire or cable.
- A Wi-Fi network is simply an internet connection that is shared with multiple devices in a home or business via a wireless router.
- The router is connected directly to your internet modem and acts as a hub to broadcast the internet signal to all your Wi-Fi enabled devices.
- This gives you flexibility to stay connected to the internet as long as you are within your network coverage area.
- Wi-Fi uses radio waves to transmit data from your wireless router to your Wi-Fi enabled devices like your TV, smartphone, tablet and computer.
- Since they communicate with each other through air, the devices and personal information can become vulnerable to hackers, cyber-attacks and other threats.

- This is especially true when you connect to a public Wi-Fi network at places like a coffee shop or airport.
- When possible, it is best to connect to a wireless network that is password-protected or a personal hotspot.
- Wi-Fi refers to Wireless Fidelity.



INTRODUCTION TO BLUETOOTH AND INFRARED DEVICES

1) BLUETOOTH

- Bluetooth is used to transfer data using radio waves.
- It is used to transfer data on a particular frequency of 2.4 gigahertz.
- It is used to send data from one device to another.
- It is known as a wireless technology.
- It is used for the wireless communication between the two devices.
- It is used to send data on a short distance.
- The maximum range of Bluetooth is 10 meters.
- The data rate ranges from 1 mbps and 3 mbps.
- The common effective speed is 3 mbps.
- Bluetooth is mostly used in mobile devices.
- Bluetooth uses Radio waves for the transmission of data instead of light.
- The communicating devices can be placed anywhere within the effective range.

Bluetooth Devices

2) INFRARED

- Infrared is the wireless technology that is commonly used for wireless communication between electronic devices.
- It uses wireless infrared pulses for transmission of data.
- These pulses are not seen by the human eye but can be detected by a sensor for receiving data.
- It is a very effective technique used in a different applications.
- Effective range for infrared is very short.
- It is used to transfer data not more than 5 meters, and often closer to each other.
- The data rate ranges from 115 kbps and 15 mbps depending upon the type of devices and also depends upon the position of the devices.
- The battery used in infrared devices run for a long time
- It has a faster response time.
- Infrared waves are damaged by dust Smoke, etc.
- It requires line-of-sight between the sender and receiver.

Infrared Devices

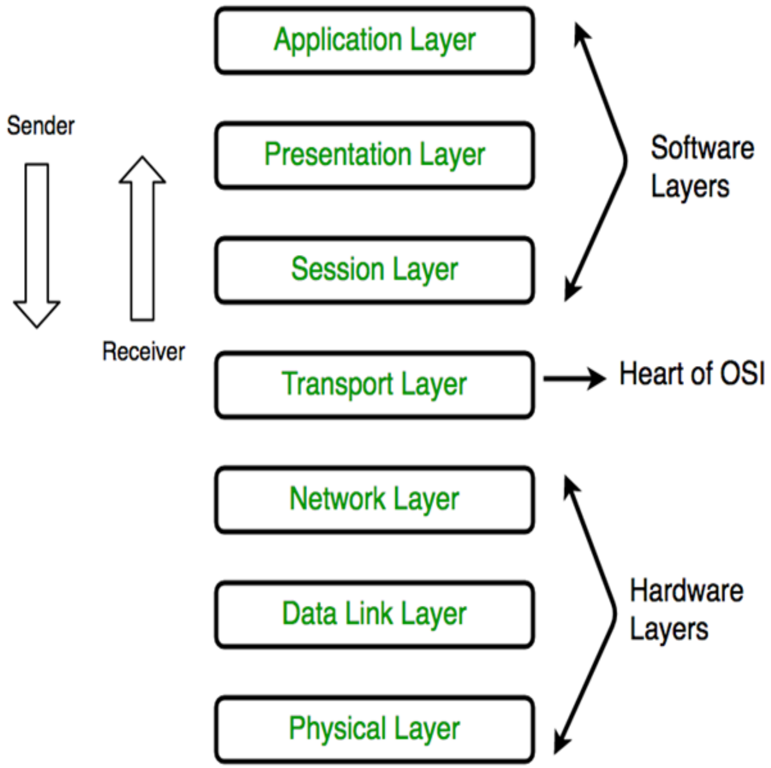
METRAVI PIR-1
36.5°C
MEASUREMENT USING PALM INDUCTION
METRAVI PIR-1
36.5°C
MEASUREMENT USING WRIST THERMOMETRY

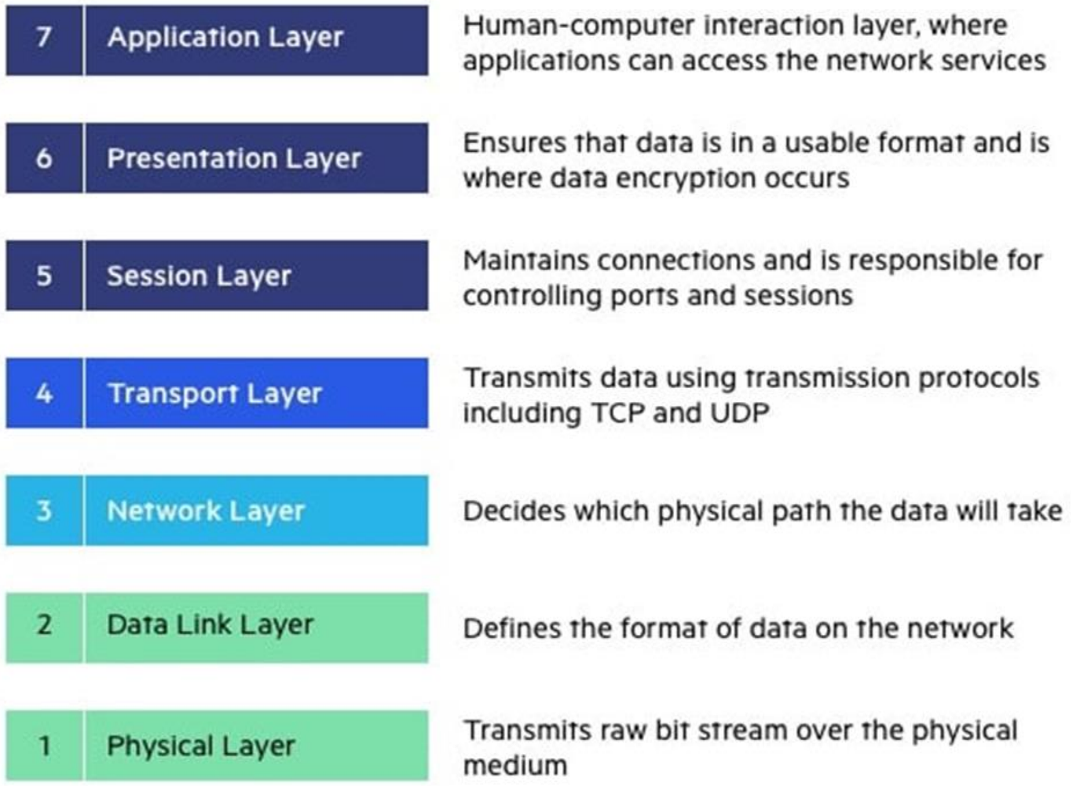
Comparison between Bluetooth and Infrared

Bluetooth	**Infrared**
Bluetooth uses radio waves	Infrared uses pulses of infrared light that are not visible to eyes
Bluetooth sends data over 10 meters	Infrared transfer data over not more than 5 meters
Communicating devices can be placed anywhere in the effective range	Communicating devices must be close to each other
It has less data transmission speed than IR	It has maximum data transmission speed
It is mostly used in mobile phones for data transmission	It is mostly used in electronic devices
It needs no line of sight.	It needs line of sight or point to point transmission

OSI MODEL- Open System Interconnection

- OSI model is a standard model that can allow two different kinds of systems to communicate with each other whether their architectures are the same or different.
- OSI model is considered a complete communication model because it can cover all aspects of data communication.
- 7 layers of OSI models are very famous in data communication.
- All these layers perform a specific task in data communication.
- OSI model is also known as the reference model.

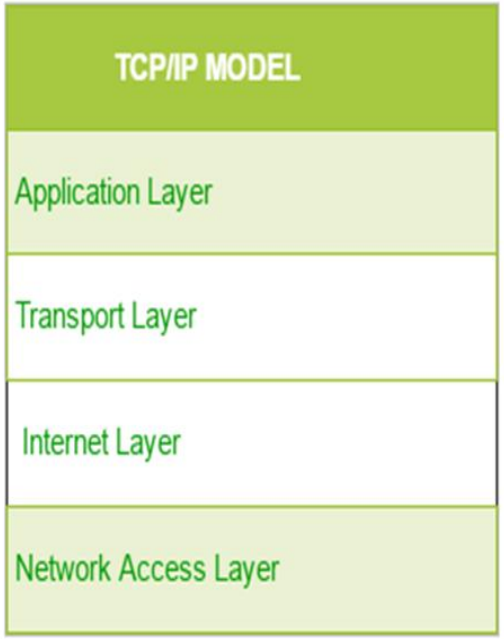




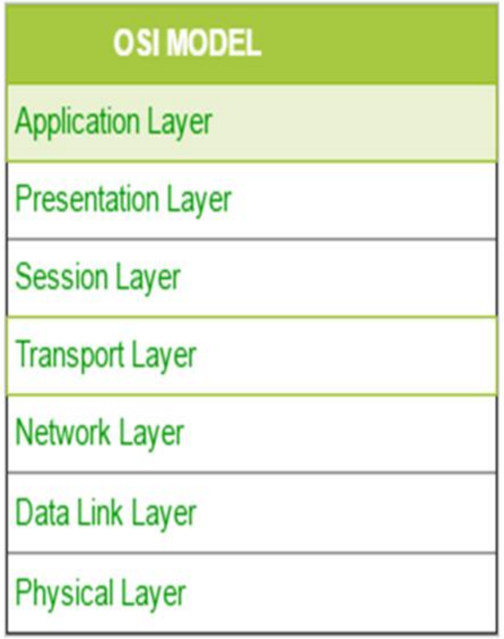
7	Application Layer	Human-computer interaction layer, where applications can access the network services
6	Presentation Layer	Ensures that data is in a usable format and is where data encryption occurs
5	Session Layer	Maintains connections and is responsible for controlling ports and sessions
4	Transport Layer	Transmits data using transmission protocols including TCP and UDP
3	Network Layer	Decides which physical path the data will take
2	Data Link Layer	Defines the format of data on the network
1	Physical Layer	Transmits raw bit stream over the physical medium

NETWORK PROTOCOL - TCP/IP PROTOCOLS

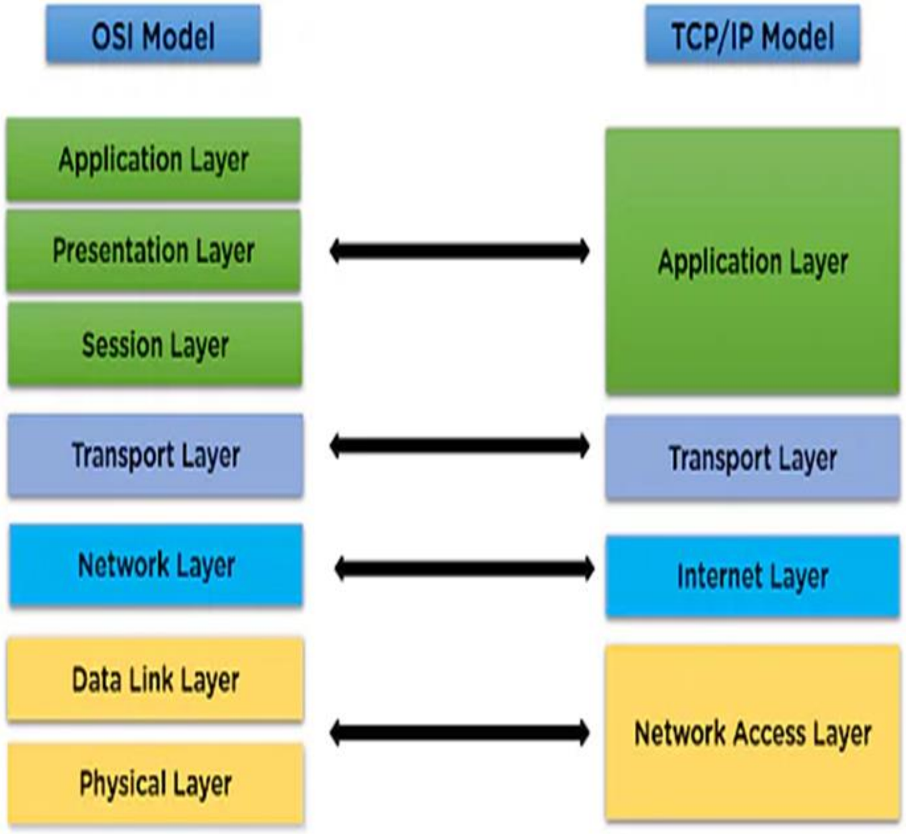
- The TCP/IP model is not exactly similar to the OSI model.
- The TCP/IP model consists of four layers: the application layer, transport layer, internet layer, and network access layer.
- TCP/IP model, it was designed and developed by Department of Defense (DoD) in 1960s and is based on standard protocols.
- The diagrammatic comparison of the TCP/IP and OSI model is as follows :



TCP/IP MODEL
Application Layer
Transport Layer
Internet Layer
Network Access Layer



OSI MODEL
Application Layer
Presentation Layer
Session Layer
Transport Layer
Network Layer
Data Link Layer
Physical Layer



OSI Model

TCP/IP Model

Application Layer

Presentation Layer

Session Layer

Application Layer

Transport Layer

Transport Layer

Network Layer

Internet Layer

Data Link Layer

Physical Layer

Network Access Layer

1) NETWORK ACCESS LAYER

- A network layer is the lowest layer of the TCP/IP model.
- A network layer is the combination of the Physical layer and Data Link layer defined in the OSI reference model.
- It defines how the data should be sent physically through the network.
- This layer is mainly responsible for the transmission of the data between two devices.
- The functions carried out by this layer are encapsulating the IP datagram into frames transmitted by the network and mapping of IP addresses into physical addresses.

2) INTERNET LAYER

- An internet layer is the second layer of the TCP/IP model.
- An internet layer is also known as the network layer.
- The main responsibility of the internet layer is to send the packets from any network, and they arrive at the destination irrespective of the route they take.

Following are the protocols used in this layer are:

1. IP -

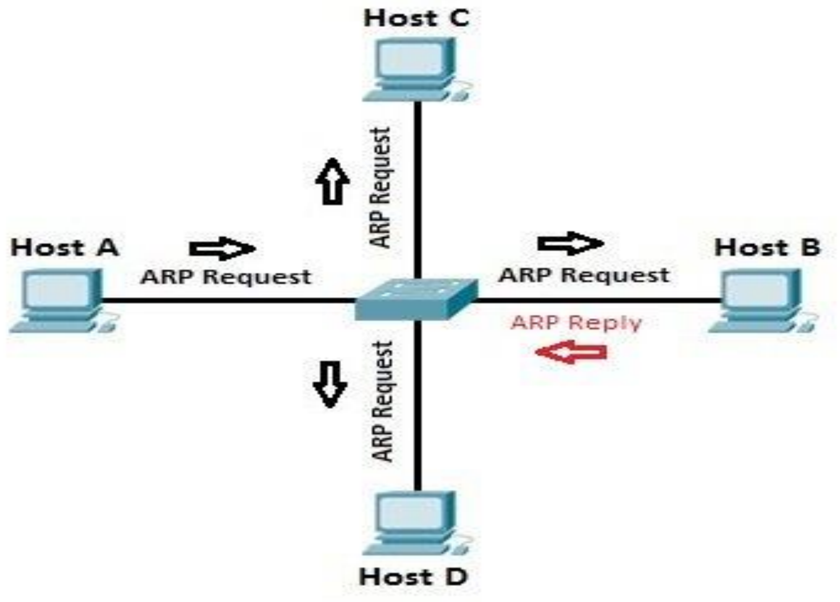
- IP protocol is used in this layer, and it is the most significant part of the entire TCP/IP suite.
- Following are the responsibilities of this protocol:

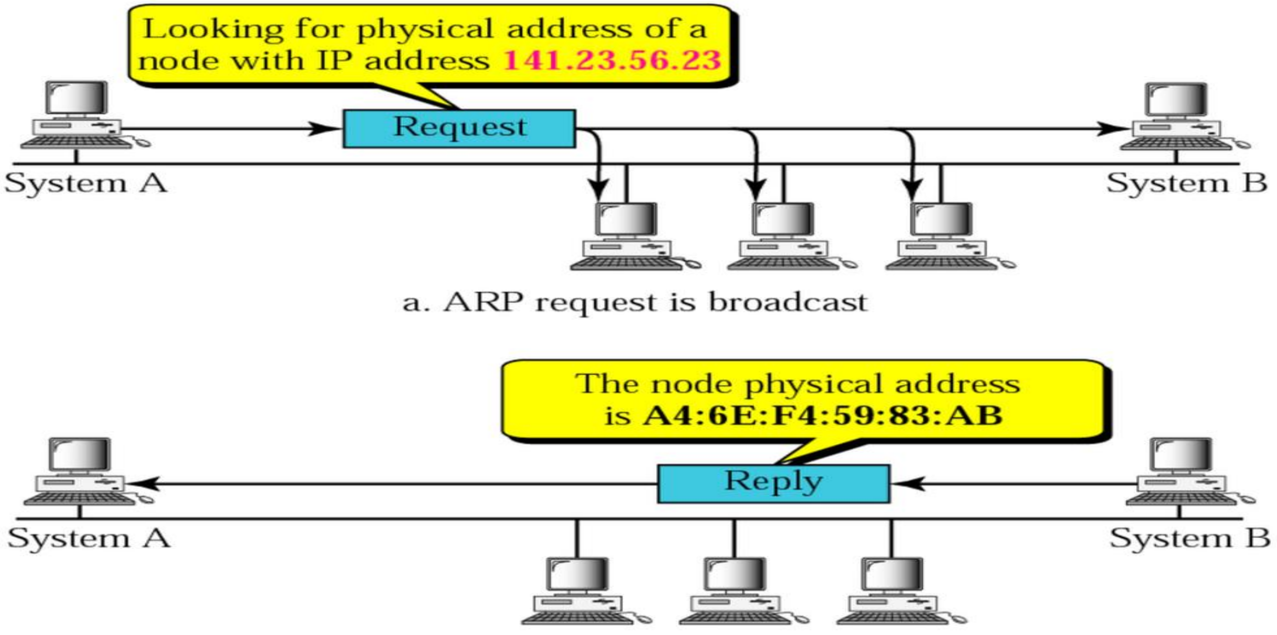
- **IP Addressing:** This protocol implements logical host addresses known as IP addresses. The IP addresses are used by the internet and higher layers to identify the device and to provide internetwork routing.
- **Host-to-host communication:** It determines the path through which the data is to be transmitted.
- **Data Encapsulation and Formatting:** An IP protocol accepts the data from the transport layer protocol. An IP protocol ensures that the data is sent and received securely, it encapsulates the data into message known as IP datagram.
- **Fragmentation and Reassembly:** The limit imposed on the size of the IP datagram by data link layer protocol is known as Maximum Transmission unit (MTU). If the size of IP datagram is greater than the MTU, then the IP protocol splits the datagram into smaller units so that they can travel over the local network. Fragmentation can be done by the sender or intermediate router. At the receiver side, all the fragments are reassembled to form an original message.
- **Routing:** When IP datagram is sent over the same local network such as LAN, MAN, WAN, it is known as direct delivery. When source and destination are on the distant network, then the IP datagram is sent indirectly. This can be accomplished by routing the IP datagram through various devices such as routers.

2. ARP -

- ARP stands for Address Resolution Protocol.
- ARP is a network layer protocol which is used to find the physical address from the IP address.
- The two terms are mainly associated with the ARP Protocol:

- **ARP request:** When a sender wants to know the physical address of the device, it broadcasts the ARP request to the network.
- **ARP reply:** Every device attached to the network will accept the ARP request and process the request, but only recipient recognize the IP address and sends back its physical address in the form of ARP reply. The recipient adds the physical address both to its cache memory and to the datagram header.



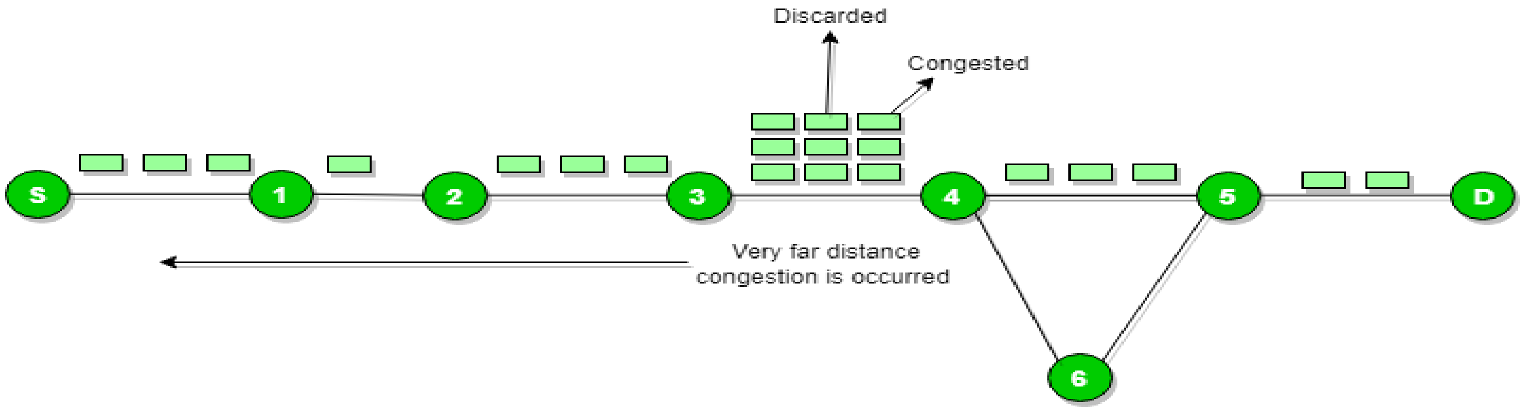

Looking for physical address of a node with IP address 141.23.56.23
Request
System A
System B
The node physical address is A4:6E:F4:59:83:AB
Reply
System A
System B

a. ARP request is broadcast

b. ARP reply is unicast

3. ICMP –

- ICMP stands for Internet Control Message Protocol.
- It is a mechanism used by the hosts or routers to send notifications regarding datagram problems back to the sender.
- A datagram travels from router-to-router until it reaches its destination.
- If a router is unable to route the data because of some unusual conditions such as disabled links, a device is on fire or network congestion, then the ICMP protocol is used to inform the sender that the datagram is undeliverable.



- An ICMP protocol mainly uses two terms:

- **ICMP Test:** ICMP Test is used to test whether the destination is reachable or not.

- **ICMP Reply:** ICMP Reply is used to check whether the destination device is responding or not.

- The core responsibility of the ICMP protocol is to report the problems, not correct them.
- The responsibility of the correction lies with the sender.
- ICMP can send the messages only to the source, but not to the intermediate routers because the IP datagram carries the addresses of the source and destination but not of the router that it is passed to.

3) *TRANSPORT LAYER*

- The transport layer is responsible for the reliability, flow control, and correction of data which is being sent over the network.
- The two protocols used in the transport layer are User Datagram protocol and Transmission control protocol.

1. UDP -

- It stands for User Datagram Protocol.
- It provides connectionless service and end-to-end delivery of transmission.
- It is an unreliable protocol as it does not specify the error.
- User Datagram Protocol discovers the error, and ICMP protocol reports the error to the sender that user datagram has been damaged.

2. TCP -

- It stands for Transmission Control Protocol.
- It creates a virtual circuit between the sender and receiver, and it is active for the duration of the transmission.
- TCP is a reliable protocol as it detects the error and retransmits the damaged frames.
- Therefore, it ensures all the segments must be received and acknowledged before the transmission is considered to be completed.
- At the sending end, TCP divides the whole message into smaller units known as segment, and each segment contains a sequence number which is required for reordering the frames to form an original message.
- At the receiving end, TCP collects all the segments and reorders them based on sequence numbers.

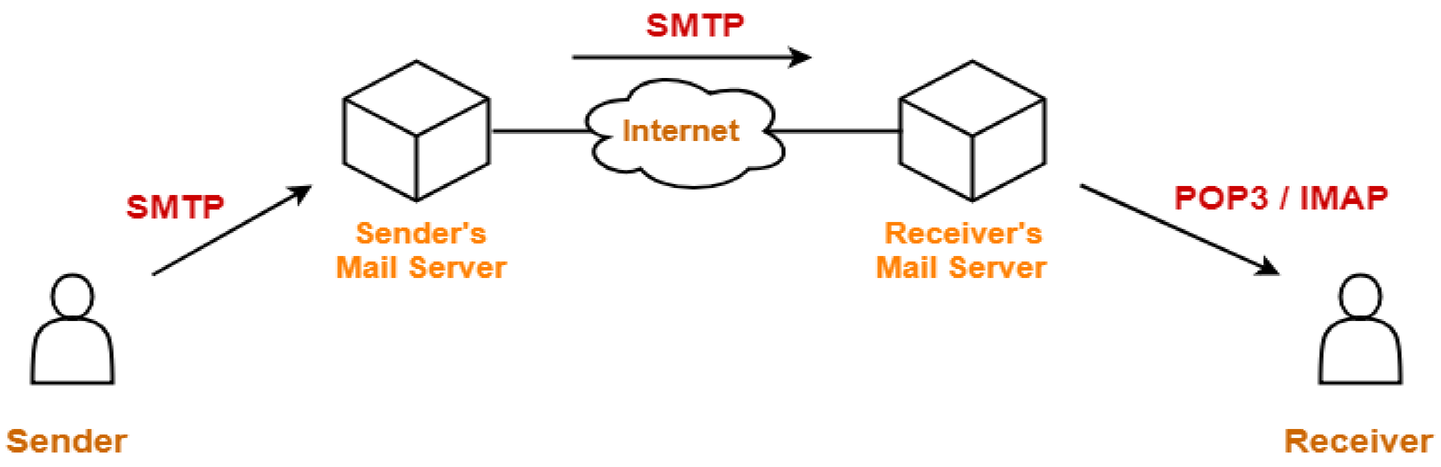
3) APPLICATION LAYER

- An application layer is the topmost layer in the TCP/IP model.
- It is responsible for handling high-level protocols, issues of representation.
- This layer allows the user to interact with the application.
- When one application layer protocol wants to communicate with another application layer, it forwards its data to the transport layer.
- There is an ambiguity occurs in the application layer.
- Every application cannot be placed inside the application layer except those who interact with the communication system.
- For example: Text editor cannot be considered in application layer while web browser using HTTP protocol to interact with the network where HTTP protocol is an application layer protocol.

Following are the main protocols used in the application layer:

1. SMTP -

- SMTP stands for Simple Mail Transfer Protocol.
- SMTP is a set of communication guidelines that allow software to transmit an electronic mail over the internet is called Simple Mail Transfer Protocol.
- It is a program used for sending messages to other computer users based on e-mail addresses.
- The main purpose of SMTP is used to set up communication rules between servers.
- The servers have a way of identifying themselves and announcing what kind of communication they are trying to perform.
- They also have a way of handling the errors such as incorrect email address.
- For example, if the recipient address is wrong, then receiving server reply with an error message of some kind.



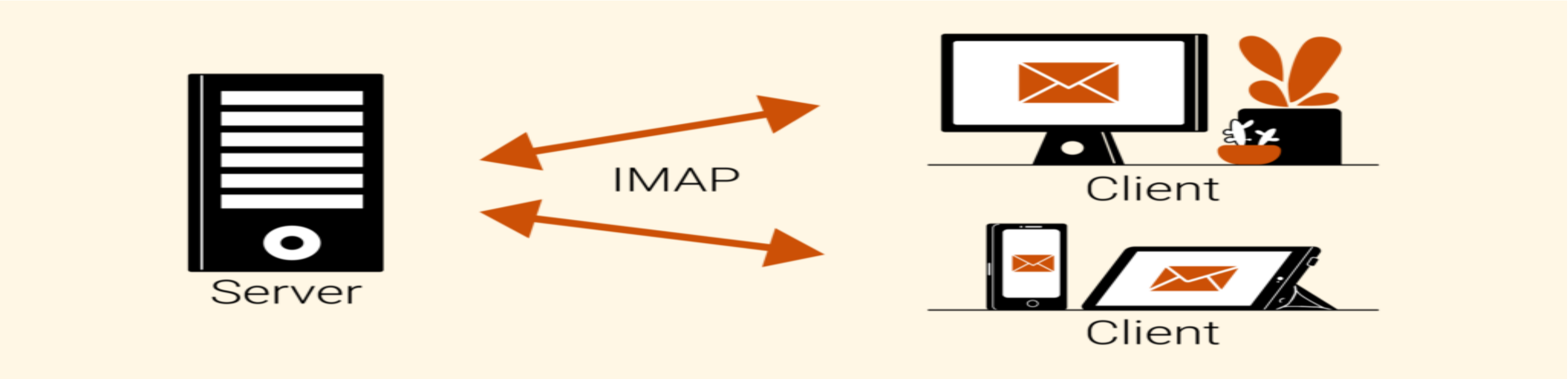
2) MULTIPURPOSE INTERNET MAIL EXTENSION (MIME) PROTOCOL

- MIME is a kind of add-on or a supplementary protocol that allows non-ASCII data to be sent through SMTP.
- It allows the users to exchange different kinds of data files on the Internet: audio, video, images, etc.

3) IMAP

- IMAP stands for Internet Message Access Protocol.
- It is an application layer protocol which is used to receive the emails from the mail server.
- As an incoming email protocol, IMAP functions as the intermediary between the email server and email client.
- When users read an email using IMAP, they read them off the server.
- They don't actually download or store the email on their local device.
- This means that the email is not tied to a particular device, and users can access it from any location in the world using different devices.
- The IMAP protocol synchronizes all the devices with the main server.
- Let's suppose we have three devices desktop, mobile, and laptop as shown in the above figure.
- If all these devices are accessing the same mailbox, then it will be synchronized with all the devices.
- Here, synchronization means that when mail is opened by one device, then it will be marked as opened in all the other devices, if we delete the mail, then the mail will also be deleted from all the other devices.

- So, we have synchronization between all the devices.
- In IMAP, we can see all the folders like spam, inbox, sent, etc.
- We can also create our own folder known as a custom folder that will be visible in all the other devices.

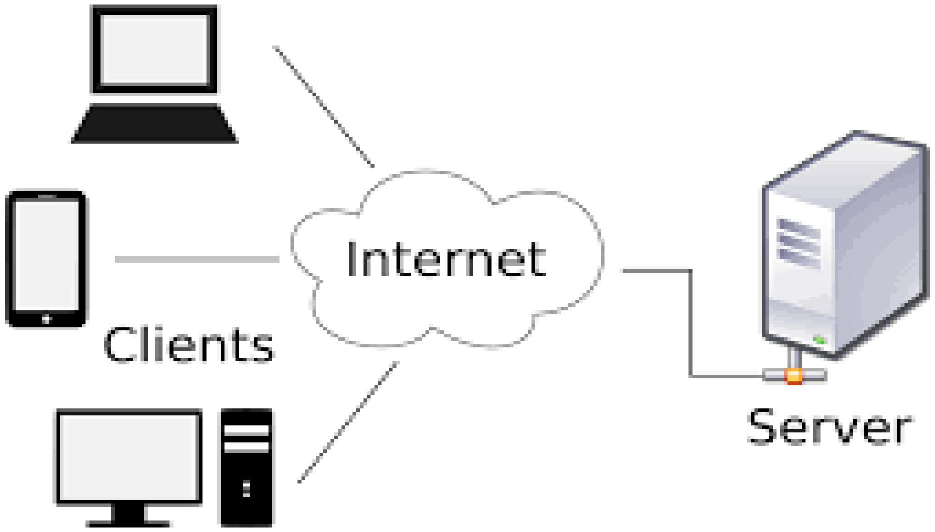


4) POP3 PROTOCOL

- Post Office Protocol version 3 (POP3) is a standard mail protocol used to receive emails from a remote server to a local email client.
- POP3 allows you to download email messages on your local computer and read them even when you are offline.
- Note, that when you use POP3 to connect to your email account, messages are downloaded locally and removed from the email server.
- This means that if you access your account from multiple locations that may not be the best option for you.

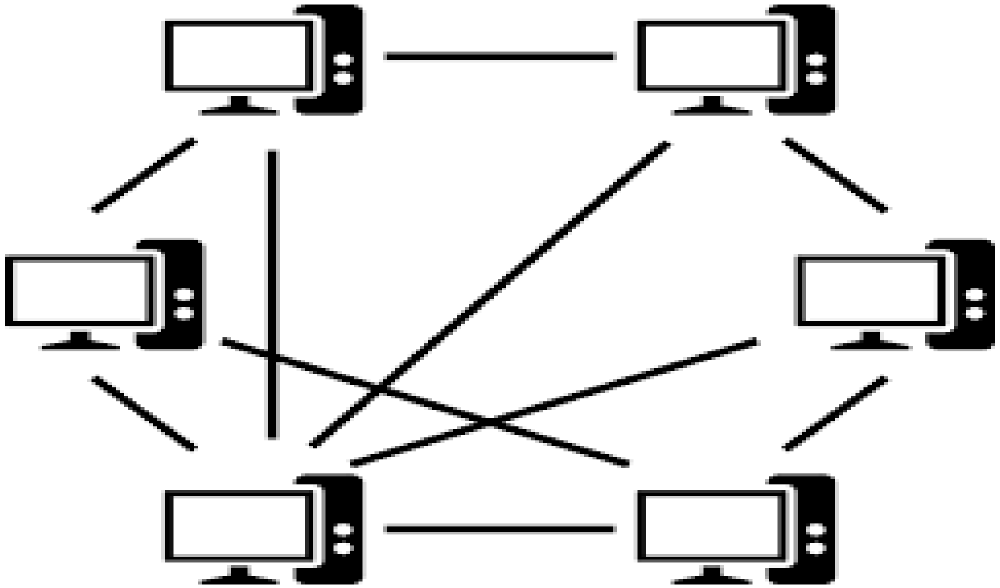
CLIENT-SERVER NETWORK

- This model is a broadly used network model.
- In Client-Server Network, Clients and server are differentiated.
- Specific server and clients are present.
- Centralized server is used to store the data because its management is centralized.
- In this, server responds the services which is requested by the Client.



PEER-TO-PEER NETWORK

- This model does not differentiate the clients and the servers.
- In this, each and every node is itself a client and a server.
- In Peer-to-Peer Network, each and every node can do both request and respond for the services.



DIFFERENCE BETWEEN CLIENT-SERVER AND PEER-TO-PEER NETWORK:

Basis of Comparison	Client-Server Network	Peer-to-Peer Network
Basic	In a client-server network, we have a specific server and specific clients connected to the server.	In a peer-to-peer network, clients are not distinguished; every node act as a client and server.
Expense	A Client-Server network is more expensive to implement.	A Peer-to-Peer is less expensive to implement.
Stability	It is more stable and scalable than a peer-to-peer network.	It is less stable and scalable.
Data	In a client-server network, the data is stored in a centralized server.	In a peer-to-peer network, each peer has its own data.
Server	A server may get overloaded when many customers make simultaneous service requests.	A server is not bottlenecked (choked/ stopped) since the services are distributed among numerous servers using a peer-to-peer network.

Basis of Comparison	**Client-Server Network**	**Peer-to-Peer Network**
Focus	Sharing the information.	Connectivity.
Service	The server provides the requested service in response to the client's request.	Each node has the ability to both request and delivers services.
Performance	Because the server does the bulk of the work, performance is unaffected by the growth of clients.	Because resources are shared in a big peer-to-peer network, performance will likely to suffer.
Security	A Client-Server network is a secured network because the server can verify a client's access to any area of the network, making it secure.	The network's security deteriorates, and its susceptibility grows as the number of peers rises.