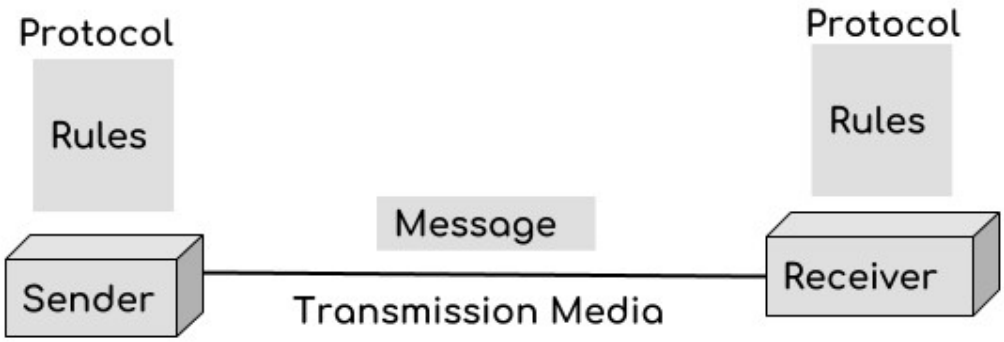
Unit-1

Introduction to 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.

How Does a Computer Network Work?

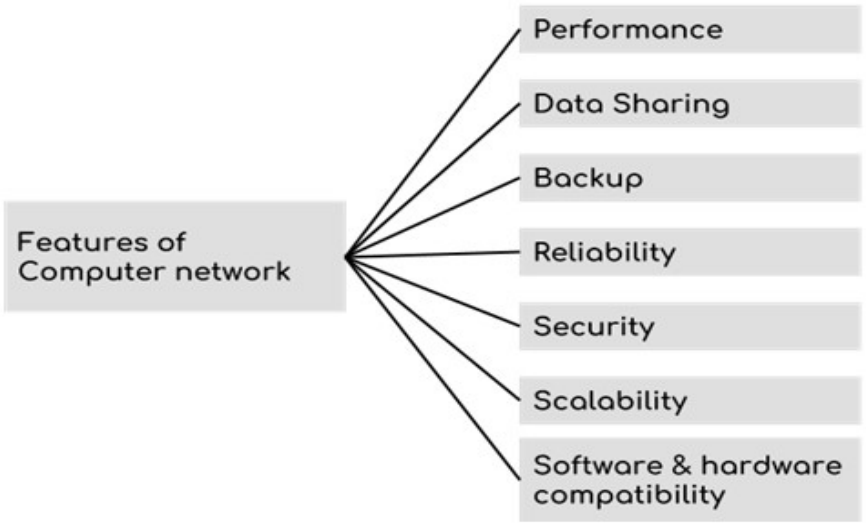
Basics building blocks of a Computer network are Nodes and Links. A Network Node can be illustrated as Equipment for Data Communication like a Modem, Router, etc., or Equipment of a Data Terminal like connecting two computers or more. Link in Computer Networks can be defined as wires or cables or free space of wireless networks.

The working of Computer Networks can be simply defined as rules or protocols which help in sending and receiving data via the links which allow Computer networks to communicate. Each device has an IP Address that helps in identifying a device.

Basic Terminologies of Computer Networks:

- **Network:** A network is a collection of computers and devices that are connected together to enable communication and data exchange.
- **Nodes:** Nodes are devices that are connected to a network. These can include computers, Servers, Printers, Routers, Switches and other devices.
- **Protocol:** A protocol is a set of rules and standards that govern how data is transmitted over a network. Examples of protocols include TCP/IP, HTTP and FTP.
- **Topology:** Network topology refers to the physical and logical arrangement of nodes on a network. The common network topologies include bus, star, ring, mesh and tree.
- **Service Provider Networks:** These types of Networks give permission to take Network Capacity and Functionality on lease from the Provider. Service Provider Networks include Wireless Communications, Data Carriers, etc.
- **IP Address**: An IP address is a unique numerical identifier that is assigned to every device on a network. IP addresses are used to identify devices and enable communication between them.
- **DNS:** The Domain Name System (DNS) is a protocol that is used to translate human-readable domain names (such as www.google.com) into IP addresses that computers can understand.
- **Firewall:** A firewall is a security device that is used to monitor and control incoming and outgoing network traffic. Firewalls are used to protect networks from unauthorized access and other security threats.

Features of a Computer Network:



A computer network has following features:

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.

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.

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.

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.

Reliability: There should not be any failure in the network or if it occurs the recovery from a failure should be fast.

Security: A computer network should be secure so that the data transmitting over a network should be safe from unauthorized 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.

Scalability: A computer network should be scalable which means it should always allow adding 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, let's 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.

The sharing of data can occur through the two feasible ways:

1. **Physical cable media**, such as fiber-optical cable, twisted pair etc.
2. **Wireless methods** such as Wi-Fi, radio communication and microwave transmission.

An example of a network is the tern LAPLINK, which allows you to copy files from one device to another device over a specific parallel port to be considered a computer network. Another example specified here is that we all may use it in our daily lives, i.e., the internet.

Some various types of networks are **LAN, MAN, WAN** *etc.*

There are various types of networks that can be used for different functions:

- **LAN:** Local area networks are mainly used to connect personal devices within a few kilometers of a limited area. These networks are used in offices, companies and factories to exchange data and Information.

- **MAN:** Metropolitan area networks are used to connect the devices over an entire city under the range of up to 50 km. These networks are used in the telephone company network and cable TV network.
- **WAN:** Wide Area Networks are used in the wide geological range over a country and continent. These networks are used in military services, mobile operators, railways and airlines reservations.
- **PAN:** Personal area networks appropriate to personal or separate workspace under the range of 10 meters. These networks are mostly used to connect tablets, smartphones and laptops.
- **CAN:** Campus area networks are used to connect limited geographic areas. CAN interconnect multiple local area networks (LAN) within Colleges, Universities, Corporates buildings, etc.

Application of computer networks:

1. Resource Sharing:

Resource sharing is an application of a computer network. Resource sharing means you can share one Hardware and Software among multiple users. Hardware includes printers, Disks, Fax Machines, etc. Computing devices. And Software includes Atom, Oracle VM Virtual Box, Postman, Android Studio, etc.

2. Information Sharing:

Using a Computer network, we can share Information over the network, and it provides Search capabilities such as WWW. Over the network, single information can be shared among the many users over the internet.

3. Communication:

Communication includes email, calls, message broadcast, electronic funds transfer system etc.

4. Entertainment Industry:

In Entertainment industry also uses computer networks widely. Some of the Entertainment industries are Video on demand, Multiperson real-time simulation games, movie/TV programs, etc.

5. Access to Remote Databases:

Computer networks allow us to access the Remote Database of the various applications by the end-users. Some applications are Reservation for Hotels, Airplane Booking, Home Banking, Automated Newspaper, Automated Library etc.

6. Home applications:

There are many common uses of the computer network are as home applications. For example, you can consider user-to-user communication, access to remote instruction, electronic commerce and entertainment. Another way is managing bank accounts, transferring money to some other banks,

paying bills electronically. A computer network arranges a robust connection mechanism between users.

7. Business applications:

The result of business application here is resource sharing. And the purpose of resource sharing is that without moving to the physical location of the resource, all the data, plans and tools can be shared to any network user. Most of the companies are doing business electronically with other companies and with other clients worldwide with the help of a computer network.

8. Mobile users:

The rapidly growing sectors in computer applications are mobile devices like notebook computers and PDAs (personal digital assistants). Here mobile users/device means portable device. The computer network is widely used in new-age technology like smartwatches, wearable devices, tablets, online transactions, purchasing or selling products online, etc.

9. Social media:

Social media is also a great example of a computer network application. It helps people to share and receive any information related to political, ethical and social issues.

Uses of Computer Network:

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

Computer Network Components:

Computer network components are the *major parts* which are needed to *install the software*. Some important network components are NIC, switch, cable, hub, router, and modem. Depending on the type of network that we need to install, some network components can also be removed. For example, the wireless network does not require a cable.

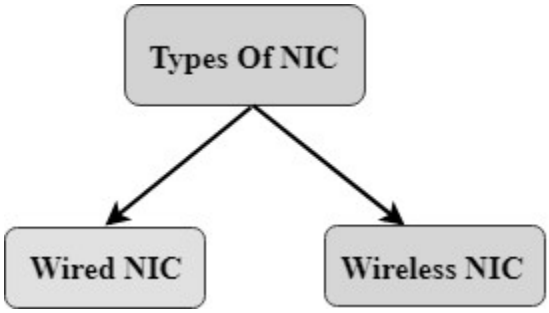
Following are the major components required to install a network:

NIC:

- NIC stands for network interface card.
- NIC is a hardware component used to connect a computer with another computer onto a network
- It can support a transfer rate of 10,100 to 1000 Mb/s.

- The MAC address or physical address is encoded on the network card chip which is assigned by the IEEE to identify a network card uniquely. The MAC address is stored in the PROM (Programmable read-only memory).

There are two types of NIC:



1. Wired NIC
2. Wireless NIC

Wired NIC: The Wired NIC is present inside the motherboard. Cables and connectors are used with wired NIC to transfer data.

Wireless NIC: The wireless NIC contains the antenna to obtain the connection over the wireless network. For example, laptop computer contains the wireless NIC.

Hub:

A Hub is a hardware device that divides the network connection among multiple devices. When computer requests for some information from a network, it first sends the request to the Hub through cable. Hub will broadcast this request to the entire network. All the devices will check whether the request belongs to them or not. If not, the request will be dropped.

The process used by the Hub consumes more bandwidth and limits the amount of communication. Nowadays, the use of hub is obsolete, and it is replaced by more advanced computer network components such as Switches, Routers.

Switch:

A switch is a hardware device that connects multiple devices on a computer network. A Switch contains more advanced features than Hub. The Switch contains the updated table that decides where the data is transmitted or not. Switch delivers the message to the correct destination based on the physical address present in the incoming message.

A Switch does not broadcast the message to the entire network like the Hub. It determines the device to whom the message is to be transmitted. Therefore, we can say that switch provides a direct connection between the source and destination. It increases the speed of the network.

Router:

- A router is a hardware device which is used to connect a LAN with an internet connection. It is used to receive, analyze and forward the incoming packets to another network.
- A router works in a Layer 3 (Network layer) of the OSI Reference model.
- A router forwards the packet based on the information available in the routing table.
- It determines the best path from the available paths for the transmission of the packet.

Advantages of Router:

- Security: The information which is transmitted to the network will traverse the entire cable, but the only specified device which has been addressed can read the data.
- Reliability: If the server has stopped functioning, the network goes down, but no other networks are affected that are served by the router.
- Performance: Router enhances the overall performance of the network. Suppose there are 24 workstations in a network generates a same amount of traffic. This increases the traffic load on the network. Router splits the single network into two networks of 12 workstations each, reduces the traffic load by half.
- Network range

Modem:

- A modem is a hardware device that allows the computer to connect to the internet over the existing telephone line.
- A modem is not integrated with the motherboard rather than it is installed on the PCI slot found on the motherboard.
- It stands for Modulator/Demodulator. It converts the digital data into an analog signal over the telephone lines.

Based on the differences in speed and transmission rate, a modem can be classified in the following categories:

- Standard PC modem or Dial-up modem
- Cellular Modem
- Cable modem

Cables and Connectors:

Cable is a transmission media used for transmitting a signal.

There are three types of cables used in transmission:

- Twisted pair cable
- Coaxial cable
- Fiber-optic cable

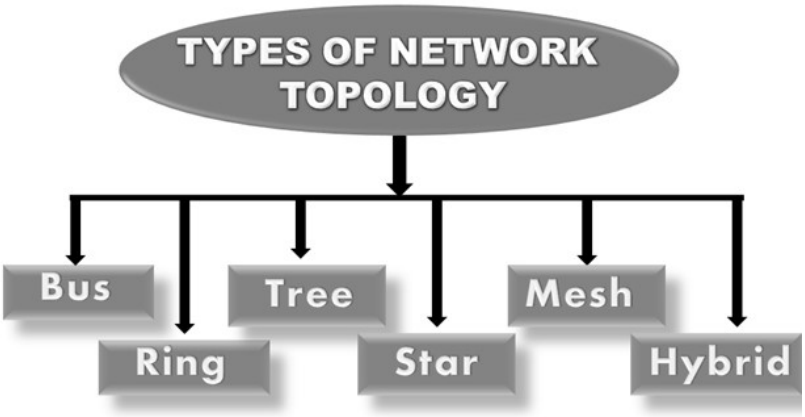
Topology:

What is Network Topology?

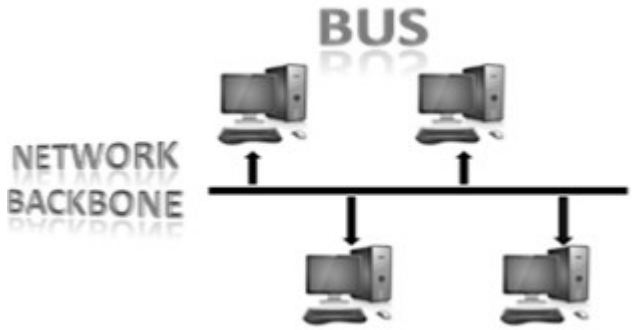
Topology defines the structure of the network of how all the components are interconnected to each other. There are two types of topology: physical and logical topology.

Types of Network Topology:

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



1) Bus Topology:



- The bus topology is designed in such a way that all the stations are connected through a single cable known as a backbone cable.
- Each node is either connected to the backbone cable by drop cable or directly connected to the backbone cable.
- When a node wants to send a message over the network, it puts a message over the network. All the stations available in the network will receive the message whether it has been addressed or not.
- The bus topology is mainly used in 802.3 (Ethernet) and 802.4 standard networks.
- The configuration of a bus topology is quite simpler as compared to other topologies.

- The backbone cable is considered as a "single lane" through which the message is broadcast to all the stations.
- The most common access method of the bus topologies is CSMA (Carrier Sense Multiple Access).

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

- **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 upto 10 Mbps.
- **Familiar technology:** Bus topology is a familiar technology as the installation and troubleshooting techniques are well known and hardware components are easily available.
- **Limited failure:** A failure in one node will not have any effect on other nodes.

Disadvantages of Bus topology:

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

2) Ring Topology:

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

Working of Token passing:

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

Advantages of Ring topology:

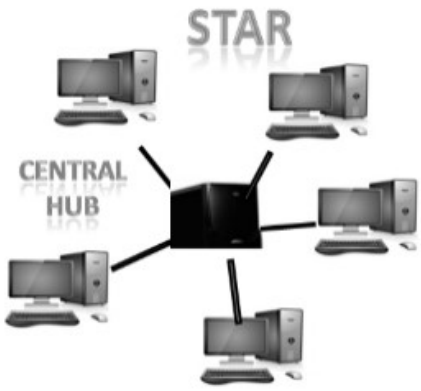
- **Network Management:** Faulty devices can be removed from the network without bringing the network down.
- **Product availability:** Many hardware and software tools for network operation and monitoring are available.

- **Cost:** Twisted pair cabling is inexpensive and easily available. Therefore, the installation cost is very low.
- **Reliable:** It is a more reliable network because the communication system is not dependent on the single host computer.

Disadvantages of Ring topology:

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

3) Star Topology:



- Star topology is an arrangement of the network in which every node is connected to the central hub, switch or a central computer.
- The central computer is known as a server and the peripheral devices attached to the server are known as clients.
- Coaxial cable or RJ-45 cables are used to connect the computers.
- Hubs or Switches are mainly used as connection devices in a physical star topology.
- Star topology is the most popular topology in network implementation.

Advantages of Star topology:

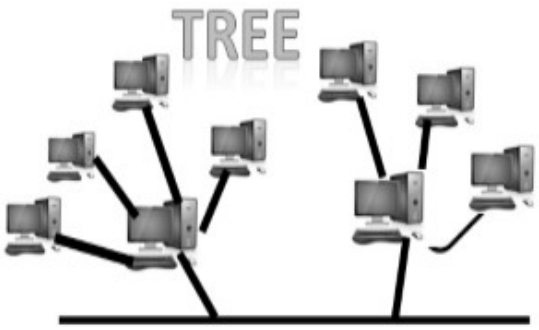
- **Efficient troubleshooting:** Troubleshooting is quite efficient in a star topology as compared to bus topology. In a bus topology, the manager has to inspect the kilometers of cable. In a star topology, all the stations are connected to the centralized network. Therefore, the network administrator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

- **Network control:** Complex network control features can be easily implemented in the star topology. Any changes made in the star topology are automatically accommodated.
- **Limited failure:** As each station is connected to the central hub with its own cable, therefore failure in one cable will not affect the entire network.
- **Familiar technology:** Star topology is a familiar technology as its tools are cost-effective.
- Easily expandable: It is easily expandable as new stations can be added to the open ports on the hub.
- **Cost effective:** Star topology networks are cost-effective as it uses inexpensive coaxial cable.
- **High data speeds:** It supports a bandwidth of approx 100Mbps. Ethernet 100BaseT is one of the most popular Star topology networks.

Disadvantages of Star topology:

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

4) Tree topology:



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

Advantages of Tree topology:

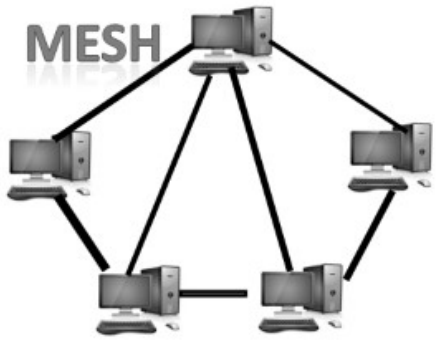
- **Support for broadband transmission:** Tree topology is mainly used to provide broadband transmission, i.e., signals are sent over long distances without being attenuated.

- **Easily expandable:** We can add the new device to the existing network. Therefore, we can say that tree topology is easily expandable.
- **Easily manageable:** In tree topology, the whole network is divided into segments known as star networks which can be easily managed and maintained.
- **Error detection:** Error detection and error correction are very easy in a tree topology.
- **Limited failure:** The breakdown in one station does not affect the entire network.
- **Point-to-point wiring:** It has point-to-point wiring for individual segments.

Disadvantages of Tree topology:

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

5) Mesh topology:



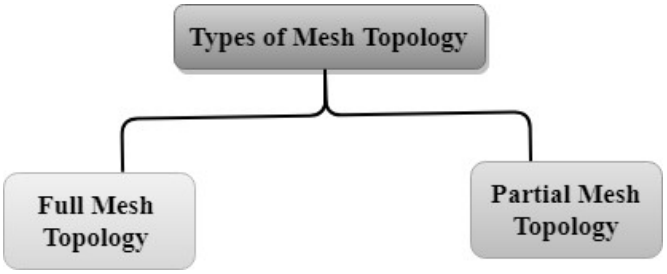
- Mesh technology is an arrangement of the network in which computers are interconnected with each other through various redundant connections.
- There are multiple paths from one computer to another computer.
- It does not contain the switch, hub or any central computer which acts as a central point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

Number of cables = (n*(n-1))/2;

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

Mesh topology is divided into two categories:

- Fully connected mesh topology
- Partially connected mesh topology



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

Advantages of Mesh topology:

Reliable: The mesh topology networks are very reliable as if any link breakdown will not affect the communication between connected computers.

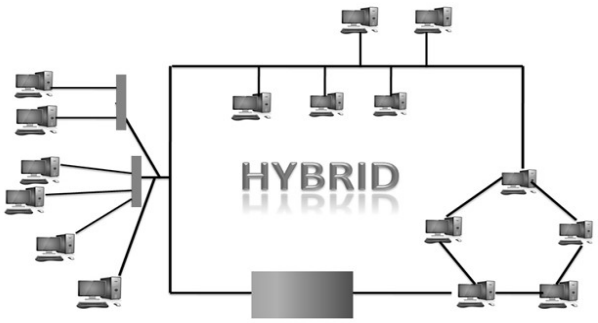
Fast Communication: Communication is very fast between the nodes.

Easier Reconfiguration: Adding new devices would not disrupt the communication between other devices.

Disadvantages of Mesh topology:

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

6) 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. For example, if there exist a ring topology in one branch of ICICI bank and bus topology in another branch of ICICI bank, connecting these two topologies will 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.

Types of Computer Networks:

1. Local Area Network (LAN)
2. Metropolitan Area Network (MAN)
3. Wide Area Network (WAN)

Local Area Network (LAN):

As the name suggests, the local area network is a computer network that operates in a small area, i.e., it connects computers in a small geographical area like within an office, company, school or any other organization. So, it exists within a specific area, e.g. home network, office network, school network, etc.

A local area network may be a wired or wireless network or a combination of both. The devices in a LAN are generally connected using an Ethernet cable, which offers an interface to connect multiple devices like router, switches, and computers. For example, using a single router, few Ethernet cables, and computers, you can create a LAN at your home, office, etc. In this network, one computer may act as a server and other computers, which are part of the network, may serve as clients.

Features of LAN:

- The network size is small, which consists of only a few kilometres.
- The data transmission rate is high, ranging from 100 Mbps to 1000 Mbps.
- LAN is included in bus, ring, mesh and star topologies.
- Some network devices connected to the LAN will be limited.
- If more devices are added than prescribed network may fail.

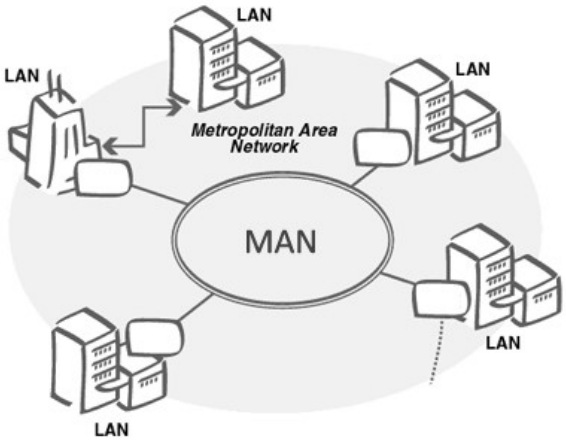
Benefits of LAN:

- It offers a higher operating speed than WAN and MAN.
- It is less expensive and easy to install and maintain.
- It perfectly fulfills the requirement of a specific organization, such as an office, school, etc.
- It can be wired or wireless or a combination of both.
- It is more secure than other networks as it is a small set up that can be easily taken care of.

Primary Functions of LAN:

- **Sharing of files:** It allows you to share or transfer files from one computer to another computer within the LAN. For example, in a bank, it can be used to send a file with the details of transactions of a customer from the server to clients.
- **Sharing of printers:** It also allows shared access to a printer, file servers, etc. For example, ten computers that are connected through LAN can use a single printer, file server, fax machine, etc.
- **Sharing of Computational capabilities:** It allows the clients to access to the computational power of a server, e.g., an application server as some applications which run on clients in a LAN may require higher computational capabilities.
- **Mail and message related services:** It allows sending and receiving mails between computers of a LAN. You are required to have a mail server for this.
- **Database services:** It also allows storing and retrieving data with the help of a database server.

Metropolitan Area Network (MAN):



MAN is a high-speed network that spreads over a large geographical area such as a metro city or town. It is set up by connecting the local area networks using routers and local telephone exchange lines. It can be operated by a private company or it may be a service provided by a company such as a local telephone company.

MAN is ideal for the people of a relatively large area who want to share data or information. It provides fast communication via high-speed carriers or transmission media such as copper, fiber optics and microwaves. The commonly used protocols for MAN are X.25, Frame Relay, Asynchronous Transfer Mode (ATM), xDSL (Digital Subscriber Line), ISDN (Integrated Services Digital Network), ADSL (Asymmetrical Digital Subscriber Line) and more. The area covered by MAN is larger than the LAN but smaller than a WAN. Its network ranges from 5 to 50 km. Furthermore, it also provides uplinks for connecting LANs to WANs and the internet. An organization can use a MAN to connect all of its LANs located at its different offices across the city.

Examples of MAN:

- Cable TV Network
- Telephone service provides that provide high-speed DSL lines
- IEEE 802.16 or WiMAX
- Connected fire stations in a city
- Connected branches of a school in a city

Features of MAN:

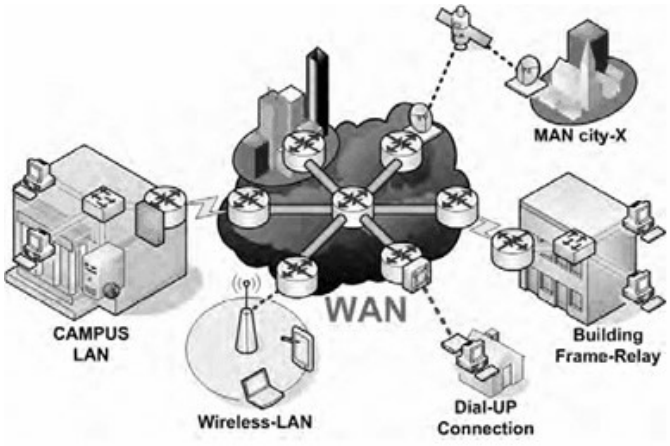
- The size of the MAN is in the range of 5km to 50km.
- The MAN ranges from the campus to the entire city.

- The MAN is maintained and managed by either the user group or the Network provider.
- Users can achieve the sharing of regional resources by using MAN.
- The data transmission rates can be medium to high

Advantages of MAN:

- **Less Expensive:** It is less expensive to set up a MAN and to connect it to a WAN.
- **High Speed:** The speed of data transfer is more than WAN.
- **Local Emails:** It can send local emails fast.
- **Access to the Internet:** It allows you to share your internet connection, and thus multiple users can have access to high-speed internet.
- **Easy to set up:** You can easily set up a MAN by connecting multiple LANs.
- **High Security:** It is more secure than WAN.

Wide Area Network (WAN):



WAN extends over a large geographical area. It is not confined within an office, school, city or town and is mainly set up by telephone lines, fiber optic, or satellite links. It is mostly used by big organizations like banks and multinational companies to communicate with their branches and customers across the world. Although it is structurally similar to MAN, it is different from MAN in terms of its range, e.g., MAN covers up to 50 Kms, whereas WAM covers distances larger than 50 Km, e.g., 1000km or more.

A WAN works by using TCP/IP protocol in combination with networking devices such as switches, routers, firewalls, and modems. It does not connect individual computers; rather, they are designed to link small networks like LANs and MANs to create a large network. The internet is considered the largest WAN in the world as it connects various LANs and MANs through ISPs.

The computers are connected to the wide area network through public networks, such as telephone systems, leased lines or satellites. The users of a WAN do not own the network as it is a large setup connecting the remote computer systems. However, they are required to subscribe to a service provided by a telecommunication provider to use this network.

Features of WAN:

- Has a much larger capacity.
- We can share the regional resources by using WAN.
- They have more bit-rate errors.
- The transmission delay is, and hence they need more communication speed.

Advantages of a WAN:

- **Large Network Range:** It spans a large geographical area of 2000 km or more, e.g., from one country to another countries.
- **Centralized data:** It allows your different office branches to use your head office server for retrieving and sharing data. Thus, you don't need to buy email servers, files server and back up servers, etc.
- **Get updated files and data:** It provides an ideal platform for companies who need a live server for their employees to exchange updated files within seconds.
- **High bandwidth:** It offers high bandwidth than a normal broadband connection. Thus, it can increase the productivity of your company by offering uninterrupted data transfer and communication.
- **Workload Distribution:** It helps distribute your workload to other locations. You can hire employees in different countries and assign them to work from your office.

Examples of WAN:

1. Internet
2. US defense department
3. Stock exchanges network
4. Railway reservation system
5. Big Banks' cash dispensers' network
6. Satellite systems

NETWORK STRUCTURE:

Network structure refers to a general system, network, or pattern of relationships that can be derived from the observable behavior of animate and inanimate actors or objects in a given population. Structure is usually understood as the arrangement of parts or elements of some complexity tied together by relations. The study of these relations is the subject of network theory.

A network consists of nodes and links that form dyads, triads, groups or a system of interconnected animate (actors) and inanimate objects, based on the specific types of relationships between them. In a dyad, ties come together, through the type of relation, to create a system of interdependence. Triads are fundamental network structures.

Network Structure Measures Network structure can be studied and measured with social and dynamic network analysis, which allows the study of network topology, network behavior, and evolution, as well as an understanding of why networks are structured the way they are. This analysis reveals the privileges of some nodes and the advantages of some types of networks over others. The basic measures at the whole network level are density and centralization.

Density measures the actual number of links between nodes in relation to all links that exist. This allows the assessment of the degree of networking of the studied system or population.

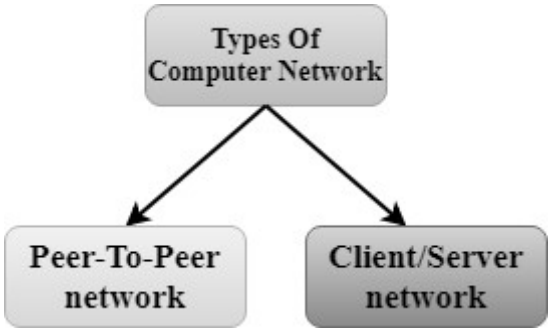
Centralization refers to the overall integration or coherence of the network. It determines the relative dominance of a single node over others in the network and then the entire network is characterized by a centralized structure in which there are many links around one node. Conversely, a network structure takes a decentralized form. Both the dense and centralized network structures have inevitable positive and negative consequences.

Network structures and positions in the network; create both opportunities and limitations depending on the functional value of the relationships studied. The network's overall efficiency can be assessed through the prism of possible fragmentation and the redundancy of nodes or relations.

Computer Network Architecture:

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.

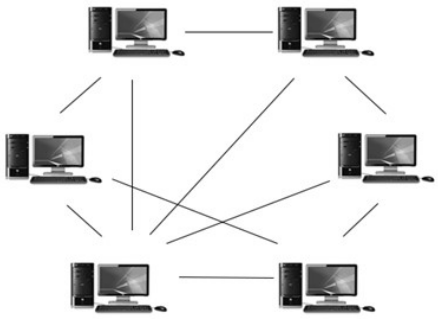
The two types of network architectures are used:



1. Peer-To-Peer network
2. Client/Server network

Peer-To-Peer network:

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



Advantages of Peer-To-Peer Network:

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

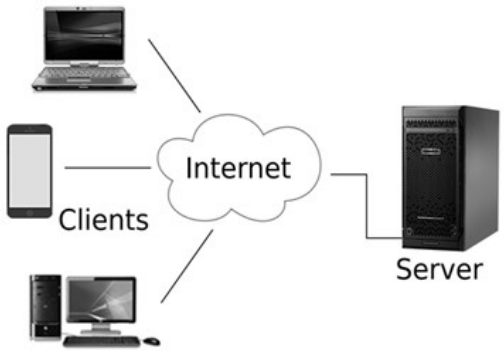
Disadvantages of Peer-To-Peer Network:

- 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.
- It has a security issue as the device is managed itself.

Client/Server Network:

- Client/Server network is a network model designed for the end users called clients, to access the resources such as songs, video, etc. from a central computer known as Server.

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



Advantages of Client/Server network:

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

Disadvantages of Client/Server network:

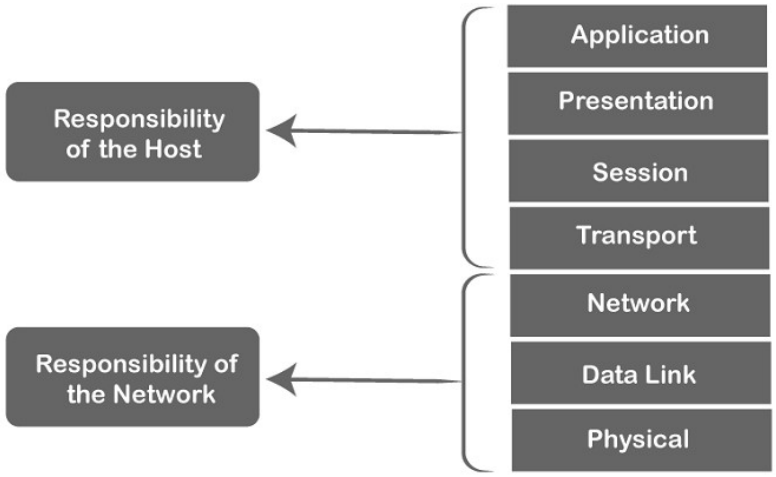
- Client/Server network is expensive as it requires the server with large memory.
- A server has a Network Operating System (NOS) to provide the resources to the clients, but the cost of NOS is very high.
- It requires a dedicated network administrator to manage all the resources.

OSI Model:

- OSI stands for Open System Interconnection is a reference model that describes how information from a software application in one computer moves through a physical medium to the software application in another computer.
- OSI consists of seven layers, and each layer performs a particular network function.
- OSI model was developed by the International Organization for Standardization (ISO) in 1984, and it is now considered as an architectural model for the inter-computer communications.

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

Characteristics of OSI Model:

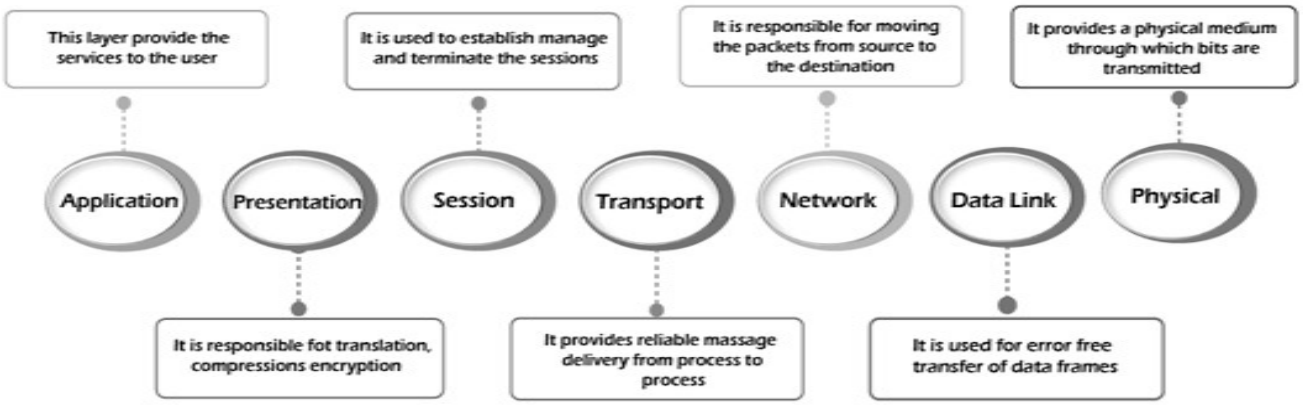


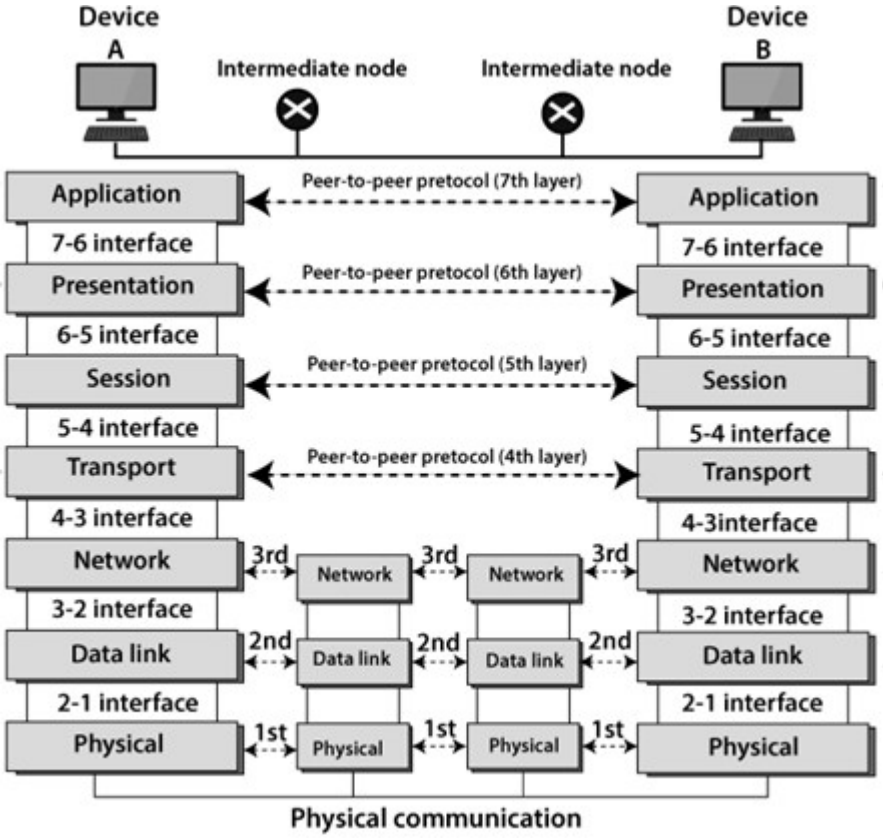
- The OSI model is divided into two layers: upper layers and lower layers.
- The upper layer of the OSI model mainly deals with the application related issues, and they are implemented only in the software. The application layer is closest to the end user. Both the end user and the application layer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

7 Layers of OSI Model:

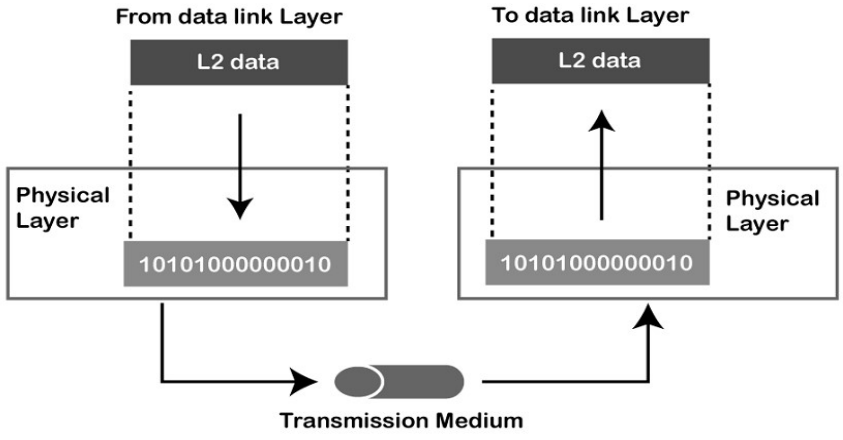
There are the seven OSI layers. Each layer has different functions. Lists of seven layers are given below:

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





1) Physical layer:

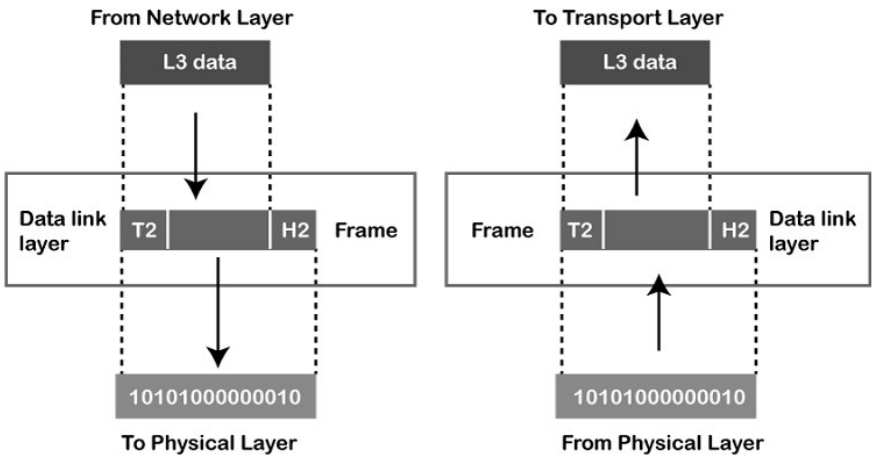


- ✓ The main functionality of the physical layer is to transmit the individual bits from one node to another node.
- ✓ It is the lowest layer of the OSI model.
- ✓ It establishes, maintains and deactivates the physical connection.
- ✓ It specifies the mechanical, electrical and procedural network interface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

Functions of a Physical layer:

- **Line Configuration:** It defines the way how two or more devices can be connected physically.
- Data Transmission**:** It defines the transmission mode whether it is simplex, half-duplex or full-duplex mode between the two devices on the network.
- Topology**:** It defines the way how network devices are arranged.
- **Signals:** It determines the type of the signal used for transmitting the information.

2) Data-Link Layer:



- This layer is responsible for the error-free transfer of data frames.
- It defines the format of the data on the network.
- It provides a reliable and efficient communication between two or more devices.
- It is mainly responsible for the unique identification of each device that resides on a local network.
- It contains two sub-layers:
    - **Logical Link Control Layer:**
        - It is responsible for transferring the packets to the Network layer of the receiver that is receiving.
        - It identifies the address of the network layer protocol from the header.
        - It also provides flow control.

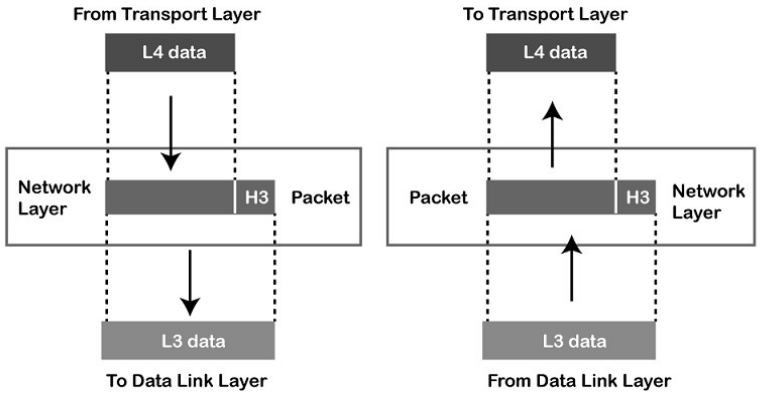
- **Media Access Control Layer:**
  - A Media access control layer is a link between the Logical Link Control layer and the network's physical layer.
  - It is used for transferring the packets over the network.

Functions of the Data-link layer:

- **Framing:** The data link layer translates the physical's raw bit stream into packets known as Frames. The Data link layer adds the header and trailer to the frame. The header which is added to the frame contains the hardware destination and source address.

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

3) Network Layer:

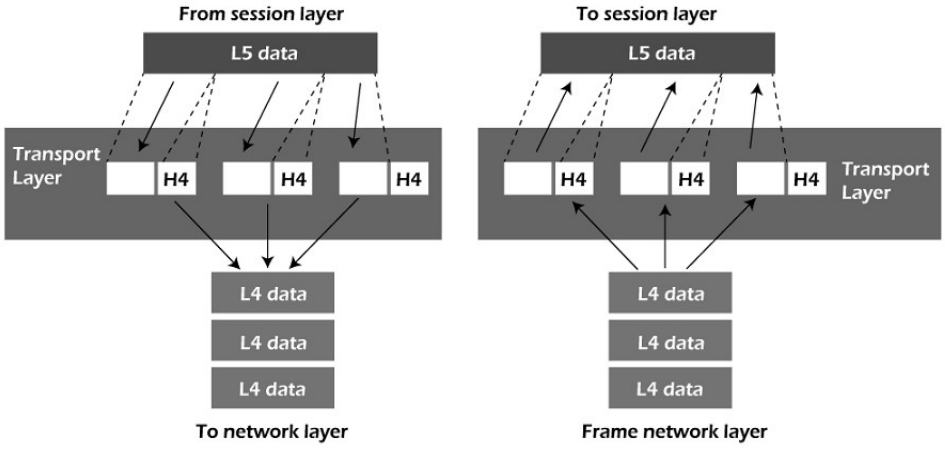


- It is a layer 3 that manages device addressing, tracks the location of devices on the network.
- It determines the best path to move data from source to the destination based on the network conditions, the priority of service and other factors.
- The Data link layer is responsible for routing and forwarding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

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

4) Transport Layer:



- 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.
- The main responsibility of the transport layer is to transfer the data completely.
- It receives the data from the upper layer and converts them into smaller units known as segments.
- 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:

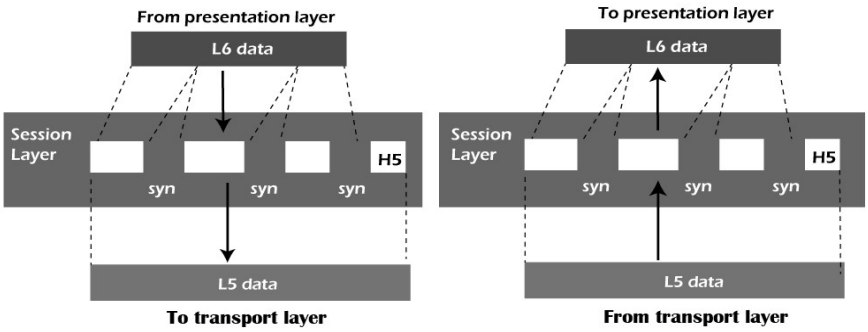
- **Transmission Control Protocol:**
  - It is a standard protocol that allows the systems to communicate over the internet.
  - It establishes and maintains a connection between hosts.
  - When data is sent over the TCP connection, then the TCP protocol divides the data into smaller units known as segments. Each segment travels over the internet using multiple routes and they arrive in different orders at the destination. The transmission control protocol reorders the packets in the correct order at the receiving end.
- **User Datagram Protocol:**
  - User Datagram Protocol is a transport layer protocol.
  - 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:

- **Service-point addressing:** Computers run several programs simultaneously due to this reason, the transmission of data from source to the destination not only from one computer to another computer but also from one process to another process. The transport layer adds the header that contains the address known as a service-point address or port address. The responsibility of the network layer is to transmit the data from one computer to another computer and the responsibility of the transport layer is to transmit the message to the correct process.
- **Segmentation and reassembly:** When the transport layer receives the message from the upper layer, it divides the message into multiple segments, and each segment is assigned with a sequence number that uniquely identifies each segment. When the message has arrived at the destination, then the transport layer reassembles the message based on their sequence numbers.
- **Connection control:** Transport layer provides two services Connection-oriented service and connectionless service. A connectionless service treats each segment as an individual packet, and they all travel in different routes to reach the destination. A connection-oriented service makes a connection with the transport layer at the destination machine before delivering the packets. In connection-oriented service, all the packets travel in the single route.
- **Flow control:** The transport layer also responsible for flow control but it is performed end-to-end rather than across a single link.

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

5) Session Layer:

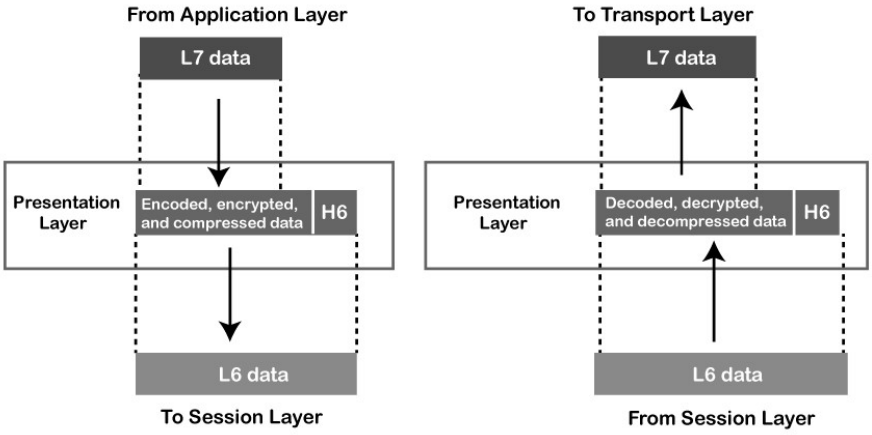


- It is a layer 3 in the OSI model.
- The Session layer is used to establish, maintain and synchronizes the interaction between communicating devices.

Functions of Session layer:

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

6) Presentation Layer:



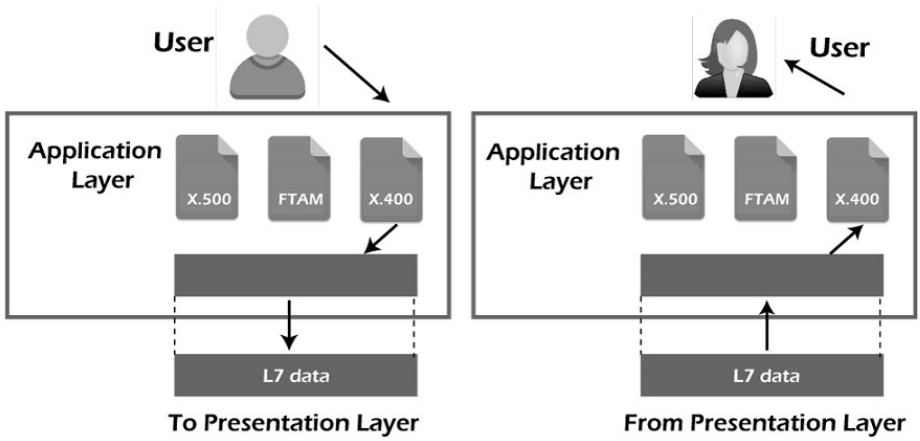
- A Presentation layer is mainly concerned with the syntax and semantics of the information exchanged between the two systems.
- It acts as a data translator for a network.

- This layer is a part of the operating system that converts the data from one presentation format to another format.
- The Presentation layer is also known as the syntax layer.

Functions of Presentation layer:

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

7) Application Layer:



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

Functions of Application layer:

- **File transfer, access and management (FTAM):** An application layer allows a user to access the files in a remote computer, to retrieve the files from a computer and to manage the files in a remote computer.
- **Mail services:** An application layer provides the facility for email forwarding and storage.

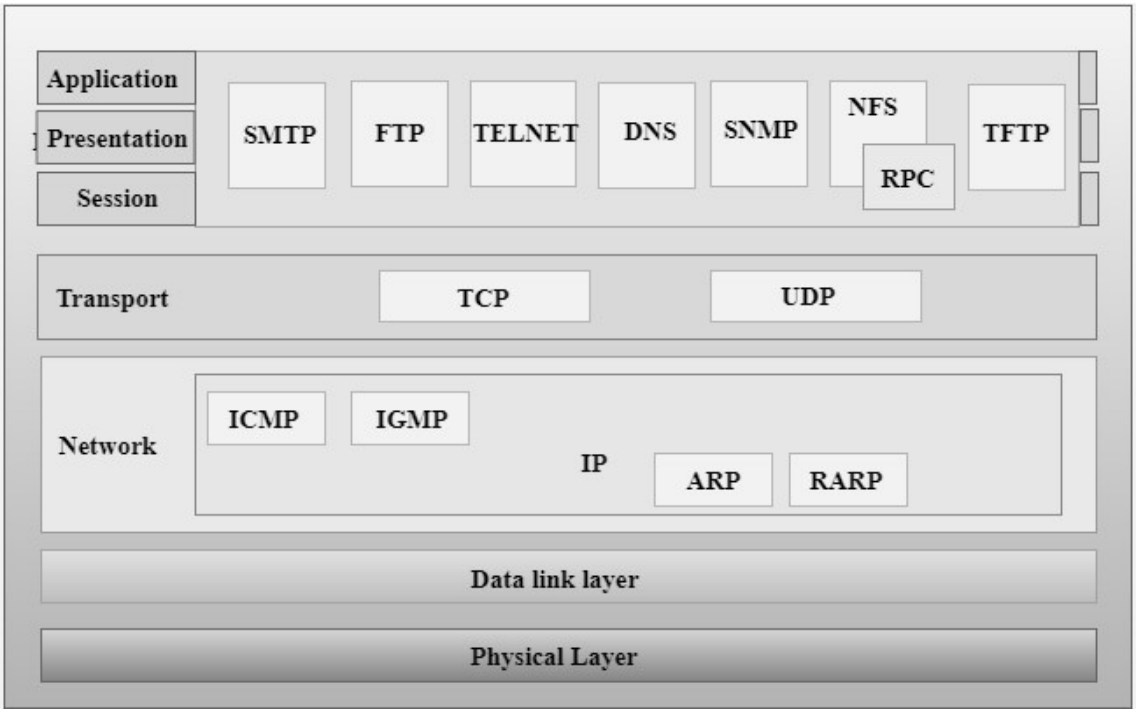
- **Directory services:** An application provides the distributed database sources and is used to provide that global information about various objects.

TCP/IP Model:

1. The TCP/IP model was developed prior to the OSI model.
2. The TCP/IP model is not exactly similar to the OSI model.
3. The TCP/IP model consists of five layers: the application layer, transport layer, network layer, data link layer and physical layer.
4. The first four layers provide physical standards, network interface, internetworking, and transport functions that correspond to the first four layers of the OSI model and these four layers are represented in TCP/IP model by a single layer called the application layer.
5. 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:

- 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 on the same network.
- 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.
- The protocols used by this layer are ethernet, token ring, FDDI, X.25, frame relay.

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:

IP Protocol: 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 unit, 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.

ARP Protocol:

- ✓ 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 send 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

ICMP Protocol:

- ❖ 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.

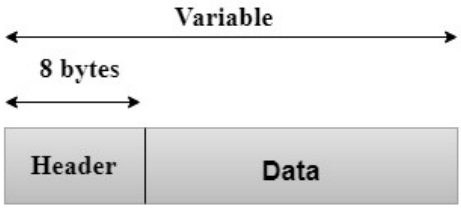
Transport Layer:

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.

- **User Datagram Protocol (UDP):**

  - It provides connectionless service and end-to-end delivery of transmission.
  - It is an unreliable protocol as it discovers the errors but 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.
  - UDP consists of the following fields:
    Source port address: The source port address is the address of the application program that has created the message.
    Destination port address: The destination port address is the address of the application program that receives the message.
    Total length: It defines the total number of bytes of the user datagram in bytes.
    Checksum: The checksum is a 16-bit field used in error detection.
  - UDP does not specify which packet is lost. UDP contains only checksum; it does not contain any ID of a data segment.



Header Format

Source port address 16 bits	Destination port address 16 bits
Total length 16 bits	Checksum 16 bits

- **Transmission Control Protocol (TCP):**

1. It provides a full transport layer services to applications.
2. It creates a virtual circuit between the sender and receiver, and it is active for the duration of the transmission.
3. 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 and a virtual circuit is discarded.

4. 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.
5. At the receiving end, TCP collects all the segments and reorders them based on sequence numbers.

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:

- ❖ **HTTP:** HTTP stands for Hypertext transfer protocol. This protocol allows us to access the data over the World Wide Web. It transfers the data in the form of plain text, audio, video. It is known as a Hypertext transfer protocol as it has the efficiency to use in a hypertext environment where there are rapid jumps from one document to another.
- ❖ **SNMP:** SNMP stands for Simple Network Management Protocol. It is a framework used for managing the devices on the internet by using the TCP/IP protocol suite.
- ❖ **SMTP:** SMTP stands for Simple mail transfer protocol. The TCP/IP protocol that supports the e-mail is known as a Simple mail transfer protocol. This protocol is used to send the data to another e-mail address.
- ❖ **DNS:** DNS stands for Domain Name System. An IP address is used to identify the connection of a host to the internet uniquely. But, people prefer to use the names instead of addresses. Therefore, the system that maps the name to the address is known as Domain Name System.
- ❖ **TELNET:** It is an abbreviation for Terminal Network. It establishes the connection between the local computer and remote computer in such a way that the local terminal appears to be a terminal at the remote system.
- ❖ **FTP:** FTP stands for File Transfer Protocol. FTP is a standard internet protocol used for transmitting the files from one computer to another computer.

Transmission media:

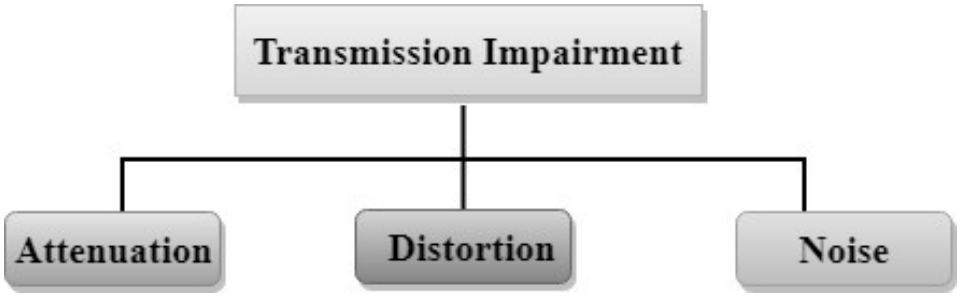
What is Transmission media?

- Transmission media is a communication channel that carries the information from the sender to the receiver. Data is transmitted through the electromagnetic signals.
- The main functionality of the transmission media is to carry the information in the form of bits through LAN (Local Area Network).
- It is a physical path between transmitter and receiver in data communication.
- In a copper-based network, the bits in the form of electrical signals.
- In a fibre based network, the bits in the form of light pulses.
- In OSI (Open System Interconnection) phase, transmission media supports the Layer 1. Therefore, it is considered to be as a Layer 1 component.
- The electrical signals can be sent through the copper wire, fibre optics, atmosphere, water and vacuum.
- The characteristics and quality of data transmission are determined by the characteristics of medium and signal.
- 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.
- Different transmission media have different properties such as bandwidth, delay, cost and ease of installation and maintenance.
- 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:

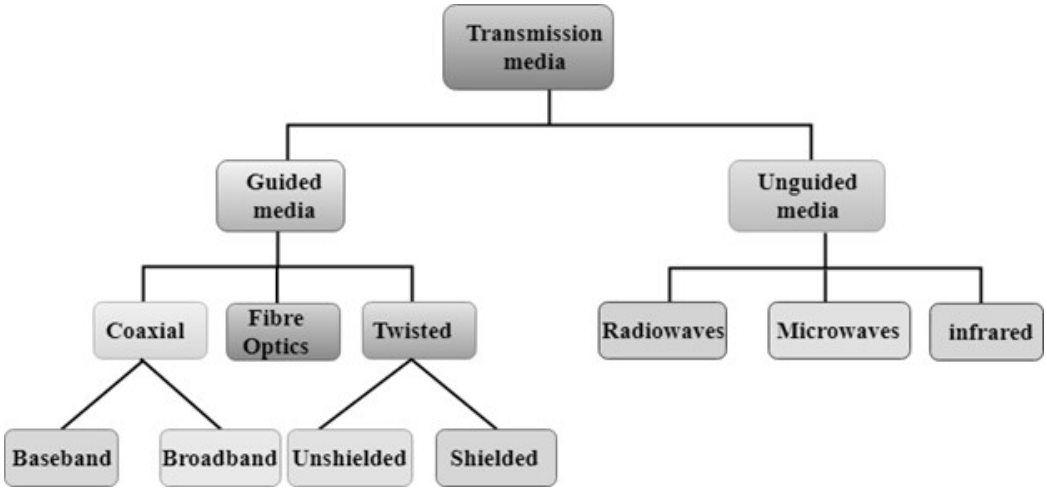
- **Bandwidth:** All the factors are remaining constant, the greater the bandwidth of a medium, the higher the data transmission rate of a signal.
- **Transmission impairment:** When the received signal is not identical to the transmitted one due to the transmission impairment. The quality of the signals will get destroyed due to transmission impairment.
- **Interference:** 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:



- **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.
- **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.
- **Noise:** When data is travelled over a transmission medium, some unwanted signal is added to it which creates the noise.

Classification of Transmission Media:



1. Guided Transmission Media
2. Unguided Transmission Media

Guided Media:

It is defined as the physical medium through which the signals are transmitted. It is also known as Bounded media.

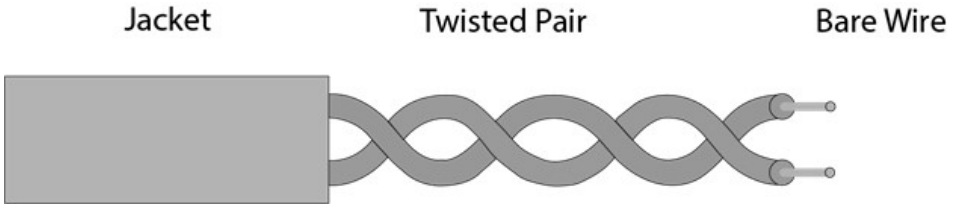
Types of Guided media:

Twisted pair:

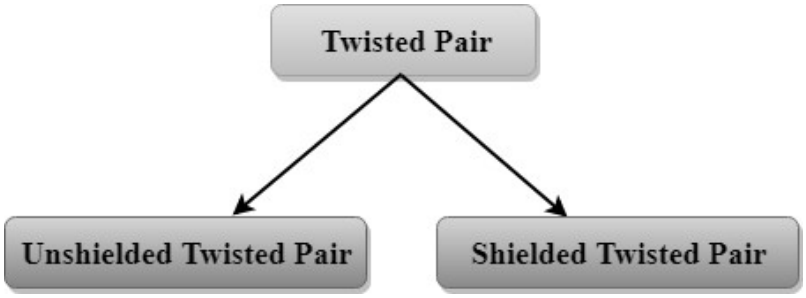
Twisted pair is a physical media made up of a pair of cables twisted with each other. A twisted pair cable is cheap as compared to other transmission media. Installation of the twisted pair cable is easy, and it is a lightweight cable. The frequency range for twisted pair cable is from 0 to 3.5KHz.

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:

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

Advantages of Unshielded Twisted Pair:

1. It is cheap.
2. Installation of the unshielded twisted pair is easy.
3. It can be used for high-speed LAN.

Disadvantage:

- 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.

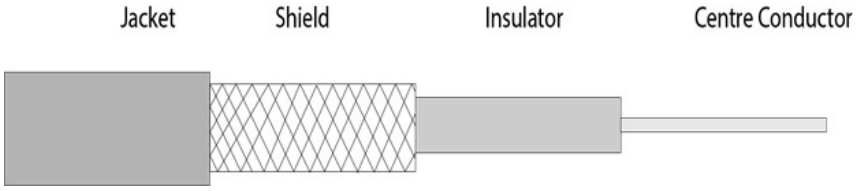
- It has higher capacity as compared to unshielded twisted pair cable.
- It has a higher attenuation.
- It is shielded that provides the higher data transmission rate.

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).



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.

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

Diagrammatic representation of fibre optic cable:

Basic elements of Fibre optic cable:

1. **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.
2. **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.
3. **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:

- **Greater Bandwidth:** The fibre optic cable provides more bandwidth as compared copper. Therefore, the fibre optic carries more data as compared to copper cable.
- **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.
- **Longer distances:** The fibre optic cable carries the data at a longer distance as compared to copper cable.
- **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.
- **Thinner and Sturdier:** Fibre optic cable is thinner and lighter in weight so it can withstand more pull pressure than copper cable.

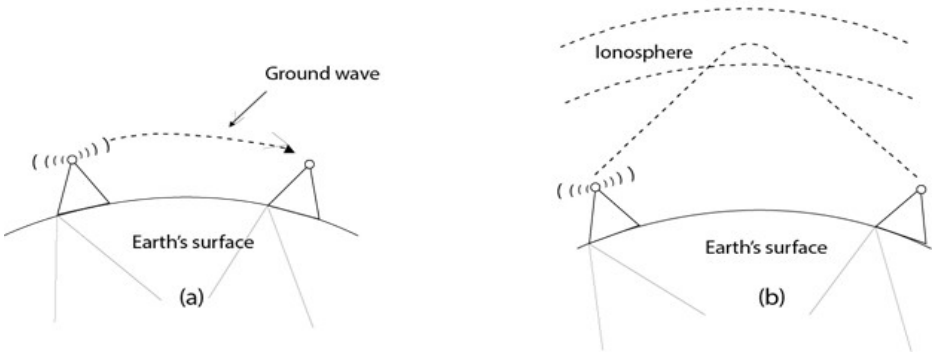
Unguided Transmission:

- An unguided transmission transmits the electromagnetic waves without using any physical medium. Therefore it is also known as wireless transmission.
- In unguided media, air is the media through which the electromagnetic energy can flow easily.

Unguided transmission is broadly classified into three categories:

1. Radio waves:

1. Radio waves are the electromagnetic waves that are transmitted in all the directions of free space.
2. Radio waves are omnidirectional, i.e., the signals are propagated in all the directions.
3. The range in frequencies of radio waves is from 3Khz to 1 khz.
4. 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.
5. An example of the radio wave is FM radio.



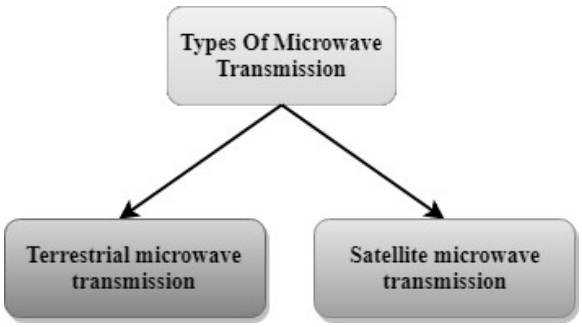
Applications of Radio waves:

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

Advantages of Radio transmission:

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

2. Microwaves:



Microwaves are of two types:

1. Terrestrial microwave
2. Satellite microwave communication.

Terrestrial Microwave Transmission:

- ✓ Terrestrial Microwave transmission is a technology that transmits the focused beam of a radio signal from one ground-based microwave transmission antenna to another.
- ✓ Microwaves are the electromagnetic waves having the frequency in the range from 1GHz to 1000 GHz.
- ✓ Microwaves are unidirectional as the sending and receiving antenna is to be aligned, i.e., the waves sent by the sending antenna are narrowly focused.
- ✓ In this case, antennas are mounted on the towers to send a beam to another antenna which is km away.
- ✓ 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:

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

Advantages of Microwave:

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

Disadvantages of Microwave transmission:

- ❖ Eavesdropping: An eavesdropping creates insecure communication. Any malicious user can catch the signal in the air by using its own antenna.
- ❖ Out of phase signal: A signal can be moved out of phase by using microwave transmission.
- ❖ 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.

- ❖ Bandwidth limited: Allocation of bandwidth is limited in the case of microwave transmission.
- ❖ Satellite Microwave Communication
- ❖ A satellite is a physical object that revolves around the earth at a known height.
- ❖ Satellite communication is more reliable nowadays as it offers more flexibility than cable and fibre optic systems.
- ❖ 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:

- ✓ Satellite designing and development requires more time and higher cost.
- ✓ The Satellite needs to be monitored and controlled on regular periods so that it remains in orbit.
- ✓ 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:

1. An infrared transmission is a wireless technology used for communication over short ranges.
2. The frequency of the infrared in the range from 300 GHz to 400 THz.
3. 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:

- ➢ It supports high bandwidth, and hence the data rate will be very high.
- ➢ Infrared waves cannot penetrate the walls. Therefore, the infrared communication in one room cannot be interrupted by the nearby rooms.

- An infrared communication provides better security with minimum interference.
- Infrared communication is unreliable outside the building because the sun rays will interfere with the infrared waves.

Multiplexing:

Multiplexing is a technique used to combine and send the multiple data streams over a single medium. The process of combining the data streams is known as multiplexing and hardware used for multiplexing is known as a multiplexer.

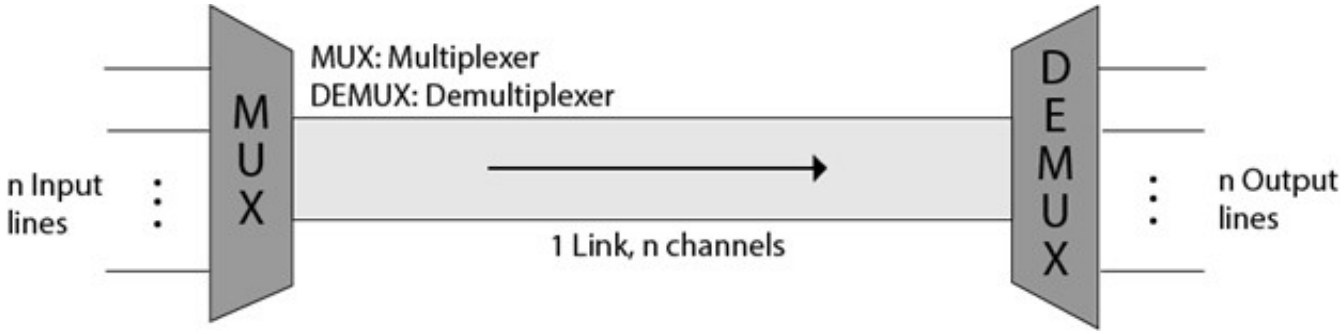
Multiplexing is achieved by using a device called Multiplexer (MUX) that combines n input lines to generate a single output line. Multiplexing follows many-to-one, i.e., n input lines and one output line.

Demultiplexing is achieved by using a device called Demultiplexer (DEMUX) available at the receiving end. DEMUX separates a signal into its component signals (one input and n outputs). Therefore, we can say that demultiplexing follows the one-to-many approach.

Why Multiplexing?

- The transmission medium is used to send the signal from sender to receiver. The medium can only have one signal at a time.
- If there are multiple signals to share one medium, then the medium must be divided in such a way that each signal is given some portion of the available bandwidth. For example: If there are 10 signals and bandwidth of medium is100 units, then the 10 unit is shared by each signal.
- When multiple signals share the common medium, there is a possibility of collision. Multiplexing concept is used to avoid such collision.
- Transmission services are very expensive.

Concept of Multiplexing:



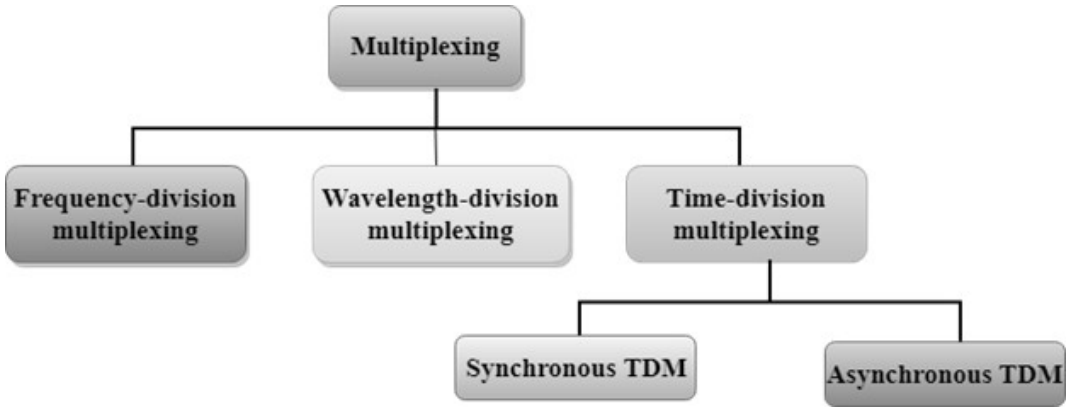
- The 'n' input lines are transmitted through a multiplexer and multiplexer combines the signals to form a composite signal.
- The composite signal is passed through a Demultiplexer and demultiplexer separates a signal to component signals and transfers them to their respective destinations.

Advantages of Multiplexing:

- More than one signal can be sent over a single medium.
- The bandwidth of a medium can be utilized effectively.

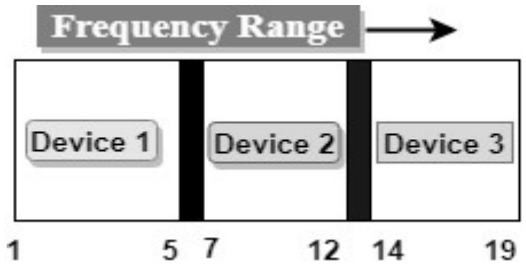
Multiplexing Techniques:

Multiplexing techniques can be classified as:

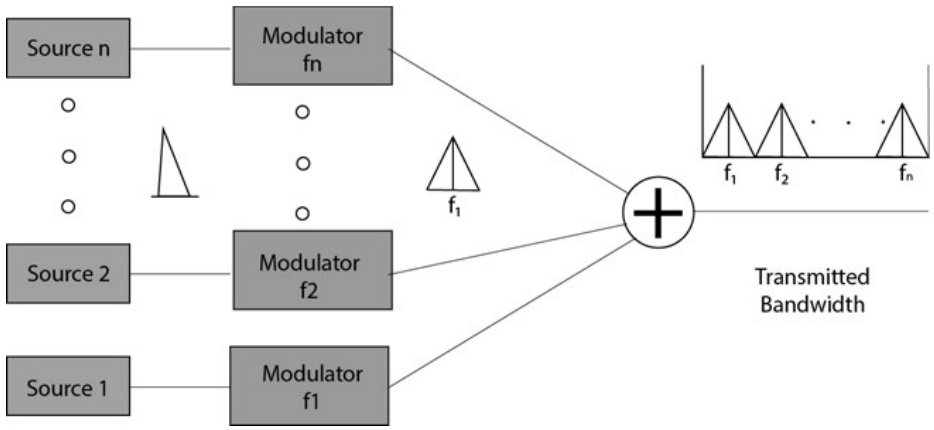


Frequency-division Multiplexing (FDM):

- It is an analog technique.
- Frequency Division Multiplexing is a technique in which the available bandwidth of a single transmission medium is subdivided into several channels.



- In the above diagram, a single transmission medium is subdivided into several frequency channels, and each frequency channel is given to different devices. Device 1 has a frequency channel of range from 1 to 5.
- The input signals are translated into frequency bands by using modulation techniques and they are combined by a multiplexer to form a composite signal.
- The main aim of the FDM is to subdivide the available bandwidth into different frequency channels and allocate them to different devices.
- Using the modulation technique, the input signals are transmitted into frequency bands and then combined to form a composite signal.
- The carriers which are used for modulating the signals are known as sub-carriers. They are represented as f1, f2… fn.
- FDM is mainly used in radio broadcasts and TV networks.



Advantages of FDM:

- ✓ FDM is used for analog signals.
- ✓ FDM process is very simple and easy modulation.
- ✓ A Large number of signals can be sent through an FDM simultaneously.
- ✓ It does not require any synchronization between sender and receiver.

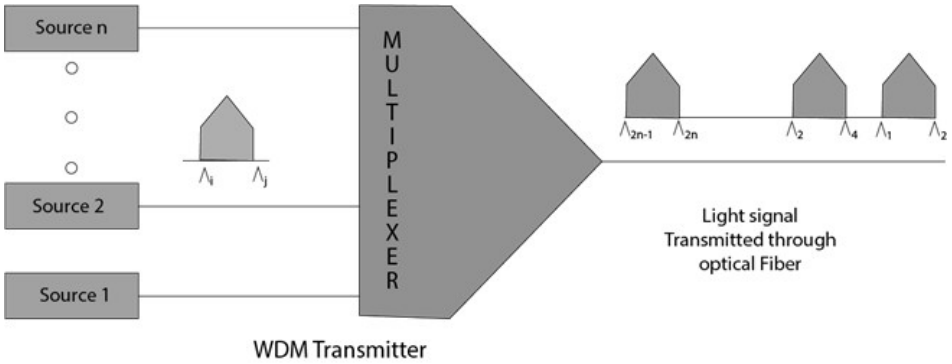
Disadvantages of FDM:

- ➢ FDM technique is used only when low-speed channels are required.
- ➢ It suffers the problem of crosstalk.
- ➢ A Large number of modulators are required.
- ➢ It requires a high bandwidth channel.

Applications of FDM:

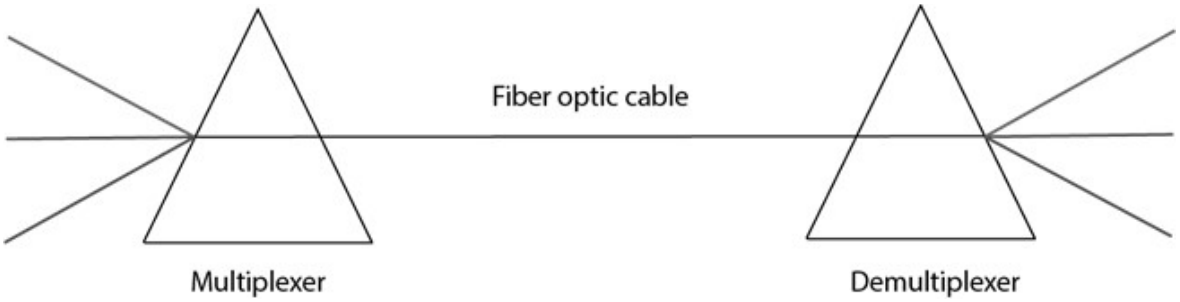
- o FDM is commonly used in TV networks.
- o It is used in FM and AM broadcasting. Each FM radio station has different frequencies, and they are multiplexed to form a composite signal. The multiplexed signal is transmitted in the air.

Wavelength Division Multiplexing (WDM):



- Wavelength Division Multiplexing is same as FDM except that the optical signals are transmitted through the fibre optic cable.
- WDM is used on fibre optics to increase the capacity of a single fibre.

- It is used to utilize the high data rate capability of fibre optic cable.
- It is an analog multiplexing technique.
- Optical signals from different source are combined to form a wider band of light with the help of multiplexer.
- At the receiving end, demultiplexer separates the signals to transmit them to their respective destinations.
- Multiplexing and Demultiplexing can be achieved by using a prism.
- Prism can perform a role of multiplexer by combining the various optical signals to form a composite signal, and the composite signal is transmitted through a fibre optical cable.
- Prism also performs a reverse operation, i.e., demultiplexing the signal.



Time Division Multiplexing:

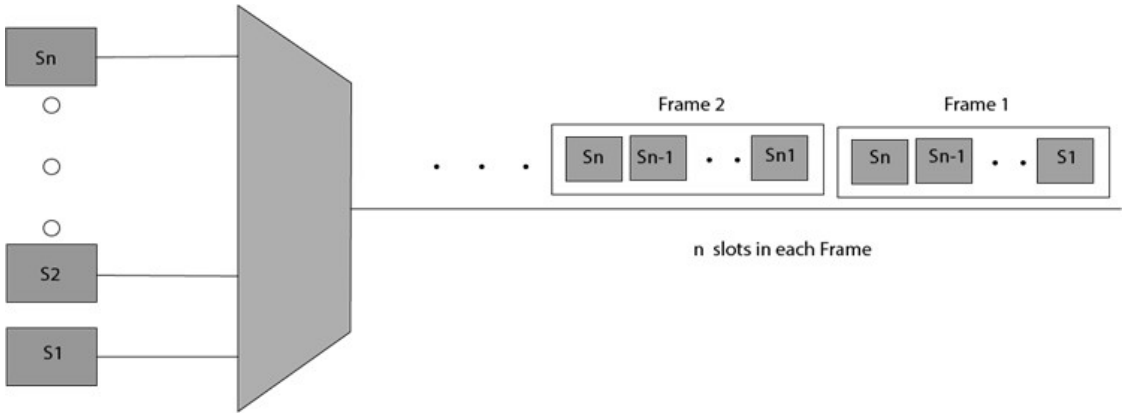
- It is a digital technique.
- In Frequency Division Multiplexing Technique, all signals operate at the same time with different frequency, but in case of Time Division Multiplexing technique, all signals operate at the same frequency with different time.
- In Time Division Multiplexing technique, the total time available in the channel is distributed among different users. Therefore, each user is allocated with different time interval known as a Time slot at which data is to be transmitted by the sender.
- A user takes control of the channel for a fixed amount of time.
- In Time Division Multiplexing technique, data is not transmitted simultaneously rather the data is transmitted one-by-one.
- In TDM, the signal is transmitted in the form of frames. Frames contain a cycle of time slots in which each frame contains one or more slots dedicated to each user.
- It can be used to multiplex both digital and analog signals but mainly used to multiplex digital signals.

There are two types of TDM:

1. Synchronous TDM
2. Asynchronous TDM

Synchronous TDM:

- A Synchronous TDM is a technique in which time slot is preassigned to every device.
- In Synchronous TDM, each device is given some time slot irrespective of the fact that the device contains the data or not.
- If the device does not have any data, then the slot will remain empty.
- In Synchronous TDM, signals are sent in the form of frames. Time slots are organized in the form of frames. If a device does not have data for a particular time slot, then the empty slot will be transmitted.
- The most popular Synchronous TDM are T-1 multiplexing, ISDN multiplexing and SONET multiplexing.
- If there are n devices, then there are n slots.



Disadvantages of Synchronous TDM:

- The capacity of the channel is not fully utilized as the empty slots are also transmitted which is having no data. In the above figure, the first frame is completely filled, but in the last two frames, some slots are empty. Therefore, we can say that the capacity of the channel is not utilized efficiently.
- The speed of the transmission medium should be greater than the total speed of the input lines. An alternative approach to the Synchronous TDM is Asynchronous Time Division Multiplexing.

Asynchronous TDM:

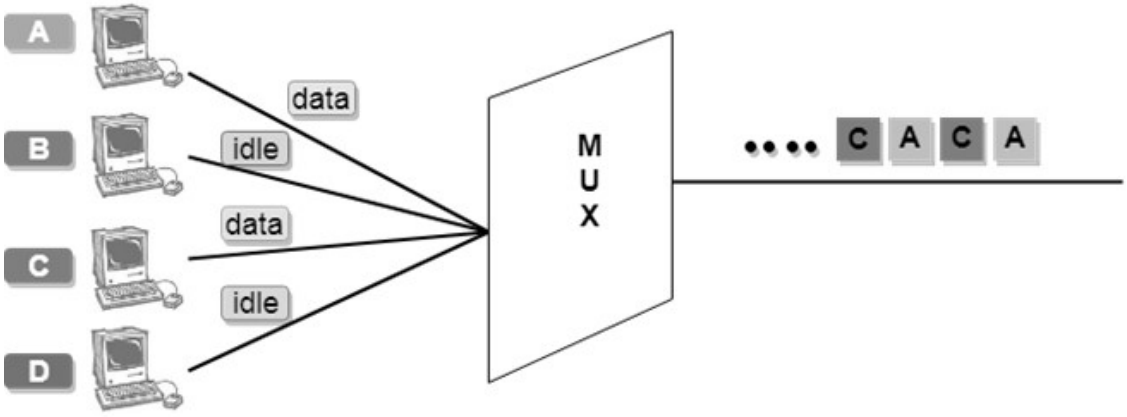
- An asynchronous TDM is also known as Statistical TDM.
- An asynchronous TDM is a technique in which time slots are not fixed as in the case of Synchronous TDM. Time slots are allocated to only those devices which have the data to send. Therefore, we can say that Asynchronous Time Division multiplexor transmits only the data from active workstations.
- An asynchronous TDM technique dynamically allocates the time slots to the devices.

- In Asynchronous TDM, total speed of the input lines can be greater than the capacity of the channel.
- Asynchronous Time Division multiplexor accepts the incoming data streams and creates a frame that contains only data with no empty slots.
- In Asynchronous TDM, each slot contains an address part that identifies the source of the data.

ADDRESS	DATA

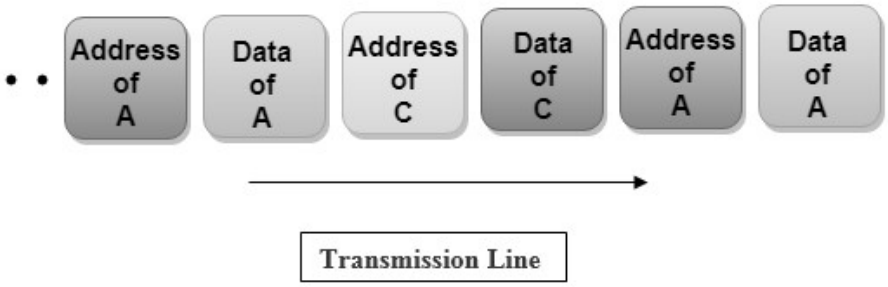
- The difference between Asynchronous TDM and Synchronous TDM is that many slots in Synchronous TDM are unutilized, but in Asynchronous TDM, slots are fully utilized. This leads to the smaller transmission time and efficient utilization of the capacity of the channel.
- In Synchronous TDM, if there are n sending devices, then there are n time slots. In Asynchronous TDM, if there are n sending devices, then there are m time slots where m is less than n (m<n).
- The number of slots in a frame depends on the statistical analysis of the number of input lines.

Concept of Asynchronous TDM:



In the above diagram, there are 4 devices, but only two devices are sending the data, i.e., A and C. Therefore, the data of A and C are only transmitted through the transmission line.

Frame of above diagram can be represented as:



The above figure shows that the data part contains the address to determine the source of the data.