UNIT I
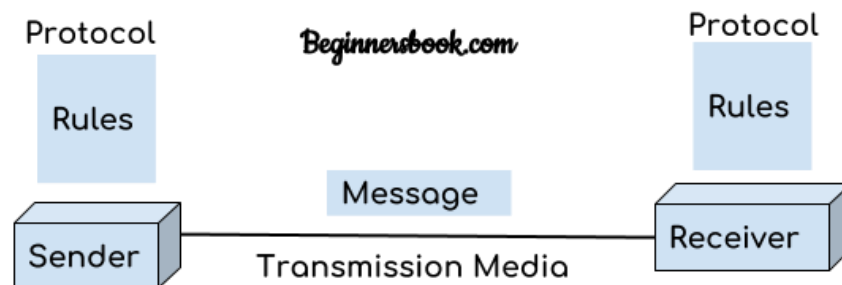
Computer Network

- ➢ A computer network is a group of devices connected with each other through a transmission medium such as wires, cables etc.
- ➢ These devices can be computers, printers, scanners, Fax machines etc.
- ➢ The purpose of having computer network is to send and receive data stored in other devices over the network.
- ➢ These devices are often referred as nodes.

There are **five basic components** of a computer network

Message: It is the data or information which needs to be transferred from one device to another device over a computer network.

- • **Sender**: Sender is the device that has the data and needs to send the data to other device connected to the network.
- • **Receiver**: A receiver is the device which is expecting the data from other device on the network.
  Transmission media: In order to transfer data from one device to another device we need a transmission media such as wires, cables, radio waves etc.
- • **Protocol**: A protocol is a set of rules that are agreed by both sender and receiver, without a protocol two devices can be connected to each other but they cannot communicate. In order to establish a reliable communication or data sharing between two different devices we need set of rules that are called protocol. For example, http and https are the two protocols used by web browsers to get and post the data to internet, similarly smtp protocol is used by email services connected to the internet.

Features of a Computer Network
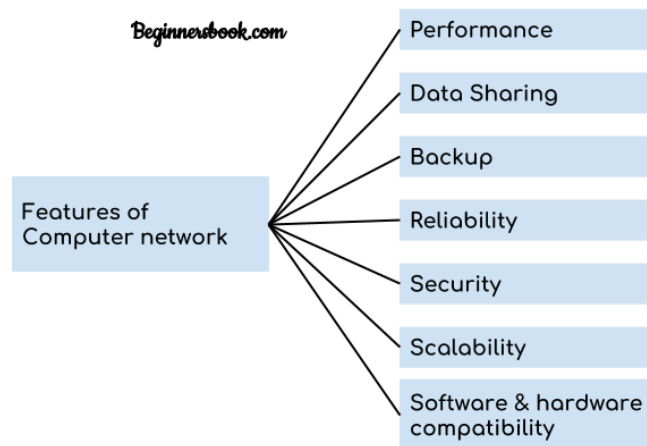
A computer network has following features:

1. **Performance**: Performance of a computer network is measured in terms of response time. The response time of sending and receiving data from one node (computer in a computer network are often referred as node) to another should be minimal.
2. **Data Sharing**: One of the reason why we use a computer network is to share the data between different systems connected with each other through a transmission media.
3. **Backup**: A computer network must have a central server that keeps the backup of all the data that is to be shared over a network so that in case of a failure it should be able to recover the data faster.
4. **Software and hardware compatibility**: A computer network must not limit all the computers in a computer network to use same software and hardware, instead it should allow the better compatibility between the different software and hardware configuration.
5. **Reliability**: There should not be any failure in the network or if it occurs the recovery from a failure should be fast.
6. **Security**: A computer network should be secure so that the data transmitting over a network should be safe from unauthorised access. Also, the sent data should be received as it is at the receiving node, which means there should not be any loss of data during transmission.
7. **Scalability**: A computer network should be scalable which means it should always allow to add new computers (or nodes) to the already existing computer network. For example, a company runs 100 computers over a computer network for their 100 employees, lets say they hire another 100 employees and want to add new 100 computers to the already existing LAN then in that case the local area computer network should allow this.
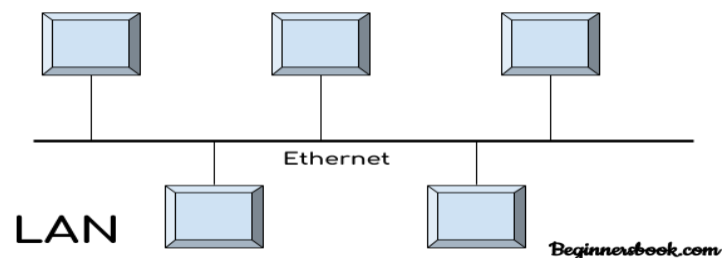
Types of Computer Network
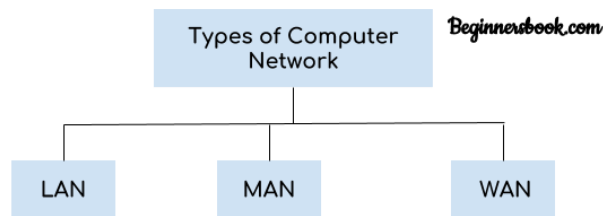
There are mainly three types of computer networks based on their size:
1. Local Area Network (LAN)
2. Metropolitan Area Network (MAN)
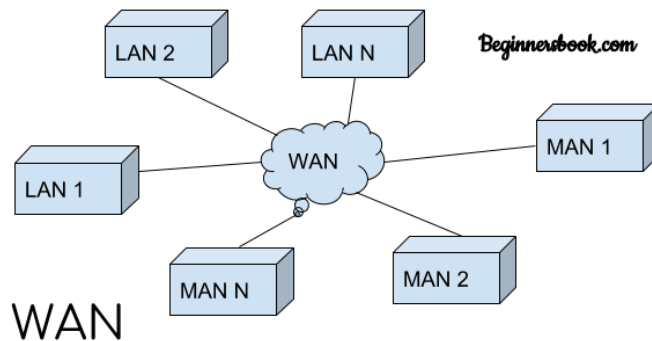3. Wide area network (WAN)

1. Local Area Network (LAN)

1. Local area network is a group of computers connected with each other in a small places such as school, hospital, apartment etc.
2. LAN is secure because there is no outside connection with the local area network thus the data which is shared is safe on the local area network and can't be accessed outside.
3. LAN due to their small size are considerably faster, their speed can range anywhere from 100 to 100Mbps.
4. LANs are not limited to wire connection, there is a new evolution to the LANs that allows local area network to work on a wireless connection.

2. Metropolitan Area Network (MAN)
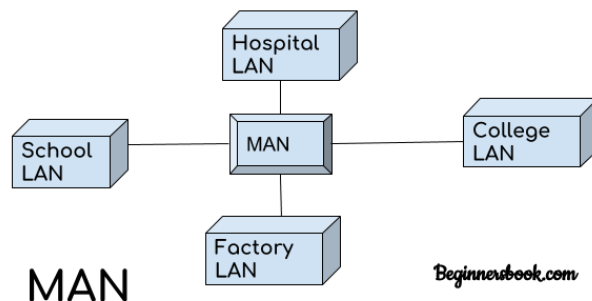
MAN network covers larger area by connections LANs to a larger network of computers. In Metropolitan area network various Local area networks are connected with each other through telephone lines. The size of the Metropolitan area network is larger than LANs and smaller than WANs(wide area networks), a MANs covers the larger area of a city or town.

3. Wide area network (WAN)

Wide area network provides long distance transmission of data. The size of the WAN is larger than LAN and MAN. A WAN can cover country, continent or even a whole world. Internet connection is an example of WAN. Other examples of WAN are mobile broadband connections such as 3G, 4G etc.

Advantages of WAN:

Centralized infrastructure: One of the main advantage of WAN is the that we do not need to maintain the backup and store data on local system as everything is stored online on a data centre, from where we can access the data through WAN.
Privacy: We can setup the WAN in such a way that it encrypts the data that we share online that way the data is secure and minimizes the risk of unauthorized access.
Increased Bandwidth: With the WAN we get to choose the bandwidth based on the need, a large organization can have larger bandwidth that can carry large amount of data faster and efficiently.
Area: A WAN can cover a large area or even a whole world though internet connection thus we can connect with the person in another country through WAN which is not possible is other type of computer networks.

Disadvantages of WAN:

Antivirus: Since our systems are connected with the large amount of systems, there is possibility that we may unknowingly download the virus that can affect our system and become threat to our privacy and may lead to data loss.
Expensive: Cost of installation is very high.
Issue resolution: Issue resolution takes time as the WAN covers large area, it is really difficult to pin point the exact location where the issues raised and causing the problem.
Interconnection of Networks:
We have read LAN, MAN and WAN above, we also talked about internet. You can say that an internet is a combination of LAN, MAN and WAN.

Different Types of Connections
- A network is two or more devices connected through links.
- A link is a communications pathway that transfers data from one device to another.
- 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: point-to-point and multipoint.
 1.Point-to-Point:

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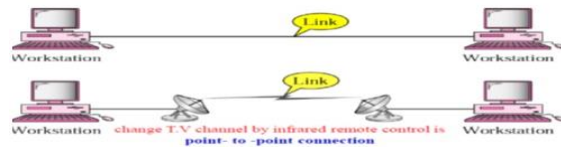
2.Multipoint:

A multipoint (also called multidrop) connection is one in which more than two specific devices share a single link


In a multipoint environment, the capacity of the channel is shared, either spatially or temporally. If several devices can use the link simultaneously, it is a spatially shared connection. If users must take turns, it is a timeshared connection.

Network Topology

Physical or Geometric representation of how the computers are connected to each other is known as topology. There are five types of topology – Mesh, Star, Bus, Ring and Hybrid.
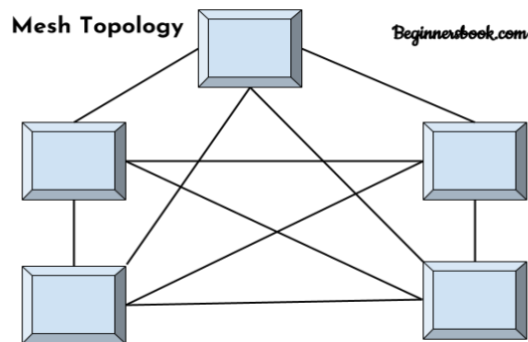
Types of Topology

There are five types of topology in computer networks:
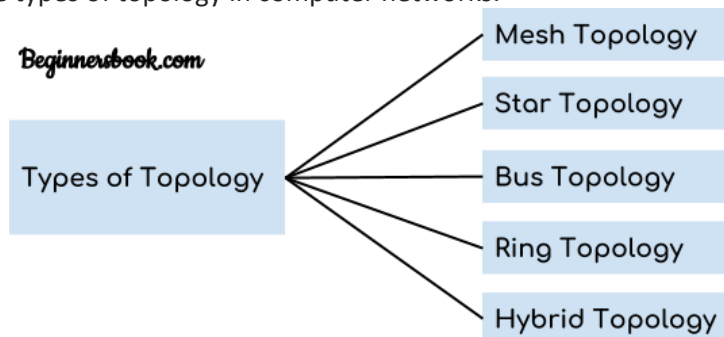
1. Mesh Topology
2. Star Topology
3. Bus Topology

4. Ring Topology
5. Hybrid Topology

Mesh Topology

In mesh topology each device is connected to every other device on the network through a dedicated point-to-point link. When we say dedicated it means that the link only carries data for the two connected devices only. Lets say we have n devices in the network then each device must be connected with (n-1) devices of the network. Number of links in a mesh topology of n devices would be n(n-1)/2.

There are two types of Mesh topology:

1. **Full Mesh Topology:** In this topology each device is connected to the all devices available on the network.
2. **Partial Mesh Topology:** In partial mesh topology, each device is connected to only those devices, to which they communicate frequently. This serves the purpose of mesh topology and saves the cost of redundant connection, where no communication happens and connection is not required.

Advantages of Mesh topology

1. **No data loss:** No data traffic issues as there is a dedicated link between two devices which means the link is only available for those two devices.
2. **Reliable:** Mesh topology is reliable and robust as failure of one link doesn't affect other links and the communication between other devices on the network.
3. **Secure:** Mesh topology is secure because there is a point to point link thus unauthorized access is not possible.
4. **Easy to troubleshoot:** Fault detection is easy as there is a separate connection between each devices.
5. **Fast communication:** As there is a dedication connection between two devices on a network, the communication is fast.

Disadvantages of Mesh topology

1. Amount of wires required to connected each system is tedious and headache.
2. Since each device needs to be connected with other devices, number of I/O ports required must be huge.

3. Scalability issues because a device cannot be connected with large number of devices with a dedicated point to point link.

Star Topology
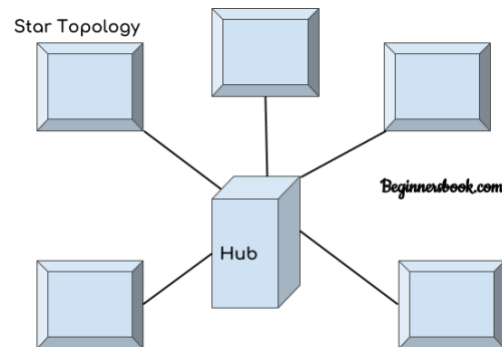
In star topology each device in the network is connected to a central device called **hub**. Unlike Mesh topology, star topology doesn't allow direct communication between devices, a device must have to communicate through hub.
If one device wants to send data to other device, it has to first send the data to hub and then the hub transmit that data to the designated device.
The **central device is known as hub** and **other devices connected to hub are called clients**. Generally Coaxial cable or RJ-45 cables are used to connect the clients to the hub.
**Advantages of Star topology**

1. **Less expensive:** Less expensive because each device only need one I/O port and needs to be connected with hub with one link.
2. **Easier to install**
3. **Cost effective:** Less amount of cables required because each device needs to be connected with the hub only.
4. **Robust:** If one link fails, other links will work just fine.
5. **Easy to troubleshoot:** Easy fault detection because the link can be easily identified.
6. **Reliable:** Each device is separately connected to the hub, so a connection failure between a device and hub doesn't affect the connection of the other devices.
7. **Expendable:** It is easy to add new devices to the network in star topology. This is because a new device just requires a connection to the hub and it can easily communicate with other devices on the network.
Disadvantages of Star topology

1. If hub goes down everything goes down, none of the devices can work without hub.
2. Hub requires more resources and regular maintenance because it is the central system of star topology.

Bus Topology
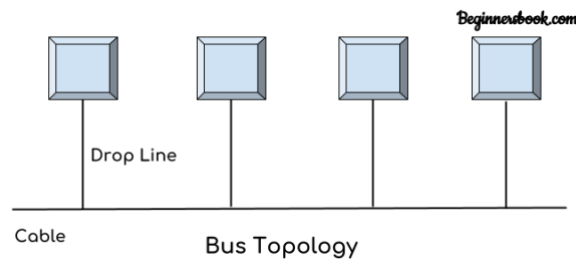
Bus Topology

In bus topology there is a main cable and all the devices are connected to this main cable through drop lines. There is a device called tap that connects the drop line to the main cable. Since all the data is transmitted over the main cable, there is a limit of drop lines and the distance a main cable can have.

- The main cable that is connected to the devices on the network using drop line is called **backbone cable**.
- The main cable **broadcast the message** to all the devices connected to it.
- When a device wants to sends a message, it **transmits the message to the backbone cable**. All the other devices connected to the backbone cable receives the message whether they are intended to receive the message or not.

Advantages of bus topology

1. **Easy installation**, each cable needs to be connected with backbone cable.
2. **Less Expensive: Less cables** are required than Mesh and star topology
3. **Limited failure:** The connection failure of one device doesn't affect the connections of other devices on network.

Disadvantages of bus topology

1. Difficultly in fault detection.
2. **Not scalable** as there is a limit of how many nodes you can connect with backbone cable.
3. **Difficult to troubleshoot:** It is difficult to identify the cause of failure.
4. **Data collision:** When two or more devices send the data simultaneously then there is a chance of data collision.

Ring Topology
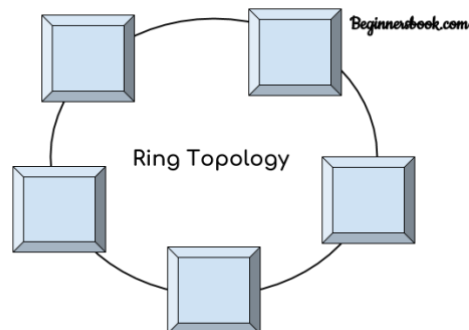
Ring Topology

In ring topology each device is connected with the two devices on either side of it. There are two dedicated point to point links a device has with the devices on the either side of it. This structure forms a ring thus it is known as ring topology.

If a device wants to send data to another device then it sends the data in one direction, each device in ring topology has a repeater, if the received data is intended for other device then repeater forwards this data until the intended device receives it.

- Data flow is **unidirectional** in ring topology.
- This topology doesn't have any end points as nodes are connected in circular fashion.
- The data transfers in ring topology in clockwise direction.

Advantages of Ring Topology

1. Easy to install.
2. Managing is easier as to add or remove a device from the topology only two links are required to be changed.
3. **Less expensive:** Generally Twisted pair cabling is used in ring topology which is inexpensive and easily available.
4. **Easy maintenance:** The network in ring topology is easy to maintain as a system failure doesn't affect other systems on network, the failed system can be easily removed and installed again after fixing the issue.

Disadvantages of Ring Topology

1. A link failure can fail the entire network as the signal will not travel forward due to failure.
2. Data traffic issues, since all the data is circulating in a ring.

Hybrid topology
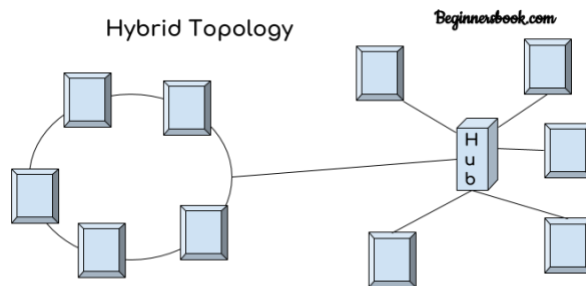
A combination of two or more topology is known as hybrid topology. For example a combination of star and mesh topology is known as hybrid topology.

Advantages of Hybrid topology

1. We can choose the topology based on the requirement for example, scalability is our concern then we can use star topology instead of bus technology.
2. Scalable as we can further connect other computer networks with the existing networks with different topologies.

Disadvantages of Hybrid topology

1. Fault detection is difficult.
2. Installation is difficult.
3. Design is complex so maintenance is high thus expensive.

Tree topology

- Tree topology is an **example of hybrid topology** as it is a combination of **star topology** and **bus topology**.
- The devices are connected to each other in hierarchical manner. Each node has arbitrary number of child nodes. The device at the top of the hierarchy is known as root node and other devices that are lower in hierarchy known as descendants of the root node.
- There is a single path between two devices and this is the path of the communication between devices.
- Tree topology is also called **star-bus topology**.

Advantages of Tree topology

1. Easy error detection.
2. **Expendable:** It is easy to add new devices to the network in tree topology.
3. **Easy maintenance:** Devices are grouped in small star networks and these star networks are connected to each other using bus topology. It is easy to manage a device in small star network.
4. **Reliable:** One system failure doesn't bring the whole network down. The failed system can be easily managed.
5. **Supports broadband transmissions:** It supports broadband transmission that is reason this topology is frequently used in corporate networks.

Disadvantages of Tree topology

1. **Cost:** Cost of broadband transmission is high.
2. **Dependant on backbone cable of bus topology:** All the devices connected in star networks are connected with other devices using backbone cable of bus topology. Failure in this main cable can affect the whole network.

The Network Edge

Computers and other devices connected to the Internet are often referred to as *end systems* as they sit at the edge of the Internet. They are also called *hosts*

A host can be classified as

Client: refers to the computer system that requests for the completion of the task.

Server: refers to the computer system that receives requests from the clients & processes them. After processing ,the server sends reply to the client who sent the request.

The concept of client and server is essential in network design. The various network design models or network architecture are 1. Peer to Peer
                                2. Client- Server

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:
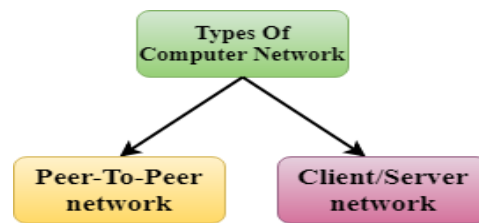
o   Peer-To-Peer network
o   Client/Server network

Peer-To-Peer network

o   Peer-To-Peer network is a network in which all the computers are linked together with equal privilege and responsibilities for processing the data.
o   Peer-To-Peer network is useful for small environments, usually up to 10 computers.
o   Peer-To-Peer network has no dedicated server.
o   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.
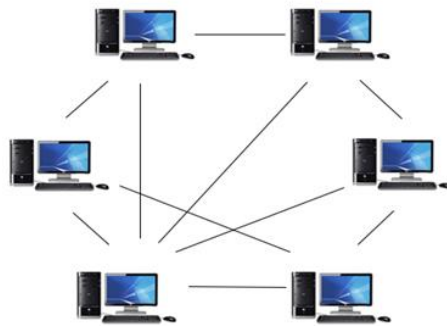
Advantages Of Peer-To-Peer Network:

o   It is less costly as it does not contain any dedicated server.
o   If one computer stops working but, other computers will not stop working.
o   It is easy to set up and maintain as each computer manages itself.

Disadvantages Of Peer-To-Peer Network:

o   In the case of Peer-To-Peer network, it does not contain the centralized system . Therefore, it cannot back up the data as the data is different in different locations.
o   It has a security issue as the device is managed itself.

Client/Server Network

o   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.
o   The central controller is known as a **server** while all other computers in the network are called **clients**.
o   A server performs all the major operations such as security and network management.

- o   A server is responsible for managing all the resources such as files, directories, printer, etc.
- o   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.
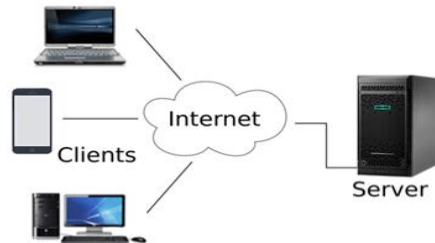
Advantages Of Client/Server network:

- o   A Client/Server network contains the centralized system. Therefore we can back up the data easily.
- o   A Client/Server network has a dedicated server that improves the overall performance of the whole system.
- o   Security is better in Client/Server network as a single server administers the shared resources.
- o   It also increases the speed of the sharing resources.

Disadvantages Of Client/Server network:

- o   Client/Server network is expensive as it requires the server with large memory.
- o   A server has a Network Operating System(NOS) to provide the resources to the clients, but the cost of NOS is very high.
- o   It requires a dedicated network administrator to manage all the resources.

The Network Core

Network core defines the connection of different network segments and the process to transmit data packets across the network.
The network core is implemented using switching techniques.

Switching:

Computer network is a group of connected devices. The main challenge we face in a computer network is – how to connect devices to make one to one communication possible between each devices. One thing we can do is to connect each device with every other device in the network like we do in Mesh Topology , however this approach is neither practical nor cost-efficient as most of the links in the network would remain idle. The better solution is **Switching** , switching is used to make an efficient computer network that allows one to one communication between each devices.

Switching modes:
There are three types of switching modes:

- o   Store-and-forward

- o Cut-through
- o Fragment-free
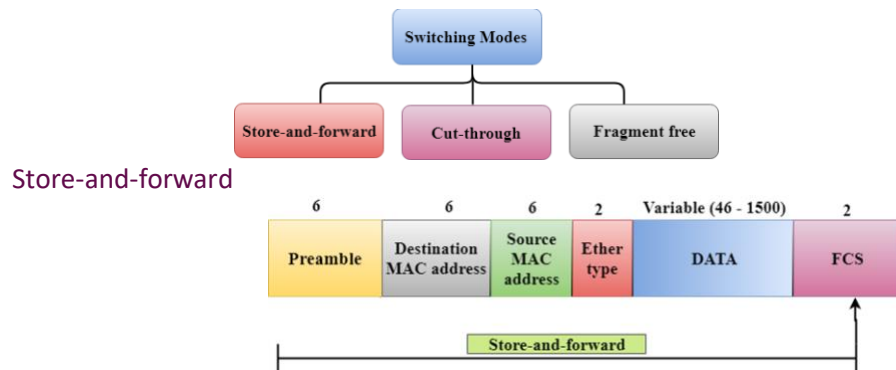
Store-and-forward

- o Store-and-forward is a technique in which the intermediate nodes store the received frame and then check for errors before forwarding the packets to the next node.
- o The layer 2 switch waits until the entire frame has received. On receiving the entire frame, switch store the frame into the switch buffer memory. This process is known as **storing the frame**.
- o When the frame is stored, then the frame is checked for the errors. If any error found, the message is discarded otherwise the message is forwarded to the next node. This process is known as **forwarding the frame**.
- o CRC (Cyclic Redundancy Check) technique is implemented that uses a number of bits to check for the errors on the received frame.
- o The store-and-forward technique ensures a high level of security as the destination network will not be affected by the corrupted frames.
- o Store-and-forward switches are highly reliable as it does not forward the collided frames.
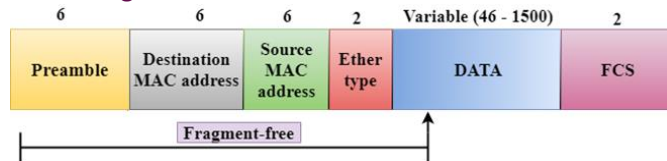
Cut-through Switching

- o Cut-through switching is a technique in which the switch forwards the packets after the destination address has been identified without waiting for the entire frame to be received.
- o Once the frame is received, it checks the first six bytes of the frame following the preamble, the switch checks the destination in the switching table to determine the outgoing interface port, and forwards the frame to the destination.
- o It has **low latency** rate as the switch does not wait for the entire frame to be received before sending the packets to the destination.
- o It has no **error checking technique**. Therefore, the errors can be sent with or without errors to the receiver.

- o A Cut-through switching technique has **low wait time** as it forwards the packets as soon as it identifies the destination MAC address.
- o In this technique, collision is not detected, if frames have collided will also be forwarded.

Fragment-free Switching

- o A Fragment-free switching is an advanced technique of the Cut-through Switching.
- o A Fragment-free switching is a technique that reads atleast 64 bytes of a frame before forwarding to the next node to provide the error-free transmission.
- o It combines the speed of Cut-through Switching with the error checking functionality.
- o This technique checks the 64 bytes of the ethernet frame where addressing information is available.
- o A collision is detected within 64 bytes of the frame, the frames which are collided will not be forwarded further.

Switching techniques

In large networks, there can be multiple paths from sender to receiver. The switching technique will decide the best route for data transmission.
Switching technique is used to connect the systems for making one-to-one communication.

Classification Of Switching Techniques
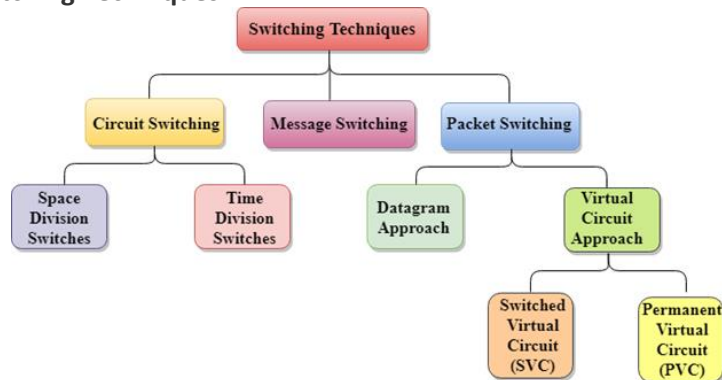
Circuit Switching

- o Circuit switching is a switching technique that establishes a dedicated path between sender and receiver.
- o In the Circuit Switching Technique, once the connection is established then the dedicated path will remain to exist until the connection is terminated.
- o Circuit switching in a network operates in a similar way as the telephone works.
- o A complete end-to-end path must exist before the communication takes place.

- o In case of circuit switching technique, when any user wants to send the data, voice, video, a request signal is sent to the receiver then the receiver sends back the acknowledgment to ensure the availability of the dedicated path. After receiving the acknowledgment, dedicated path transfers the data.
- o Circuit switching is used in public telephone network. It is used for voice transmission.
- o Fixed data can be transferred at a time in circuit switching technology.

Communication through circuit switching has 3 phases:

- o Circuit establishment
- o Data transfer
- o Circuit Disconnect
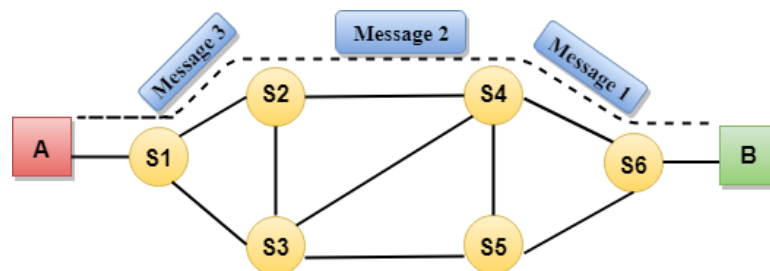
Circuit Switching can use either of the two technologies:

Space Division Switches:
- o Space Division Switching is a circuit switching technology in which a single transmission path is accomplished in a switch by using a physically separate set of crosspoints.
- o Space Division Switching can be achieved by using crossbar switch. A crossbar switch is a metallic crosspoint or semiconductor gate that can be enabled or disabled by a control unit.
- o The Crossbar switch is made by using the semiconductor. For example, Xilinx crossbar switch using FPGAs.
- o Space Division Switching has high speed, high capacity, and nonblocking switches.

Space Division Switches can be categorized in two ways:

- o **Crossbar Switch**
- o **Multistage Switch**

Crossbar Switch
The Crossbar switch is a switch that has n input lines and n output lines. The crossbar switch has n^2 intersection points known as **crosspoints.**
Disadvantage of Crossbar switch:
The number of crosspoints increases as the number of stations is increased. Therefore, it becomes very expensive for a large switch. The solution to this is to use a multistage switch.

Multistage Switch

- o   Multistage Switch is made by splitting the crossbar switch into the smaller units and then interconnecting them.
- o   It reduces the number of crosspoints.
- o   If one path fails, then there will be an availability of another path.

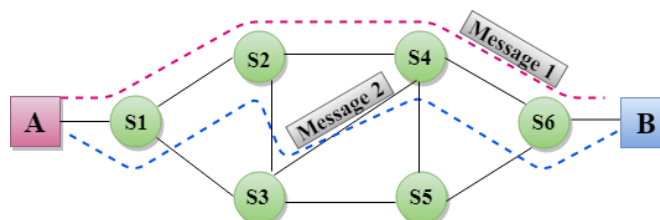**Advantages Of Circuit Switching:**
- o   In the case of Circuit Switching technique, the communication channel is dedicated.
- o   It has fixed bandwidth.

Disadvantages Of Circuit Switching:
- o   Once the dedicated path is established, the only delay occurs in the speed of data transmission.
- o   It takes a long time to establish a connection approx 10 seconds during which no data can be transmitted.
- o   It is more expensive than other switching techniques as a dedicated path is required for each connection.
- o   It is inefficient to use because once the path is established and no data is transferred, then the capacity of the path is wasted.
- o   In this case, the connection is dedicated therefore no other data can be transferred even if the channel is free.

Message Switching

- o   Message Switching is a switching technique in which a message is transferred as a complete unit and routed through intermediate nodes at which it is stored and forwarded.
- o   In Message Switching technique, there is no establishment of a dedicated path between the sender and receiver.
- o   The destination address is appended to the message. Message Switching provides a dynamic routing as the message is routed through the intermediate nodes based on the information available in the message.
- o   Message switches are programmed in such a way so that they can provide the most efficient routes.
- o   Each and every node stores the entire message and then forward it to the next node. This type of network is known as **store and forward network.**
- o   Message switching treats each message as an independent entity.


Advantages Of Message Switching

o   Data channels are shared among the communicating devices that improve the efficiency of using available bandwidth.
o   Traffic congestion can be reduced because the message is temporarily stored in the nodes.
o   Message priority can be used to manage the network.
o   The size of the message which is sent over the network can be varied. Therefore, it supports the data of unlimited size.

Disadvantages Of Message Switching

o   The message switches must be equipped with sufficient storage to enable them to store the messages until the message is forwarded.
o   The Long delay can occur due to the storing and forwarding facility provided by the message switching technique.

Packet Switching

o   The packet switching is a switching technique in which the message is sent in one go, but it is divided into smaller pieces, and they are sent individually.
o   The message splits into smaller pieces known as packets and packets are given a unique number to identify their order at the receiving end.
o   Every packet contains some information in its headers such as source address, destination address and sequence number.
o   Packets will travel across the network, taking the shortest path as possible.
o   All the packets are reassembled at the receiving end in correct order.
o   If any packet is missing or corrupted, then the message will be sent to resend the message.
o   If the correct order of the packets is reached, then the acknowledgment message will be sent.
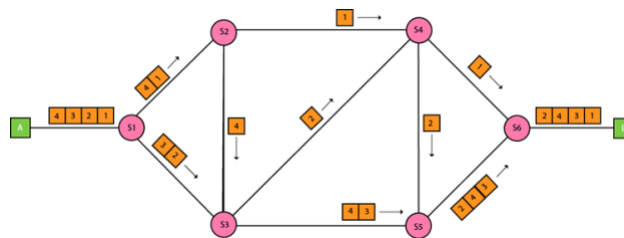
Approaches Of Packet Switching:

There are two approaches to Packet Switching:

Datagram Packet switching:

o   It is a packet switching technology in which packet is known as a datagram, is considered as an independent entity. Each packet contains the information about the destination and switch uses this information to forward the packet to the correct destination.
o   The packets are reassembled at the receiving end in correct order.
o   In Datagram Packet Switching technique, the path is not fixed.
o   Intermediate nodes take the routing decisions to forward the packets.

o Datagram Packet Switching is also known as connectionless switching.

Virtual Circuit Switching

o Virtual Circuit Switching is also known as connection-oriented switching.

o In the case of Virtual circuit switching, a preplanned route is established before the messages are sent.

o Call request and call accept packets are used to establish the connection between sender and receiver.

o In this case, the path is fixed for the duration of a logical connection.

Let's understand the concept of virtual circuit switching through a diagram:
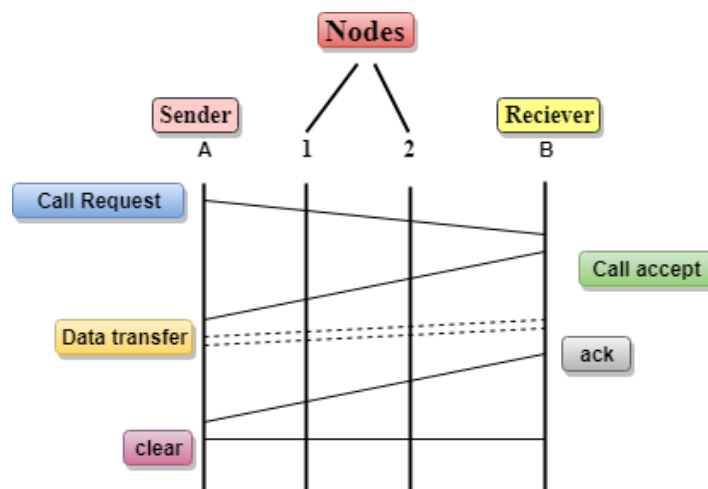
o In the above diagram, A and B are the sender and receiver respectively. 1 and 2 are the nodes.

o Call request and call accept packets are used to establish a connection between the sender and receiver.

o When a route is established, data will be transferred.

o After transmission of data, an acknowledgment signal is sent by the receiver that the message has been received.

o If the user wants to terminate the connection, a clear signal is sent for the termination.

Differences b/w Datagram approach and Virtual Circuit approach

Datagram approach	Virtual Circuit approach
Node takes routing decisions to forward the packets.	Node does not take any routing decision.

Congestion cannot occur as all the packets travel in different directions.	Congestion can occur when the node is busy, and it does not allow other packets to pass through.
It is more flexible as all the packets are treated as an independent entity.	It is not very flexible.

Advantages Of Packet Switching:

- o **Cost-effective:** In packet switching technique, switching devices do not require massive secondary storage to store the packets, so cost is minimized to some extent. Therefore, we can say that the packet switching technique is a cost-effective technique.
- o **Reliable:** If any node is busy, then the packets can be rerouted. This ensures that the Packet Switching technique provides reliable communication.
- o **Efficient:** Packet Switching is an efficient technique. It does not require any established path prior to the transmission, and many users can use the same communication channel simultaneously, hence makes use of available bandwidth very efficiently.

Disadvantages Of Packet Switching:

- o Packet Switching technique cannot be implemented in those applications that require low delay and high-quality services.
- o The protocols used in a packet switching technique are very complex and requires high implementation cost.
- o If the network is overloaded or corrupted, then it requires retransmission of lost packets. It can also lead to the loss of critical information if errors are nor recovered.

Delay, Loss and Throughput in Packet-Switched Networks

Computer networks necessarily constrain **throughput** (the amount of data per second that can be transferred) between end system, introduce delays between end systems and can actually lose packets.

1.4.1 Overview of Delay in Packet-Switched networks

As a packet travels from one node (host or router) to the subsequent host along his path, it suffers from several types of delays at *each* node along the path.

Types of Delay

Nodal processing Queueing (waiting for transmission) Transmission Propagation
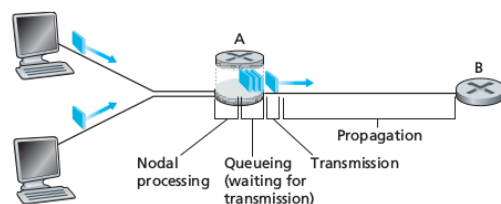
Processing Delay

The **processing delay** consists of the time required to examine the packet's header and determine where to direct the packet. It may also include other factors, such as the time needed to check for bit-level errors occurred during transmission. They typically are of the order of microseconds or less. After processing the packet is sent to the queue preceding the link to the next router

Queuing Delay

At the queue, the packet experiences a **queuing delay** as it waits to be transmitted onto the link. It depends on the number of earlier-arriving packets, therefore if the queue is empty, then the packet's queuing delay will be 0. Typically of the order of microseconds or milliseconds.

Transmission delays

If the length of the packet is L bits, and the **transmission rate** of the link is R bits/sec, then the **transmission delay** is L/R. This is the amount of time required to push (transmit) all of the packet's bits into the link. Typically on the order of microseconds to milliseconds.

Propagation Delay

The time required to propagate a bit from the beginning of the link to the next router is the **propagation delay**. The bit propagates at the propagation speed of the link, which depends on the physical medium of the link. The propagation delay is the distance between two routers divided by the propagation speed of the link.

Total nodal delay

it is the summation of the previous delays

Queuing Delay and Packet Loss

The queuing delay depends can vary from packet to packet, therefore when characterizing queuing delay, one typically uses statistical measures, such as *average queuing delay, variance of queuing delay, and the probability that the queuing delay exceeds some specified value*.

Packet Loss

A queue preceding a link has finite capacity. If a packet finds a full queue, then the router will **drop** it, the packet will be lost. The fraction of lost packets increases as the traffic intensity increases.

End-to-End Delay

Let's now consider the **total delay, from source to destination** (not only the nodal delay). Let's suppose there are *N-1* routers between the source host and the destination host, then the nodal delays accumulate and give an **end-to-end delay**:
d(end_end) = N * [d(proc) + d(queue) + d(trans) + d(prop)]

Throughput in Computer Networks

Another critical performance measure in computer networks is *end-to-end throughput*.
The **instantaneous throughput** at any instant of time is the rate (in bits/sec) at which host B is receiving a file. If the file consists of F bits and the transfers takes T seconds to transfer the whole file, then the **average throughput** of the file is *F/T bits/sec*. For a simple two-link network, the throughput is the

min of all the throughputs, that is the transmission rate of the **bottleneck link**. Therefore, the constraining factor for throughput in today's Internet is typically the *access network*.

Computer Network Models

- A **computer network** consists software and hardware that is used to send and receive data from one device to another.
- The role of hardware is to prove the physical equipment that are required in order to send and receive data while software defines the set of instructions that uses the hardware equipments for data transmission.
- **A simple transmission of data consists several steps at various layers of computer network**

Layered Architecture

- o The main aim of the layered architecture is to divide the design into small pieces.
- o Each lower layer adds its services to the higher layer to provide a full set of services to manage communications and run the applications.
- o It provides modularity and clear interfaces, i.e., provides interaction between subsystems.
- o It ensures the independence between layers by providing the services from lower to higher layer without defining how the services are implemented. Therefore, any modification in a layer will not affect the other layers.
- o The number of layers, functions, contents of each layer will vary from network to network. However, the purpose of each layer is to provide the service from lower to a higher layer and hiding the details from the layers of how the services are implemented.
- o The basic elements of layered architecture are services, protocols, and interfaces.
    - o **Service:** It is a set of actions that a layer provides to the higher layer.
    - o **Protocol:** It defines a set of rules that a layer uses to exchange the information with peer entity. These rules mainly concern about both the contents and order of the messages used.
    - o **Interface:** It is a way through which the message is transferred from one layer to another layer.
- o In a layer n architecture, layer n on one machine will have a communication with the layer n on another machine and the rules used in a conversation are known as a layer-n protocol.

**Let's take an example of the five-layered architecture.**
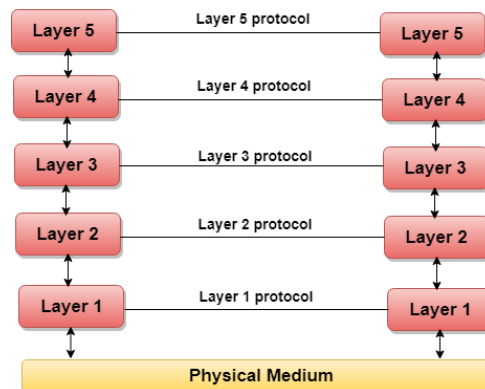
- o In case of layered architecture, no data is transferred from layer n of one machine to layer n of another machine. Instead, each layer passes the data to the layer immediately just below it, until the lowest layer is reached.
- o Below layer 1 is the physical medium through which the actual communication takes place.
- o In a layered architecture, unmanageable tasks are divided into several small and manageable tasks.
- o The data is passed from the upper layer to lower layer through an interface. A Layered architecture provides a clean-cut interface so that minimum information is shared among different layers. It also ensures that the implementation of one layer can be easily replaced by another implementation.
- o A set of layers and protocols is known as network architecture.

OSI Model

- o 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.
- o OSI consists of seven layers, and each layer performs a particular network function.
- o 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.
- o OSI model divides the whole task into seven smaller and manageable tasks. Each layer is assigned a particular task.
- o Each layer is self-contained, so that task assigned to each layer can be performed independently.

Characteristics of OSI Model:
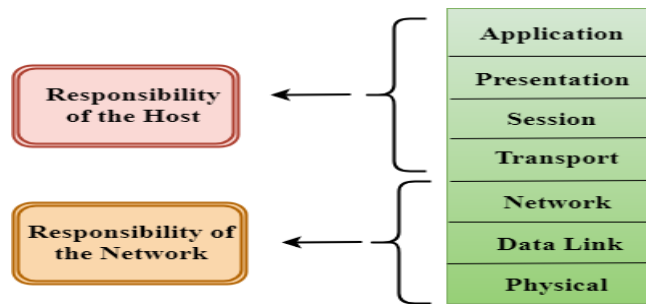
- o   The OSI model is divided into two layers: upper layers and lower layers.
- o   The upper layer of the OSI model mainly deals with the application related issues, and they are implemented only in the software. The application layer is closest to the end user. Both the end user and the application layer interact with the software applications. An upper layer refers to the layer just above another layer.
- o   The lower layer of the OSI model deals with the data transport issues. The data link layer and the physical layer are implemented in hardware and software. The physical layer is the lowest layer of the OSI model and is closest to the physical medium. The physical layer is mainly responsible for placing the information on the physical medium.
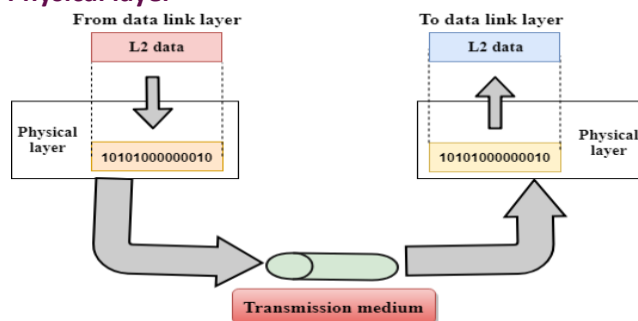
Functions of the OSI Layers

There are the seven OSI layers. Each layer has different functions. A list of seven layers are given below:

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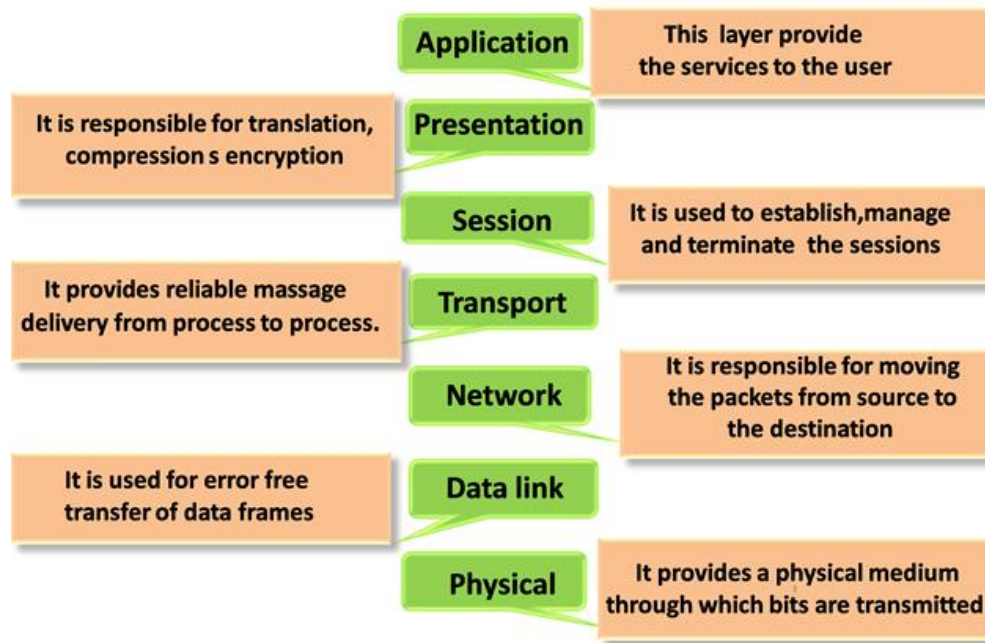
Physical layer

- o   The main functionality of the physical layer is to transmit the individual bits from one node to another node.
- o   It is the lowest layer of the OSI model.
- o   It establishes, maintains and deactivates the physical connection.
- o   It specifies the mechanical, electrical and procedural network interface specifications.

Functions of a Physical layer:

- o   **Line Configuration:** It defines the way how two or more devices can be connected physically.
- o   **Data Transmission:** It defines the transmission mode whether it is simplex, half-duplex or full-duplex mode between the two devices on the network.
- o   **Topology:** It defines the way how network devices are arranged.
- o   **Signals:** It determines the type of the signal used for transmitting the information.
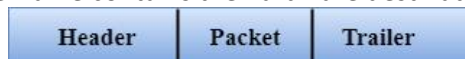
Data-Link Layer
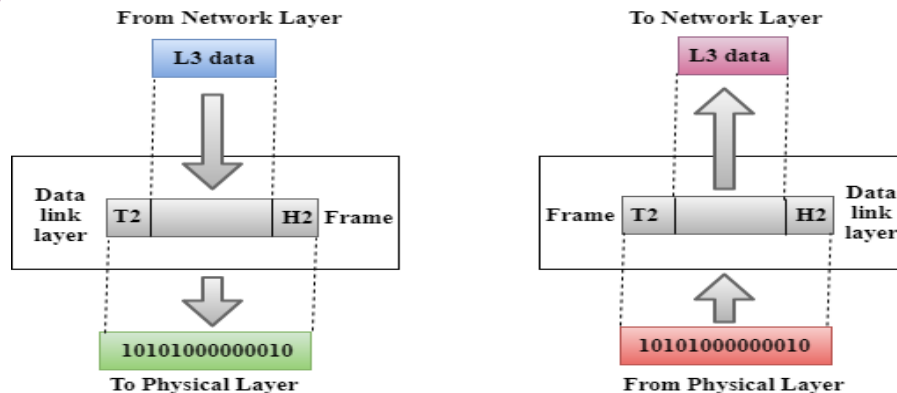
o This layer is responsible for the error-free transfer of data frames.
o It defines the format of the data on the network.
o It provides a reliable and efficient communication between two or more devices.
o It is mainly responsible for the unique identification of each device that resides on a local network.
o It contains two sub-layers:
   o **Logical Link Control Layer**
      o It is responsible for transferring the packets to the Network layer of the receiver that is receiving.
      o It identifies the address of the network layer protocol from the header.
      o It also provides flow control.
   o **Media Access Control Layer**
      o A Media access control layer is a link between the Logical Link Control layer and the network's physical layer.
      o It is used for transferring the packets over the network.

Functions of the Data-link layer

o **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.


o **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.
o **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.
o **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 occurr, then the receiver sends the acknowledgment for the retransmission of the corrupted frames.

- o **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.

Network Layer
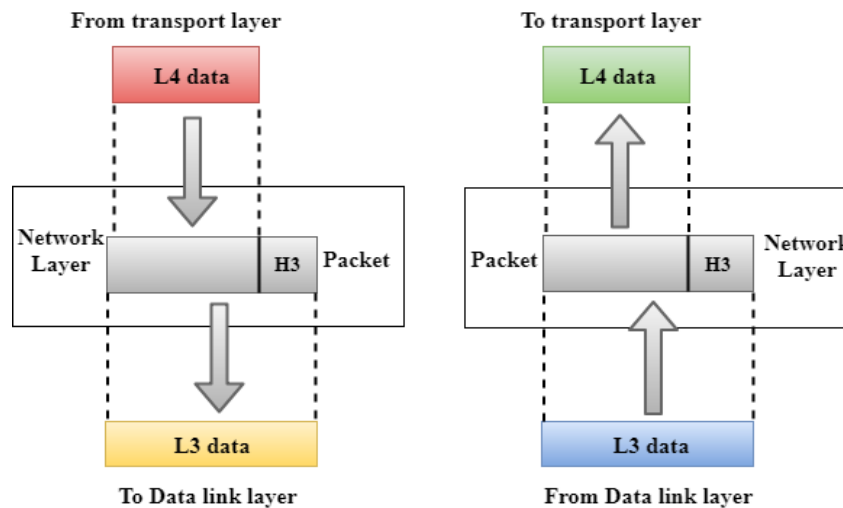
- o It is a layer 3 that manages device addressing, tracks the location of devices on the network.
- o It determines the best path to move data from source to the destination based on the network conditions, the priority of service, and other factors.
- o The Data link layer is responsible for routing and forwarding the packets.
- o Routers are the layer 3 devices, they are specified in this layer and used to provide the routing services within an internetwork.
- o The protocols used to route the network traffic are known as Network layer protocols. Examples of protocols are IP and Ipv6.

Functions of Network Layer:

- o **Internetworking:** An internetworking is the main responsibility of the network layer. It provides a logical connection between different devices.
- o **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.
- o **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.
- o **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).

Transport Layer
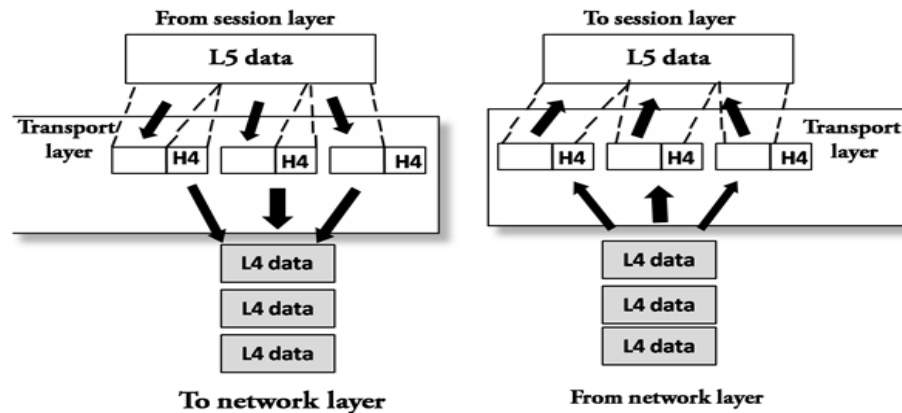
- o The Transport layer is a Layer 4 ensures that messages are transmitted in the order in which they are sent and there is no duplication of data.
- o The main responsibility of the transport layer is to transfer the data completely.
- o It receives the data from the upper layer and converts them into smaller units known as segments.
- o This layer can be termed as an end-to-end layer as it provides a point-to-point connection between source and destination to deliver the data reliably.

The two protocols used in this layer are:

- o **Transmission Control Protocol**
    - o It is a standard protocol that allows the systems to communicate over the internet.
    - o It establishes and maintains a connection between hosts.
    - o 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.

- o **User Datagram Protocol**
    - o User Datagram Protocol is a transport layer protocol.
    - o It is an unreliable transport protocol as in this case 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.

Functions of Transport Layer:

- o **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.

o **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.

o **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.

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

o **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.
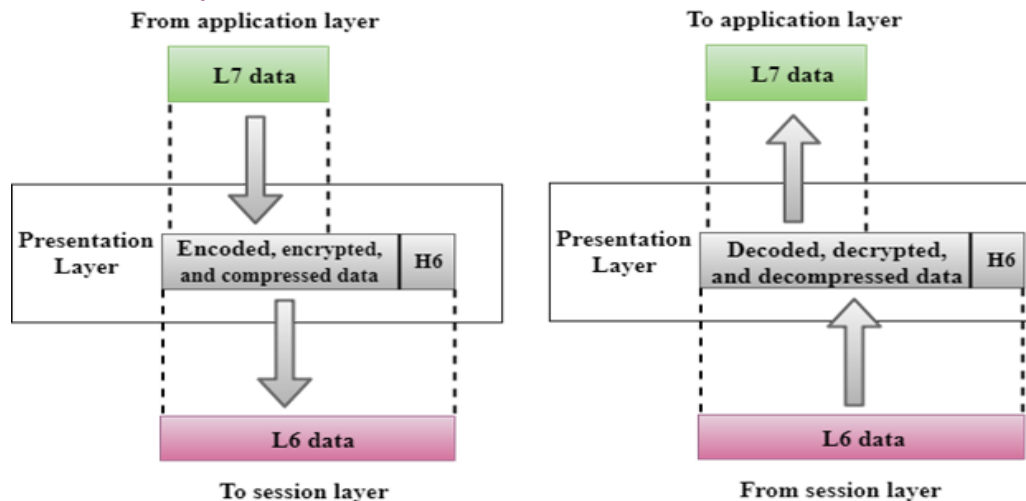
Session Layer
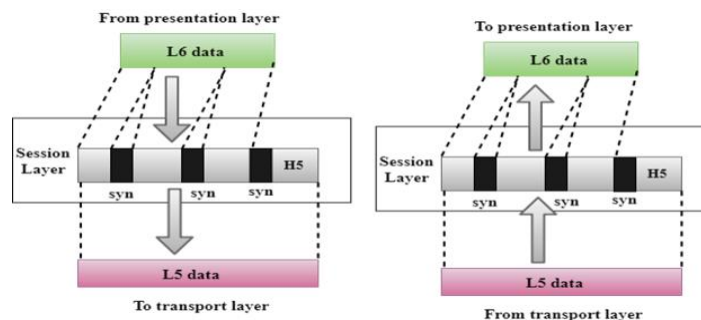
o It is a layer 3 in the OSI model.

o The Session layer is used to establish, maintain and synchronizes the interaction between communicating devices.

Functions of Session layer:

o **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.

o **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.

Presentation Layer

From application layer

L7 data

Presentation Layer | Encoded, encrypted, and compressed data | H6

L6 data

To session layer

To application layer

L7 data

Presentation Layer | Decoded, decrypted, and decompressed data | H6

L6 data

From session layer

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

Functions of Presentation layer:
- o **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.
- o **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.
- o **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.

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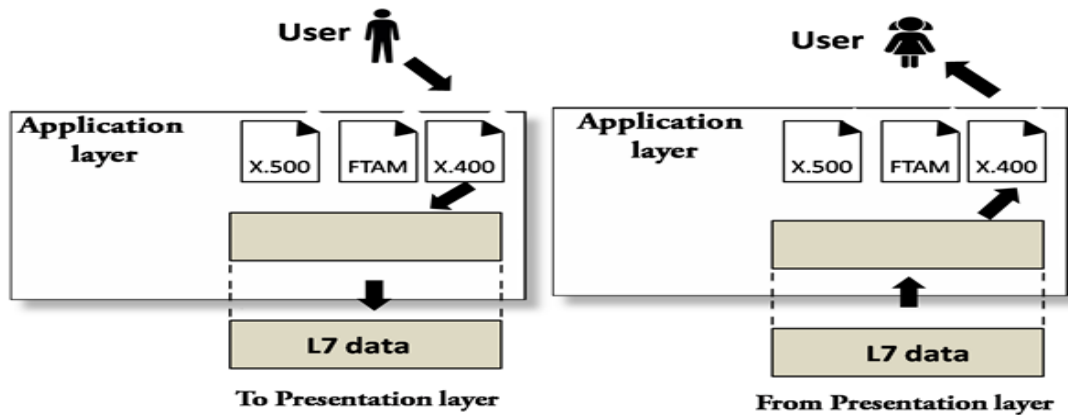
o An application layer serves as a window for users and application processes to access network service.
o It handles issues such as network transparency, resource allocation, etc.
o An application layer is not an application, but it performs the application layer functions.
o This layer provides the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

Functions of Application layer:

o **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.
o **Mail services:** An application layer provides the facility for email forwarding and storage.
o Directory services: An application provides the distributed database sources and is used to provide that global information about various objects.

TCP/IP model
o The TCP/IP model was developed prior to the OSI model.
o The TCP/IP model is not exactly similar to the OSI model.
o The TCP/IP model consists of five layers: the application layer, transport layer, network layer, data link layer and physical layer.
o The first four layers provide physical standards, network interface, internetworking, and transport functions that correspond to the first four layers of the OSI model
o TCP/IP is a hierarchical protocol made up of interactive modules, and each of them provides specific functionality.

Here, hierarchical means that each upper-layer protocol is supported by two or more lower-level protocols.

Functions of TCP/IP layers:
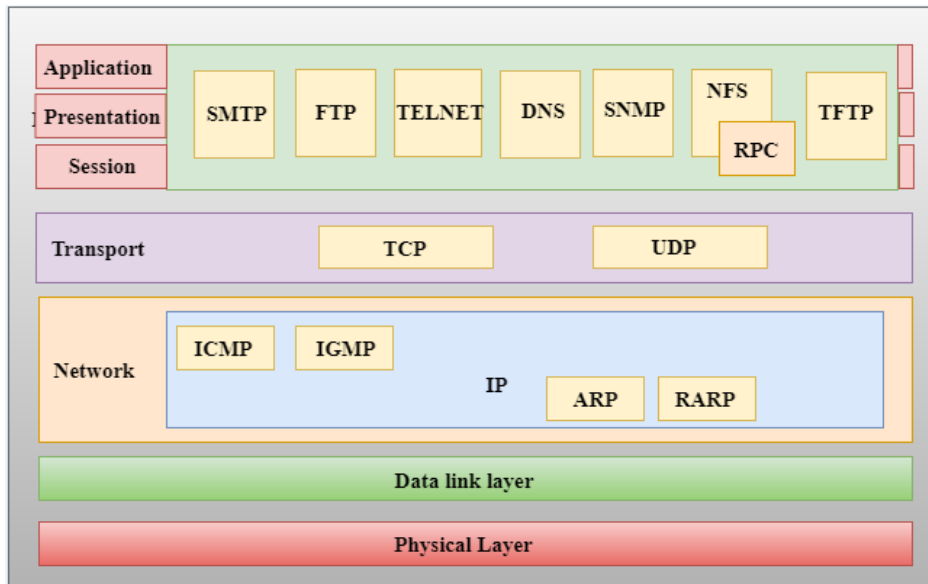
Network Access Layer

- o   A network layer is the lowest layer of the TCP/IP model.
- o   A network layer is the combination of the Physical layer and Data Link layer defined in the OSI reference model.
- o   It defines how the data should be sent physically through the network.
- o   This layer is mainly responsible for the transmission of the data between two devices on the same network.
- o   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.
- o   The protocols used by this layer are ethernet, token ring, FDDI, X.25, frame relay.

Internet Layer

- o   An internet layer is the second layer of the TCP/IP model.
- o   An internet layer is also known as the network layer.
- o   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.

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**.

Application Layer

o An application layer is the topmost layer in the TCP/IP model.

o It is responsible for handling high-level protocols, issues of representation.

o This layer allows the user to interact with the application.

o When one application layer protocol wants to communicate with another application layer, it forwards its data to the transport layer.

o 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.

Transmission media

Transmission media is a communication channel that carries the information from the sender to the receiver. Data is transmitted through the electromagnetic signals**.**

o The main functionality of the transmission media is to carry the information in the form of bits through **LAN**(Local Area Network).

o It is a physical path between transmitter and receiver in data communication.

o In a copper-based network, the bits in the form of electrical signals.

o In a fibre based network, the bits in the form of light pulses.

o In **OSI**(Open System Interconnection) phase, transmission media supports the Layer 1. Therefore, it is considered to be as a Layer 1 component.

o The electrical signals can be sent through the copper wire, fibre optics, atmosphere, water, and vacuum.

o The characteristics and quality of data transmission are determined by the characteristics of medium and signal.

o Transmission media is of two types are wired media and wireless media. In wired media, medium characteristics are more important whereas, in wireless media, signal characteristics are more important.

o Different transmission media have different properties such as bandwidth, delay, cost and ease of installation and maintenance.

o The transmission media is available in the lowest layer of the OSI reference model, i.e., **Physical layer**.

Some factors need to be considered for designing the transmission media:

o **Bandwidth:** All the factors are remaining constant, the greater the bandwidth of a medium, the higher the data transmission rate of a signal.

- o **Transmission impairment:** When the received signal is not identical to the transmitted one due to the transmission impairment. The quality of the signals will get destroyed due to transmission impairment.
- o **Interference:** An interference is defined as the process of disrupting a signal when it travels over a communication medium on the addition of some unwanted signal.

Causes Of Transmission Impairment:
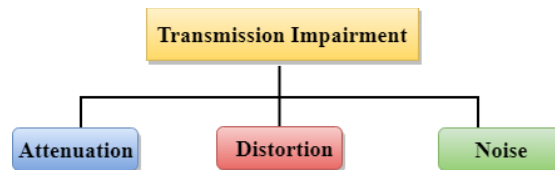
- o **Attenuation:** Attenuation means the loss of energy, i.e., the strength of the signal decreases with increasing the distance which causes the loss of energy.
- o **Distortion:** Distortion occurs when there is a change in the shape of the signal. This type of distortion is examined from different signals having different frequencies. Each frequency component has its own propagation speed, so they reach at a different time which leads to the delay distortion.
- o **Noise:** When data is travelled over a transmission medium, some unwanted signal is added to it which creates the noise.

**Classification Of Transmission Media:**
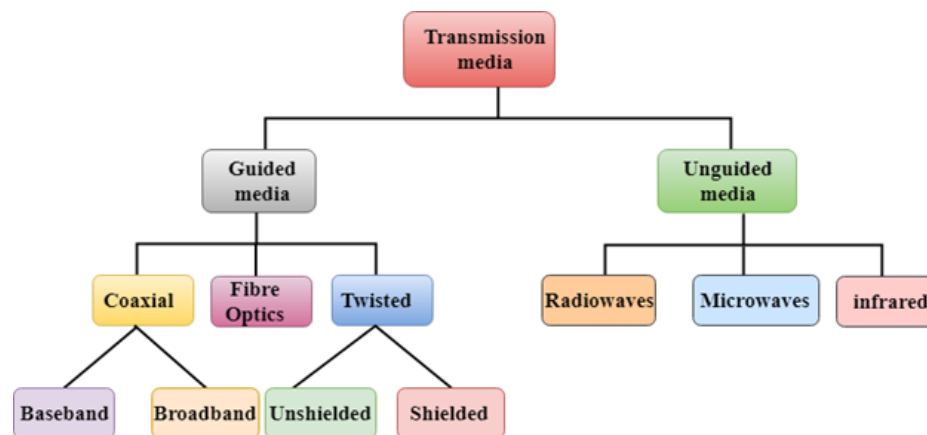
Guided Media
It is defined as the physical medium through which the signals are transmitted. It is also known as Bounded media.

Types Of Guided media:
Twisted pair:
- • Twisted pair is a physical media made up of a pair of cables twisted with each other.

- A twisted pair cable is cheap as compared to other transmission media.
- Installation of the twisted pair cable is easy, and it is a lightweight cable.
- The frequency range for twisted pair cable is from 0 to 3.5KHz.
- A twisted pair consists of two insulated copper wires arranged in a regular spiral pattern.
- The degree of reduction in noise interference is determined by the number of turns per foot.
- Increasing the number of turns per foot decreases noise interference.
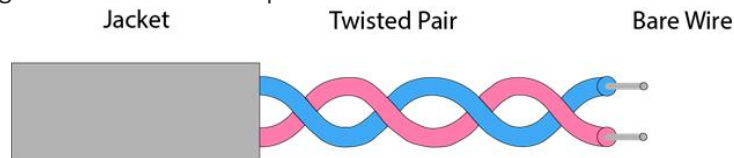
Types of Twisted pair:
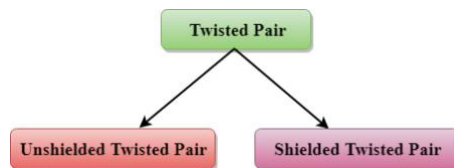
Unshielded Twisted Pair:
An unshielded twisted pair is widely used in telecommunication. Following are the categories of the unshielded twisted pair cable:

- o **Category 1:** Category 1 is used for telephone lines that have low-speed data.
- o **Category 2:** It can support upto 4Mbps.
- o **Category 3:** It can support upto 16Mbps.
- o **Category 4:** It can support upto 20Mbps. Therefore, it can be used for long-distance communication.
- o **Category 5:** It can support upto 200Mbps.

Advantages Of Unshielded Twisted Pair:
- o It is cheap.
- o Installation of the unshielded twisted pair is easy.
- o It can be used for high-speed LAN.

Disadvantage:
- o This cable can only be used for shorter distances because of attenuation.

Shielded Twisted Pair
A shielded twisted pair is a cable that contains the mesh surrounding the wire that allows the higher transmission rate.

**Characteristics Of Shielded Twisted Pair:**

- The cost of the shielded twisted pair cable is not very high and not very low.
- An installation of STP is easy.
- It has higher capacity as compared to unshielded twisted pair cable.
- It has a higher attenuation.
- It is shielded that provides the higher data transmission rate.

Disadvantages

- It is more expensive as compared to UTP and coaxial cable.
- It has a higher attenuation rate.

Coaxial Cable

- Coaxial cable is very commonly used transmission media, for example, TV wire is usually a coaxial cable.
- The name of the cable is coaxial as it contains two conductors parallel to each other.
- It has a higher frequency as compared to Twisted pair cable.
- The inner conductor of the coaxial cable is made up of copper, and the outer conductor is made up of copper mesh. The middle core is made up of non-conductive cover that separates the inner conductor from the outer conductor.
- The middle core is responsible for the data transferring whereas the copper mesh prevents from the **EMI**(Electromagnetic interference).

| Jacket | Shield | Insulator | Centre Conductor |
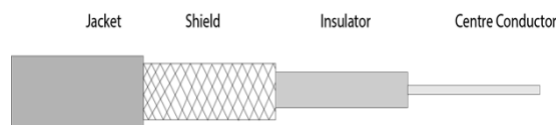
Coaxial cable is of two types:

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

Advantages Of Coaxial cable:

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

Disadvantages Of Coaxial cable:

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

Fibre Optic

- Fibre optic cable is a cable that uses electrical signals for communication.

o   Fibre optic is a cable that holds the optical fibres coated in plastic that are used to send the data by pulses of light.
o   The plastic coating protects the optical fibres from heat, cold, electromagnetic interference from other types of wiring.
o   Fibre optics provide faster data transmission than copper wires.

Diagrammatic representation of fibre optic cable:

Basic elements of Fibre optic cable:

o   **Core:** The optical fibre consists of a narrow strand of glass or plastic known as a core. A core is a light transmission area of the fibre. The more the area of the core, the more light will be transmitted into the fibre.
o   **Cladding:** The concentric layer of glass is known as cladding. The main functionality of the cladding is to provide the lower refractive index at the core interface as to cause the reflection within the core so that the light waves are transmitted through the fibre.
o   **Jacket:** The protective coating consisting of plastic is known as a jacket. The main purpose of a jacket is to preserve the fibre strength, absorb shock and extra fibre protection.

Following are the advantages of fibre optic cable over copper:

o   **Greater Bandwidth:** The fibre optic cable provides more bandwidth as compared copper. Therefore, the fibre optic carries more data as compared to copper cable.
o   **Faster speed:** Fibre optic cable carries the data in the form of light. This allows the fibre optic cable to carry the signals at a higher speed.
o   **Longer distances:** The fibre optic cable carries the data at a longer distance as compared to copper cable.
o   **Better reliability:** The fibre optic cable is more reliable than the copper cable as it is immune to any temperature changes while it can cause obstruct in the connectivity of copper cable.
o   **Thinner and Sturdier:** Fibre optic cable is thinner and lighter in weight so it can withstand more pull pressure than copper cable.

UnGuided Transmission

o   An unguided transmission transmits the electromagnetic waves without using any physical medium. Therefore it is also known as **wireless transmission**.

o   In unguided media, air is the media through which the electromagnetic energy can flow easily.
Unguided transmission is broadly classified into three categories:

Radio waves

- o   Radio waves are the electromagnetic waves that are transmitted in all the directions of free space.
- o   Radio waves are omnidirectional, i.e., the signals are propagated in all the directions.
- o   The range in frequencies of radio waves is from 3Khz to 1 khz.
- o   In the case of radio waves, the sending and receiving antenna are not aligned, i.e., the wave sent by the sending antenna can be received by any receiving antenna.
- o   An example of the radio wave is **FM radio**.
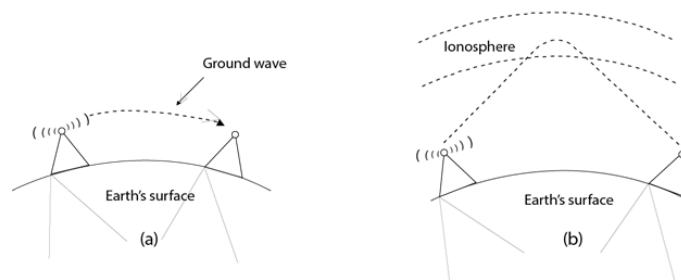
Applications Of Radio waves:

- o   A Radio wave is useful for multicasting when there is one sender and many receivers.
- o   An FM radio, television, cordless phones are examples of a radio wave.

Advantages Of Radio transmission:

- o   Radio transmission is mainly used for wide area networks and mobile cellular phones.
- o   Radio waves cover a large area, and they can penetrate the walls.
- o   Radio transmission provides a higher transmission rate.

Microwaves
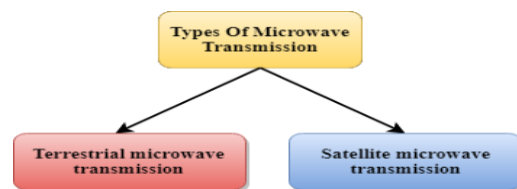
Microwaves are of two types:
- o   Terrestrial microwave
- o   Satellite microwave communication.

Terrestrial Microwave Transmission

- o   Terrestrial Microwave transmission is a technology that transmits the focused beam of a radio signal from one ground-based microwave transmission antenna to another.

- o Microwaves are the electromagnetic waves having the frequency in the range from 1GHz to 1000 GHz.
- o Microwaves are unidirectional as the sending and receiving antenna is to be aligned, i.e., the waves sent by the sending antenna are narrowly focussed.
- o In this case, antennas are mounted on the towers to send a beam to another antenna which is km away.
- o It works on the line of sight transmission, i.e., the antennas mounted on the towers are the direct sight of each other.

Characteristics of Microwave:

- o **Frequency range:** The frequency range of terrestrial microwave is from 4-6 GHz to 21-23 GHz.
- o **Bandwidth:** It supports the bandwidth from 1 to 10 Mbps.
- o **Short distance:** It is inexpensive for short distance.
- o **Long distance:** It is expensive as it requires a higher tower for a longer distance.
- o **Attenuation:** Attenuation means loss of signal. It is affected by environmental conditions and antenna size.

Advantages Of Microwave:

- o Microwave transmission is cheaper than using cables.
- o It is free from land acquisition as it does not require any land for the installation of cables.
- o Microwave transmission provides an easy communication in terrains as the installation of cable in terrain is quite a difficult task.
- o Communication over oceans can be achieved by using microwave transmission.

Disadvantages of Microwave transmission:

- o **Eavesdropping:** An eavesdropping creates insecure communication. Any malicious user can catch the signal in the air by using its own antenna.
- o **Out of phase signal:** A signal can be moved out of phase by using microwave transmission.
- o **Susceptible to weather condition:** A microwave transmission is susceptible to weather condition. This means that any environmental change such as rain, wind can distort the signal.
- o **Bandwidth limited:** Allocation of bandwidth is limited in the case of microwave transmission.

Satellite Microwave Communication

- o A satellite is a physical object that revolves around the earth at a known height.
- o Satellite communication is more reliable nowadays as it offers more flexibility than cable and fibre optic systems.
- o We can communicate with any point on the globe by using satellite communication.

How Does Satellite work?
The satellite accepts the signal that is transmitted from the earth station, and it amplifies the signal. The amplified signal is retransmitted to another earth station.

Advantages Of Satellite Microwave Communication:

- o The coverage area of a satellite microwave is more than the terrestrial microwave.
- o The transmission cost of the satellite is independent of the distance from the centre of the coverage area.
- o Satellite communication is used in mobile and wireless communication applications.
- o It is easy to install.
- o It is used in a wide variety of applications such as weather forecasting, radio/TV signal broadcasting, mobile communication, etc.

Disadvantages Of Satellite Microwave Communication:

- o Satellite designing and development requires more time and higher cost.
- o The Satellite needs to be monitored and controlled on regular periods so that it remains in orbit.
- o The life of the satellite is about 12-15 years. Due to this reason, another launch of the satellite has to be planned before it becomes non-functional.

Infrared

- o An infrared transmission is a wireless technology used for communication over short ranges.
- o The frequency of the infrared in the range from 300 GHz to 400 THz.
- o It is used for short-range communication such as data transfer between two cell phones, TV remote operation, data transfer between a computer and cell phone resides in the same closed area.

Characteristics Of Infrared:

- o It supports high bandwidth, and hence the data rate will be very high.
- o Infrared waves cannot penetrate the walls. Therefore, the infrared communication in one room cannot be interrupted by the nearby rooms.
- o An infrared communication provides better security with minimum interference.
- o Infrared communication is unreliable outside the building because the sun rays will interfere with the infrared waves.