# Data Communication & Computer Networks

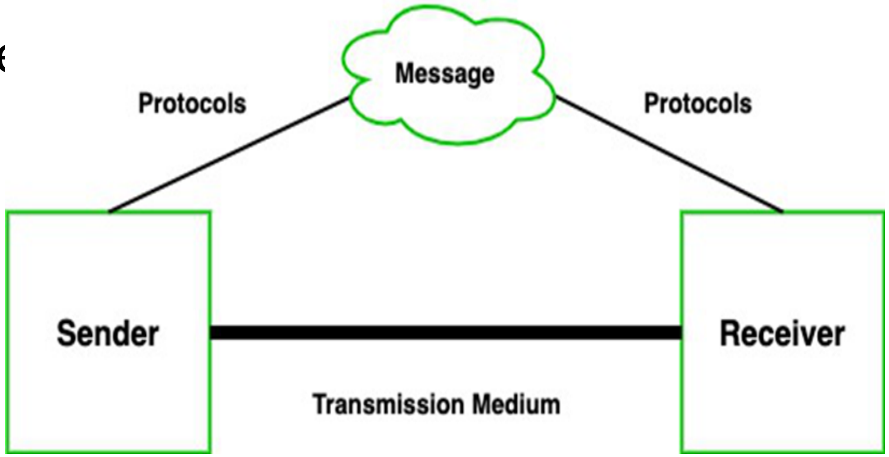
UNIT-1

# Data Communication

- Communication is defined as a process in which more than one computer transfers information, instructions to each other and for sharing resources.
- Or in other words, communication is a process or act in which we can send or receive data.
- A network of computers is defined as an interconnected collection of autonomous computers.
- Autonomous means no computer can start, stop or control another computer.

# Components of Data Communication

- A communication system is made up of the following components:
- **Message:** A message is a piece of information that is to be transmitte from one person to another. It cou be a text file, an audio file, a video file, etc.
- **Sender:** It is simply a device that sends data messages. It can be a computer, mobile, telephone, laptop, video camera, or workstation, etc.
- **Receiver:** It is a device that receives messages. It can be a computer, telephone mobile, workstation, etc.



- **Transmission Medium / Communication Channels:** Communication channels are the medium that connect two or more workstations. Workstations can be connected by either wired media or wireless media.
- **Set of rules (Protocol):** When someone sends the data (The sender), it should be understandable to the receiver also otherwise it is meaningless.

- Therefore, there are some set of rules (protocols) that is followed by every computer connected to the internet and they are:
- **TCP(Transmission Control Protocol)**: It is responsible for dividing messages into packets on the source computer and reassembling the received packet at the destination or recipient computer. It also makes sure that the packets have the information about the source of the message data, the destination of the message data, the sequence in which the message data should be re-assembled, and checks if the message has been sent correctly to the specific destination.
- **IP(Internet Protocol)**: Do You ever wonder how computer determines which packet belongs to which device. What happens if the message you sent to your friend is received by your father? Scary Right. Well! IP is responsible for handling the address of the destination computer so that each packet is sent to its proper destination.

# Type of data communication

- **Simplex Communication:** It is one-way communication or we can say that unidirectional communication in which one device only receives and another device only sends data and devices uses their entire capacity in transmission. For example, IoT, entering data using a keyboard, listing music using a speaker, etc.
- **Half Duplex communication:** It is a two-way communication, or we can say that it is a bidirectional communication in which both the devices can send and receive data but not at the same time. When one device is sending data then another device is only receiving and vice-versa. For example, walkie-talkie.
- **Full-duplex communication:** It is a two-way communication or we can say that it is a bidirectional communication in which both the devices can send and receive data at the same time. For example, mobile phones, landlines, etc.

# Communication Channels

- Communication channels are the medium that connects two or more workstations. Workstations can be connected by either wired media or wireless media. It is also known as a transmission medium. The transmission medium or channel is a link that carries messages between two or more devices. We can group the communication media into two categories:
  - Guided media transmission
  - Unguided media transmission

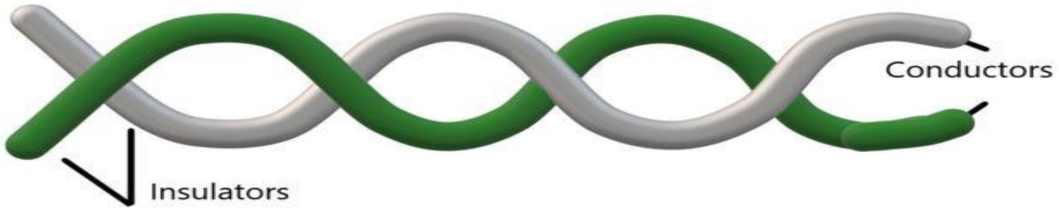
- Guided media
  - Twisted pair cable
  - Coaxial Cable
  - Optical fibers
- Unguided Media
  - Microwave
  - Radio wave
  - Infrared

# Types of Transmission Media

- Transmission media refer to the physical pathways through which data is transmitted from one device to another within a network. These pathways can be wired or wireless. The choice of medium depends on factors like distance, speed, and interference.

# Guided media

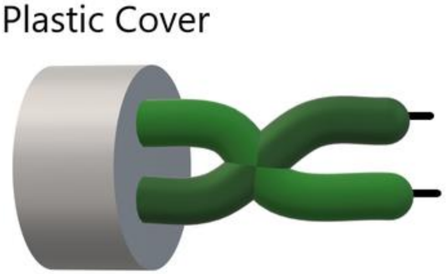
- Twisted pair cable - These are a type of guided media. It was invented by Alexander Graham Bell. Twisted pair cables have two conductors that are generally made up of copper and each conductor has insulation. These two conductors are twisted together, thus giving the name twisted pair cables.
-



- **Twisted Pair Cables are further of two types :**

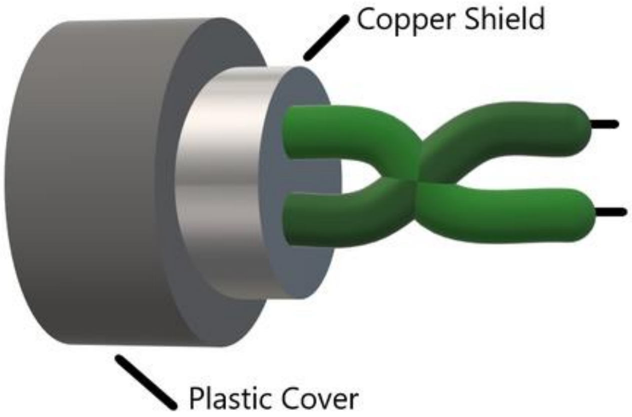
**1. Unshielded Twisted Pair Cables (UTP) :**

  - These are a pair of two insulated copper wires twisted together without any other insulation or shielding and hence are called unshielded twisted pair cables.
  - They reduce the external interference due to the presence of insulation.
  - Unshielded twisted pair cables are arranged in pairs so that we can add a new connection whenever required.



## 2. Shielded Twisted Pair Cables (STP)

- These types of cables have extra insulation or protective covering over the conductors in the form of a copper braid covering.
- This covering provides strength to the overall structure of the cable. It also reduces noise and signal interference in the cable.



- **Applications of Twisted pair cables :**
  - Twisted Pair cables are used in telephone lines to provide data and voice channels.
  - The DSL lines make use of these cables.
  - Local Area Networks (LAN) also make use of twisted pair cables.
  - They can be used for both analog and digital transmission.
  - RJ-45 is a very common application of twisted pair cables.

# Advantages

- Cost-effective: Twisted pair cables are the most cost-effective option for communication and networking.
- Easy to install: They are easy to install and terminate, making them ideal for small to medium-sized networks.
- Flexibility: Twisted pair cables come in different categories, including Cat5, Cat6, and Cat7, offering different levels of performance and flexibility.
- Suitable for short distances: Twisted pair cables are suitable for communication over short distances, making them ideal for use in homes and small businesses.

# Disadvantages

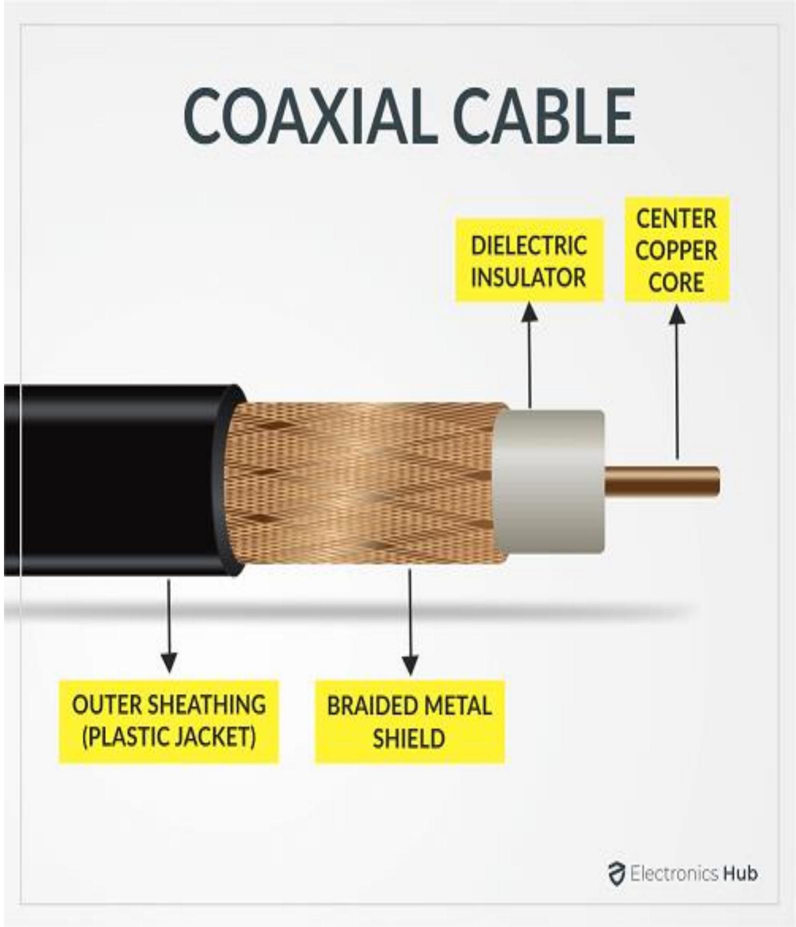
- Limited bandwidth: Twisted pair cables have limited bandwidth, which can restrict data transfer rates and performance.
- Susceptible to interference: Twisted pair cables are susceptible to interference from other electrical equipment, leading to data errors and loss.
- Limited distance: Twisted pair cables are limited in terms of distance, making them less suitable for larger networks.

# Coaxial Cable

- Coaxial Cable is a type of guided media made of Plastics, and copper wires which transmit the signal in electrical form rather than light form. Coaxial cable is also known as **coax.**
- The core copper conductor is used for the transmission of signals and the insulator is used to provide insulation to the copper conductor the insulator is surrounded by a braided metal conductor which helps to prevent the interference of electrical signals and prevent cross talk.
- This entire setup is again covered with a protective plastic layer to provide extra safety to the cable.

# Structure of Coaxial Cable

- **Copper conductor:** A central conductor, which consists of copper. The conductor is the point at which data is transmitted.
- **Insulator:** Dielectric plastic insulation around the copper conductor. it is used to maintain the spacing between the center conductor and shield.



- **Braided mesh:** A braided mesh of copper helps to shield from electromagnetic interference, The braid provides a barrier against EMI moving into and out of the coaxial cable.
- **Protective plastic layer:** An external polymer layer, which has a plastic coating. It is used to protect internal layers from damage.

**Advantages of Coaxial Cable**

- Coaxial cables support high bandwidth.
- It is easy to install coaxial cables.
- Coaxial cables have better cut-through resistance so they are more reliable and durable.
- Less affected by noise or cross-talk or electromagnetic inference.
- Coaxial cables support multiple channels

**Disadvantages of Coaxial Cable**

- Coaxial cables are expensive.
- The coaxial cable must be grounded in order to prevent any crosstalk.
- As a Coaxial cable has multiple layers it is very bulky.
- There is a chance of breaking the coaxial cable and attaching a “t-joint” by hackers, this compromises the security of the data.

# Uses of Coaxial Cable

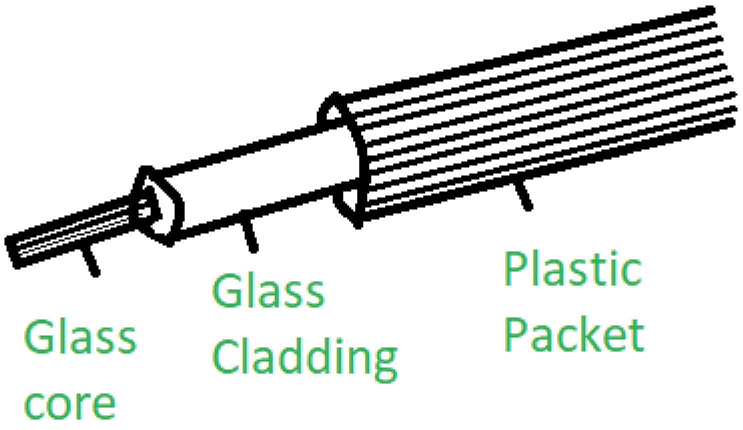
- Television
- Internet
- CCTV
- Video
- HDTV

# Fiber Optics

- Fiber optics refers to the technology and method of transmitting information as light pulses along a glass or plastic strand or fiber.
- Fiber optic cables are used for long-distance and high-performance data networking.
- They are capable of transmitting data over longer distances and at higher bandwidths (data rates) than electrical cables, making them a critical component in modern telecommunications, internet, and computer networking.

# Main Elements of Fiber Optics

- **Core:** It is the central tube of very thin size made of optically transparent dielectric medium and carries the light transmitter to receiver and the core diameter may vary from about 5um to 100 um.



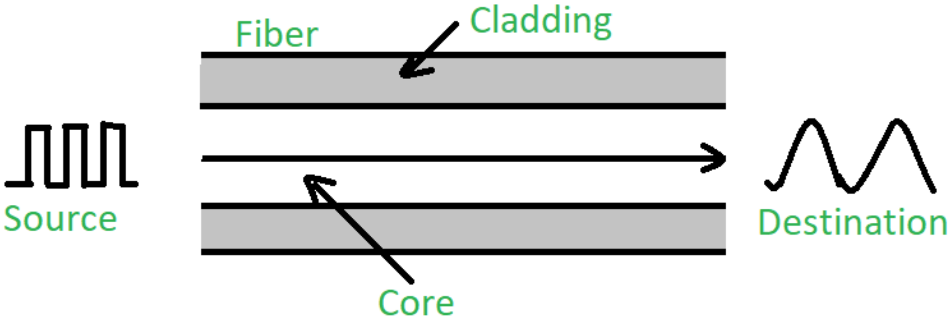
- **Cladding:** It is an outer optical material surrounding the core having a reflecting index lower than the core and cladding helps to keep the light within the core throughout the phenomena of total internal reflection.
- **Buffer Coating:** It is a plastic coating that protects the fiber made of silicon rubber. The typical diameter of the fiber after the coating is 250-300 um.

# Types of Fiber Optics

- There are different types of fiber optics based on several categories as mentioned below:
- **Based on the Number of Modes**

  **1. Single-mode fiber:** In single-mode fiber, only one type of ray of light can propagate through the fiber. This type of fiber has a small core diameter (5um) and high cladding diameter (70um) and the difference between the refractive index of core and cladding is very small.

- There is no dispersion i.e. no degradation of the signal during traveling through the fiber. The light is passed through it through a laser diode.

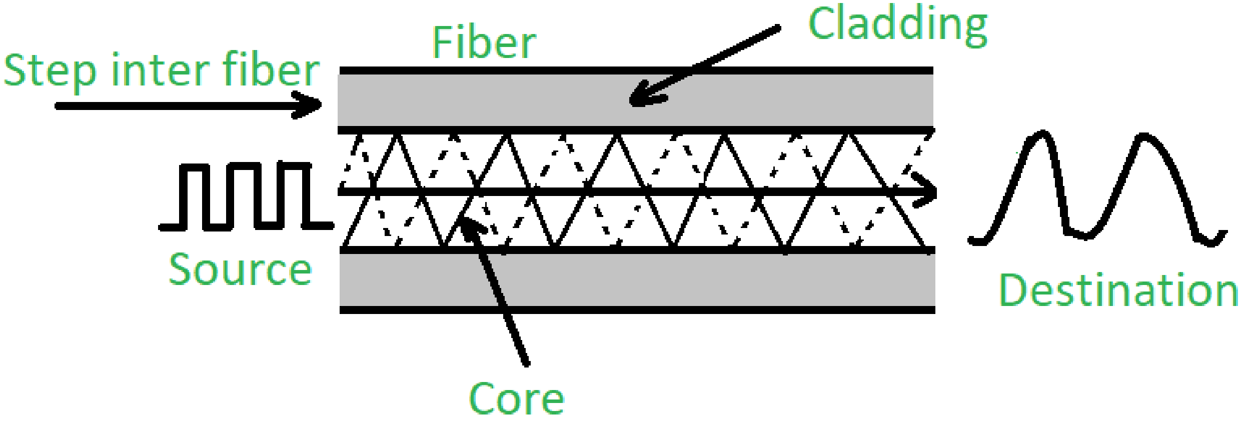


**2. Multi-mode fiber:** Multimode fiber allows many modes for the light rays traveling through it.

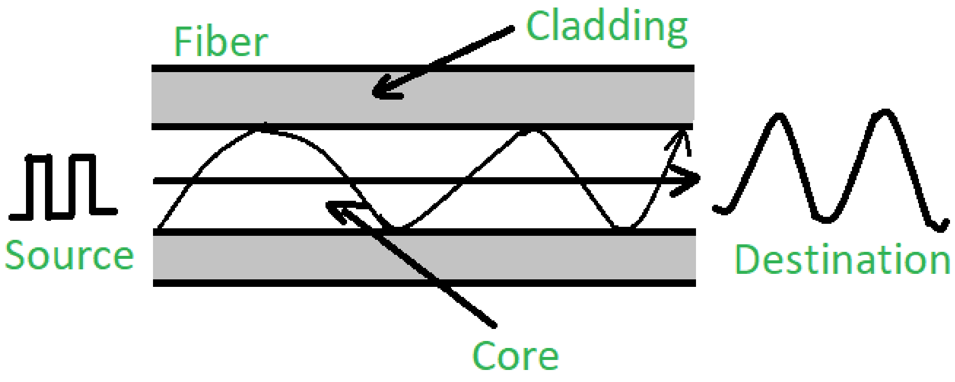
- The core diameter is generally (40um) and that of cladding is (70um). The relative refractive index difference is also greater than single-mode fiber.
- There is signal degradation due to multimode dispersion. It is not suitable for long-distance communication due to the large dispersion and attenuation of the signal.
- There are two categories based on Multi-mode fiber i.e. **Step Index Fiber** and **Graded Index Fiber**. These are categories under the types of optical fiber based on the Refractive Index

# Based on Refractive Index

- **Step-index optical fiber:** The refractive index of the core is constant. The refractive index of the cladding is also continuous. The rays of light propagate through it in the form of meridional rays which cross the fiber axis during every reflection at the core-cladding boundary.



- **Graded index optical fiber:** In this type of fiber, the core has a non-uniform refractive index that gradually decreases from the center towards the core-cladding interface. The cladding has a uniform refractive index. The light rays propagate through it in the form of skew rays or helical rays. it does not cross the fiber axis at any time.



# Uses of Fiber Optics

- Fiber Optics can be used in Computer Broadcasting and Networking
- Fiber Optics are used on the Internet. They are also used in Television Cable.
- Fiber Optics are widely used in Military Activities. They are also used in Medical Purposes like for precise illumination.
- They can also be used in Underwater environments as they don’t require to be replaced frequently.

# Advantages of Fiber Optics

- Fiber Optics supports bandwidth with higher capacities.
- Electromagnetic Interference is very little with Fiber Optics.
- Fiber Optics are stronger and lighter than copper cables.
- Very little Maintenance is required in Optical Fiber.

# Disadvantages of Fiber Optics

- Fiber Optics is more costly than Copper Wire.
- Huge manual work is required to install new cables.
- Some optical fibers like glass fiber require more protection.
- Fiber Optics are more fragile i.e., can be easily broken, or signals can be lost easily.

# Types of Computer Networks

- A computer network is a cluster of computers over a shared communication path that works to share resources from one computer to another, provided by or located on the network nodes.

# What is a Computer Network?

- A computer network is a system that connects many independent computers to share information (data) and resources.
- The integration of computers and other different devices allows users to communicate more easily.
- A computer network is a collection of two or more computer systems that are linked together. A network connection can be established using either cable or wireless media.
- Hardware and software are used to connect computers and tools in any network.

# Uses of Computer Networks

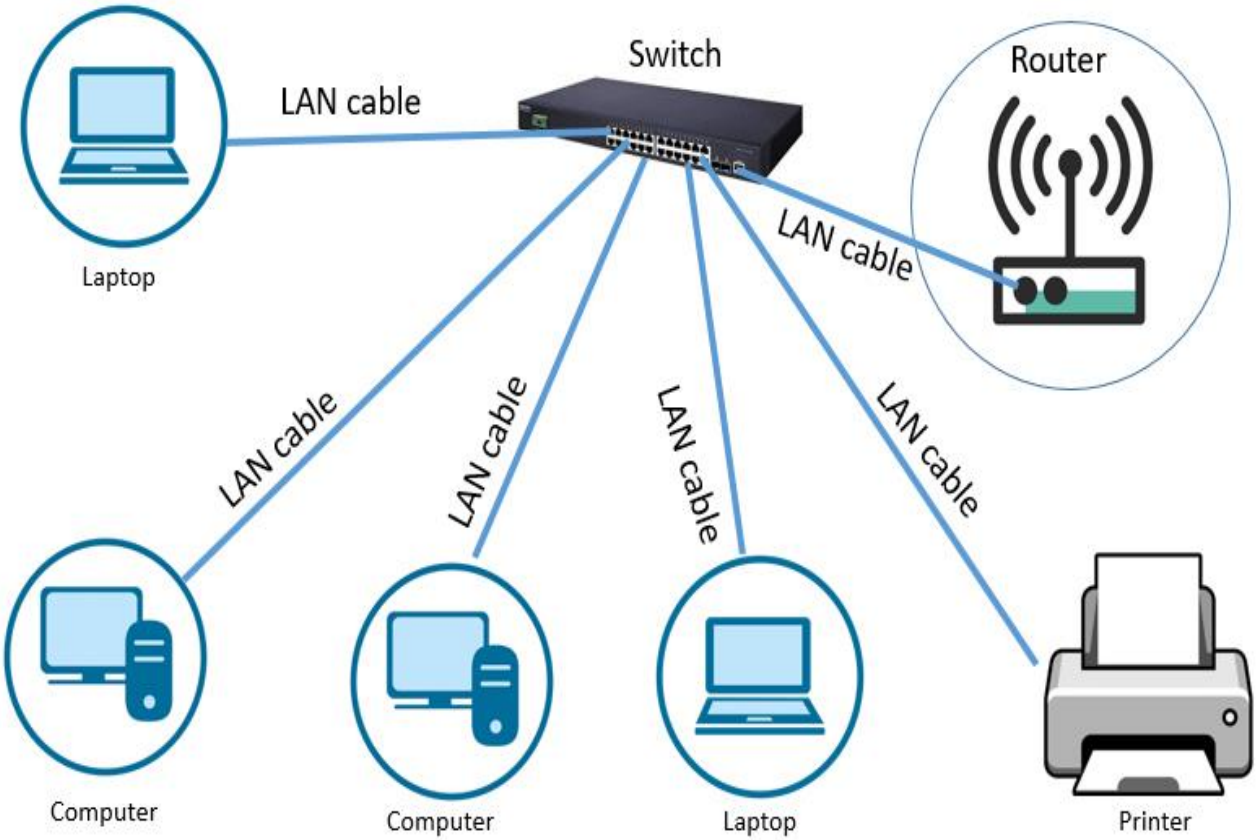
- Communicating using email, video, instant messaging, etc.
- Sharing devices such as printers, scanners, etc.
- Sharing files.
- Sharing software and operating programs on remote systems.
- Allowing network users to easily access and maintain information.

# Types of Computer Networks

- There are mainly five types of Computer Networks
- LAN
- WAN
- MAN

# Local Area Network (LAN)

- LAN is the most frequently used network. A LAN_is a computer network that connects computers through a common communication path, contained within a limited area, that is, locally.
- A LAN encompasses two or more computers connected over a server. The two important technologies involved in this network are Ethernet and Wi-Fi.
- It ranges up to 2km & transmission speed is very high with easy maintenance and low cost. Examples of LAN are networking in a home, school, library, laboratory, college, office, etc.
-



# Local Area Network

# Advantages of a LAN

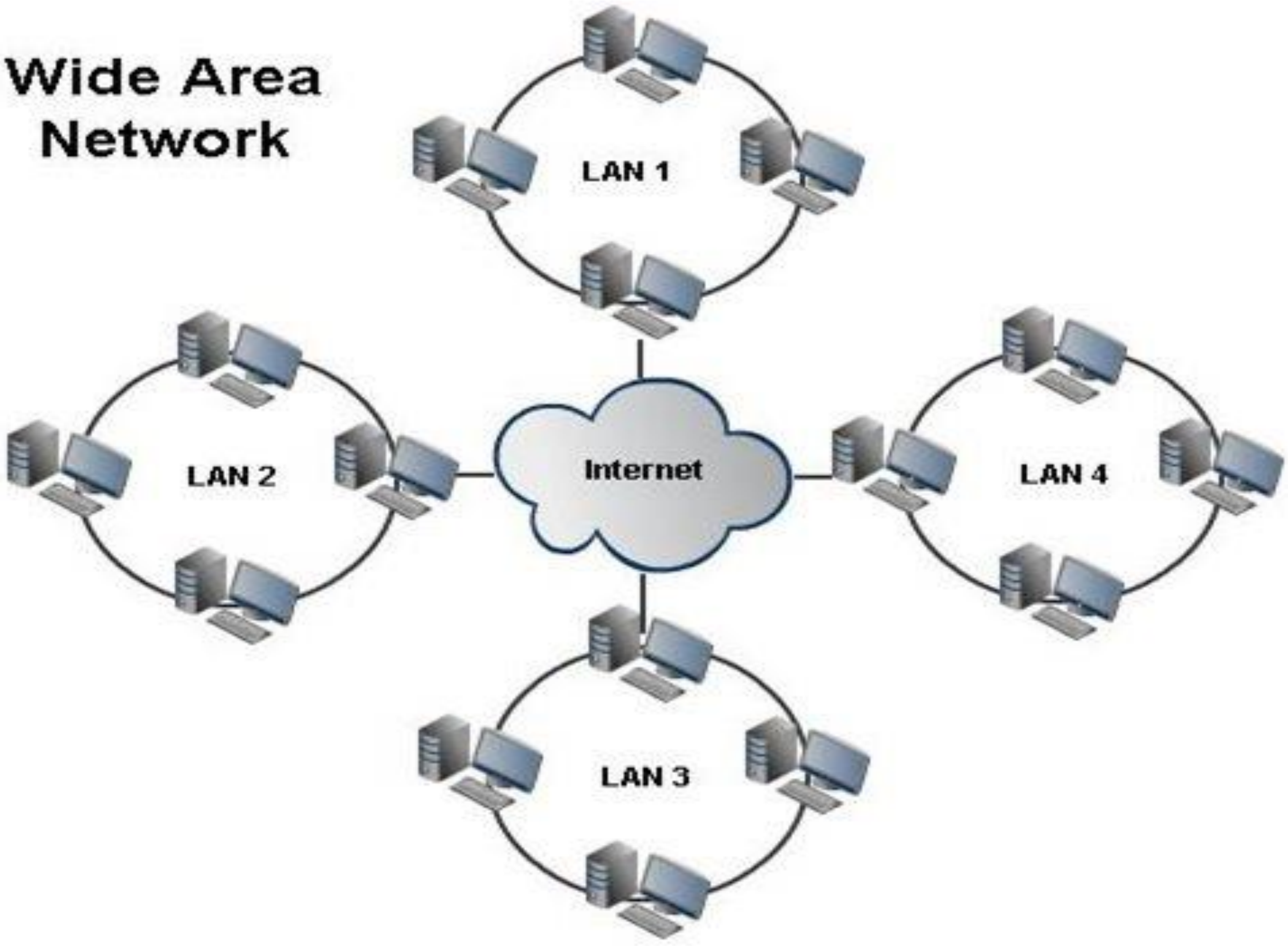
- **Privacy:** LAN is a private network, thus no outside regulatory body controls it, giving it a privacy.
- **High Speed:** LAN offers a much higher speed(around 100 mbps) and data transfer rate comparatively to WAN.
- **Supports different transmission mediums:** LAN support a variety of communications transmission medium such as an Ethernet cable (thin cable, thick cable, and twisted pair), fiber and wireless transmission.
- **Inexpensive and Simple:** A LAN usually has low cost, installation, expansion and maintenance and LAN installation is relatively easy to use, good scalability.

# Disadvantages of LAN

- The initial setup costs of installing Local Area Networks is high because there is special software required to make a server.
- Communication devices like an ethernet cable, switches, hubs, routers, cables are costly.
- LAN administrator can see and check personal data files as well as Internet history of each and every LAN user. Hence, the privacy of the users are violated
- LANs are restricted in size and cover only a limited area
- Since all the data is stored in a single server computer, if it can be accessed by an unauthorized user, can cause a serious data security threat.

# Wide Area Network (WAN)

- WAN is a type of computer network that connects computers over a large geographical distance through a shared communication path. It is not restrained to a single location but extends over many locations. WAN can also be defined as a group of local area networks that communicate with each other with a range above 50km. Here we use Leased-Line & Dial-up technology. Its transmission speed is very low and it comes with very high maintenance and very high cost. The most common example of WAN is the Internet.


Wide Area Network
LAN 1
LAN 2
Internet
LAN 4
LAN 3

# Advantages of WAN

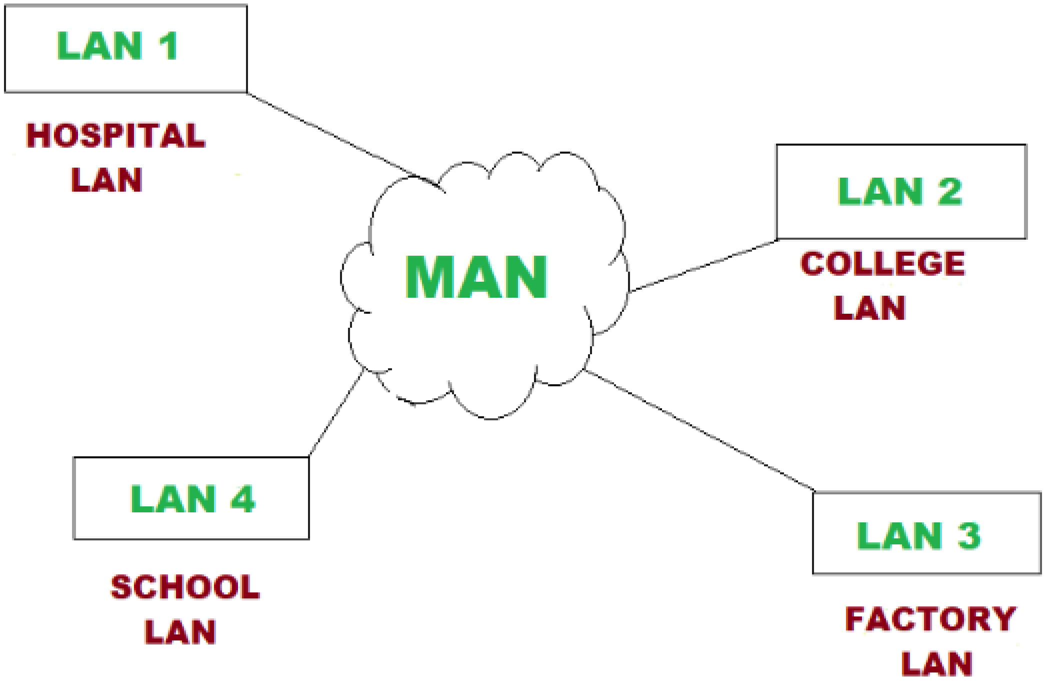
- It covers large geographical area which enhances the reach of organisation to transmit data quickly and cheaply.
- The data can be stored in centralised manner because of remote access to data provided by WAN.
- The travel charges that are needed to cover the geographical area of work can be minimised.
- WAN enables a user or organisation to connect with the world very easily and allows to exchange data and do business at global level.

# Disadvantages of WAN

- Traffic congestion in Wide Area Network is very high.
- The fault tolerance ability of WAN is very less.
- Noise and error are present in large amount due to multiple connection point.
- The data transfer rate is slow in comparison to LAN because of large distances and high number of connected system within the network.

# Metropolitan Area Network (MAN)

- A MAN is larger than a LAN but smaller than a WAN. This is the type of computer network that connects computers over a geographical distance through a shared communication path over a city, town or metropolitan area.
- This network mainly uses FDDI, CDDI, and ATM as the technology with a range from 5km to 50km. Its transmission speed is average.
- It is difficult to maintain and it comes with a high cost. Examples of MAN are networking in towns, cities, a single large city, a large area within multiple buildings, etc.


LAN 1
HOSPITAL LAN
MAN
LAN 2
COLLEGE LAN
LAN 4
SCHOOL LAN
LAN 3
FACTORY LAN

# Advantages of MAN

- MAN offers high-speed connectivity in which the speed ranges from 10-100 Mbps.
- The security level in MAN is high and strict as compared to WAN.
- It support to transmit data in both directions concurrently because of dual bus architecture.
- MAN can serve multiple users at a time with the same high-speed internet to all the users.
- MAN allows for centralized management and control of the network, making it easier to monitor and manage network resources and security.

# Disadvantages of MAN

- The architecture of MAN is quite complicated hence, it is hard to design and maintain.
- This network is highly expensive because it required the high cost to set up fiber optics.
- It provides less fault tolerance.
- The Data transfer rate in MAN is low when compare to LANs.

# Goals and applications of networks

- **Goals of Networks**
  - Computer Network means an interconnection of autonomous (standalone) computers for information exchange. The connecting media could be a copper wire, optical fiber, microwave, or satellite.
- **Networking Elements –** The computer network includes the following networking elements:
  - At least two computers
  - Transmission medium either wired or wireless
  - Protocols or rules that govern the communication
  - Network software such as Network Operating System

**Network Criteria:**

The criteria that have to be met by a computer network are:

**1. Performance –** It is measured in terms of transit time and response time.

- Transit time is the time for a message to travel from one device to another
- Response time is the elapsed time between an inquiry and a response.
- Performance is dependent on the following factors:
  - The number of users
  - Type of transmission medium
  - Capability of connected network
  - Efficiency of software
  - Bandwidth
  - Network topology
  - Network protocols
  - Distance
  - Network congestion
  - Network hardware

**2. Reliability – ** It is measured in terms of

- Frequency of failure
- Recovery from failures
- Robustness during catastrophe
- Quality of service (QoS)
- Reducing single points of failure
- Capacity planning
- Network architecture

**3. Security –** It means protecting data from unauthorized access.

**4. Network topology-** it is another crucial factor to consider when designing a computer network.

- It refers to the way in which computers, devices, and links are arranged in a network.
- Common topologies include bus, star, ring, mesh, and hybrid, each with its own advantages and disadvantages in terms of cost, scalability, reliability, and performance.
- The choice of topology depends on the specific needs and constraints of the network.
- Other important criteria that must be met by a computer network include performance, reliability, and security.

# Goals of Computer Networks:

- The following are some important goals of computer networks:
- **Resource Sharing –** Many organization has a substantial number of computers in operations, which are located apart. Ex. A group of office workers can share a common printer, fax, modem, scanner, etc.

- **High Reliability –** If there are alternate sources of supply, all files could be replicated on two or more machines. If one of them is not available, due to hardware failure, the other copies could be used.

- **Inter-process Communication –** Network users, located geographically apart, may converse in an interactive session through the network. In order to permit this, the network must provide almost error-free communications.

- **Flexible access –** Files can be accessed from any computer in the network. The project can be begun on one computer and finished on another.
- **Security**– Computer networks must be secure to protect against unauthorized access, data breaches, and other security threats. This includes implementing measures such as firewalls, antivirus software, and encryption to ensure the confidentiality, integrity, and availability of data.
- **Performance**– Computer networks must provide high performance and low latency to ensure that applications and services are responsive and available when needed. This requires optimizing network infrastructure, bandwidth utilization, and traffic management.

- **Scalability-** Computer networks must be designed to scale up or down as needed to accommodate changes in the number of users, devices, and data traffic. This requires careful planning and management to ensure the network can meet current and future needs.Other goals include Distribution of processing functions, Centralized management, and allocation of network resources, Compatibility of dissimilar equipment and software, Good network performance, Scalability, Saving money, Access to remote information, Person to person communication, etc.

# Advantages

- **Resource sharing:** Networks enable the sharing of resources such as printers, scanners, storage devices, and software applications, which can reduce costs and increase efficiency.
- **Communication and collaboration:** Networks provide a platform for communication and collaboration among users, allowing for easy sharing of information and ideas.
- **Centralized management:** Networks allow for centralized management of devices, users, and resources, making it easier to control and monitor the network.

# Advantages

- **Scalability:** Networks can be scaled up or down to accommodate changes in the number of users, devices, or data volume.
- **Accessibility:** Networks can provide remote access to resources, enabling users to work from anywhere and improving accessibility to information and resources.

# Disadvantages

- **Security vulnerabilities:** Networks can be vulnerable to security threats such as hacking, viruses, and malware, which can compromise sensitive data and disrupt network operations.
- **Complexity:** Networks can be complex to set up, configure, and maintain, requiring specialized knowledge and expertise.
- **Dependence on infrastructure:** Networks depend on the underlying infrastructure such as cables, routers, switches, and servers, which can be prone to failures or downtime, disrupting network operations.

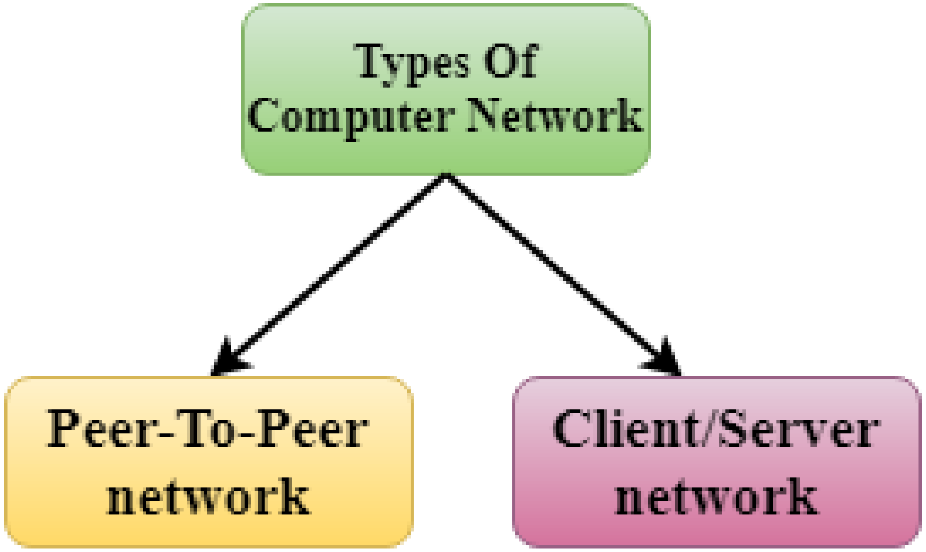
# Disadvantages

- **Cost:** Networks can be expensive to set up and maintain, requiring investments in hardware, software, and personnel.
- **Performance limitations:** Networks have performance limitations such as bandwidth constraints, latency, and congestion, which can affect the speed and reliability of network operations.

# Computer Network Architecture

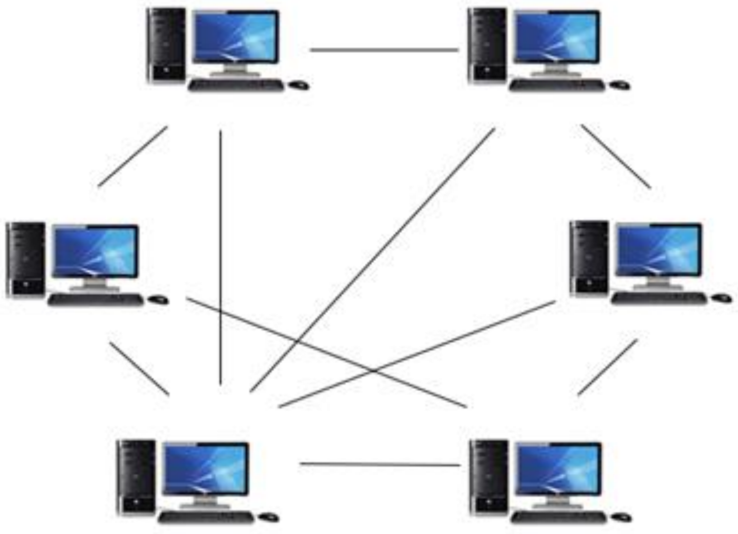
- Computer Network Architecture is defined as the physical and logical design of the software, hardware, protocols, and media of the transmission of data. Simply we can say that how computers are organized and how tasks are allocated to the computer.

- The two types of network architectures are used:
  - Peer-To-Peer network
  - 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:**

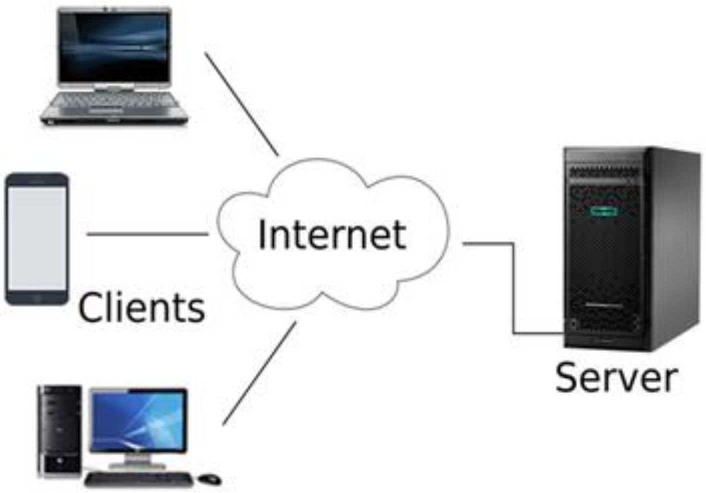
- It is less costly as it does not contain any dedicated server.
- If one computer stops working but, other computers will not stop working.
- It is easy to set up and maintain as each computer manages itself.

**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.

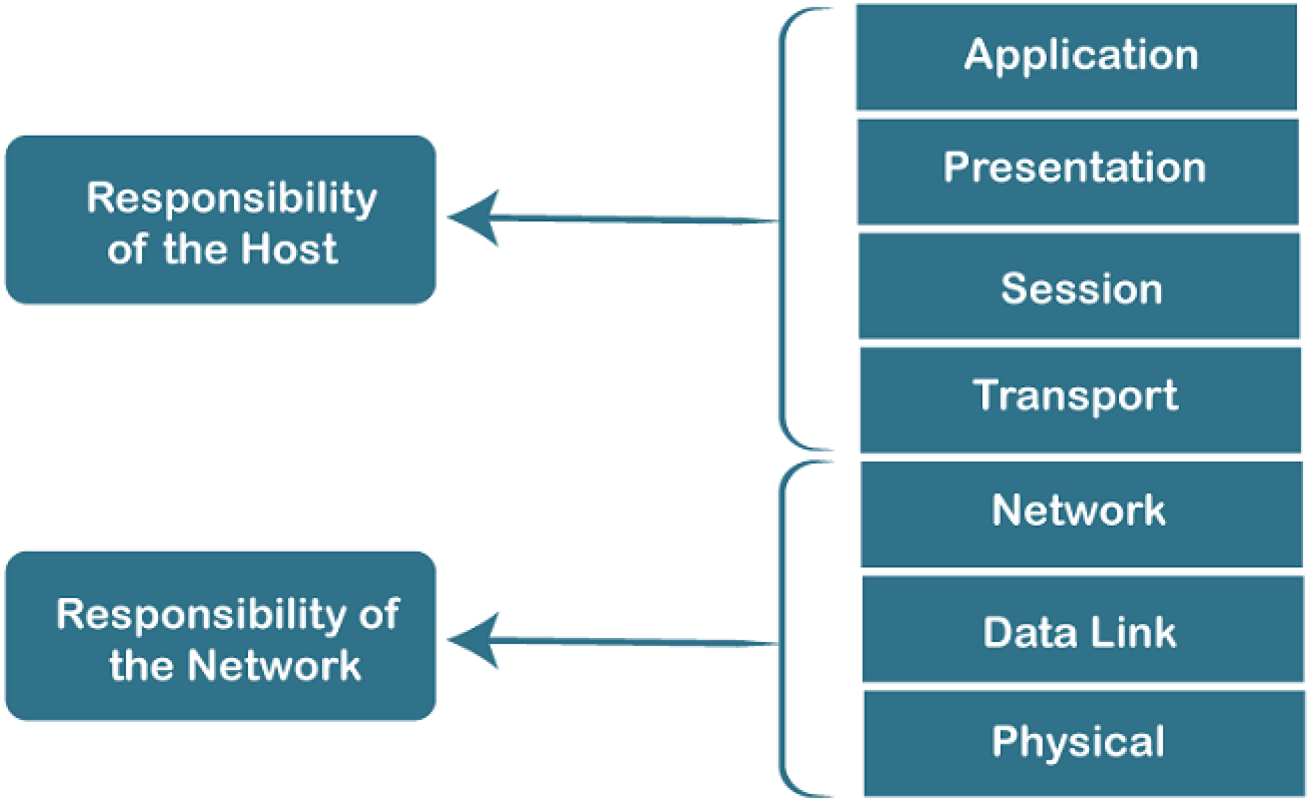
**Disadvantages Of Client/Server network:**

- 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



Responsibility of the Host

Responsibility of the Network

Application

Presentation

Session

Transport

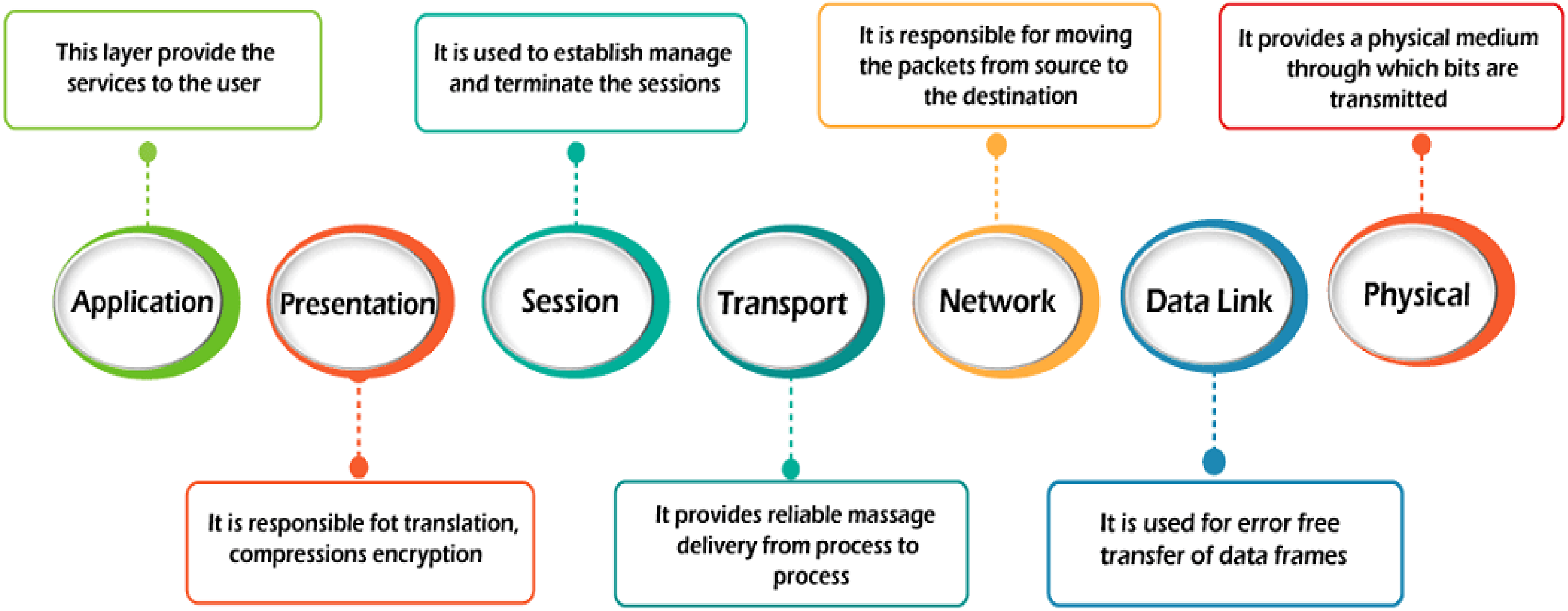
Network

Data Link

Physical

# 7 Layers of OSI Model

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



This layer provide the services to the user
It is used to establish manage and terminate the sessions
It is responsible for moving the packets from source to the destination
It provides a physical medium through which bits are transmitted
Application
Presentation
Session
Transport
Network
Data Link
Physical
It is responsible fot translation, compressions encryption
It provides reliable massage delivery from process to process
It is used for error free transfer of data frames

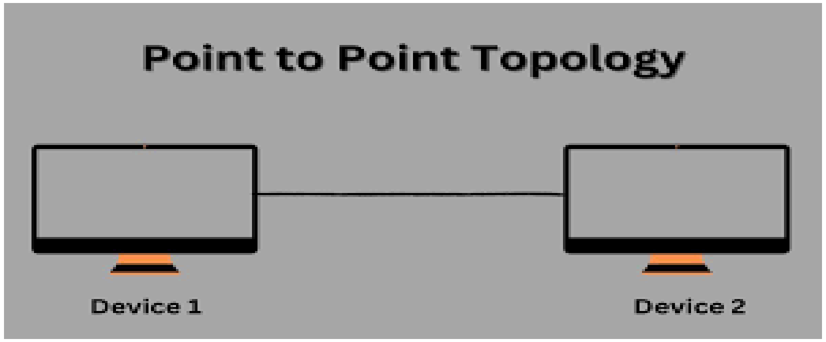
# Types of Network Topology

- Network topology refers to the arrangement of different elements like nodes, links, and devices in a computer network. It defines how these components are connected and interact with each other. Understanding various types of network topologies helps in designing efficient and robust networks. Common types include bus, star, ring, mesh, and tree topologies, each with its own advantages and disadvantages.

# Types of Network Topology

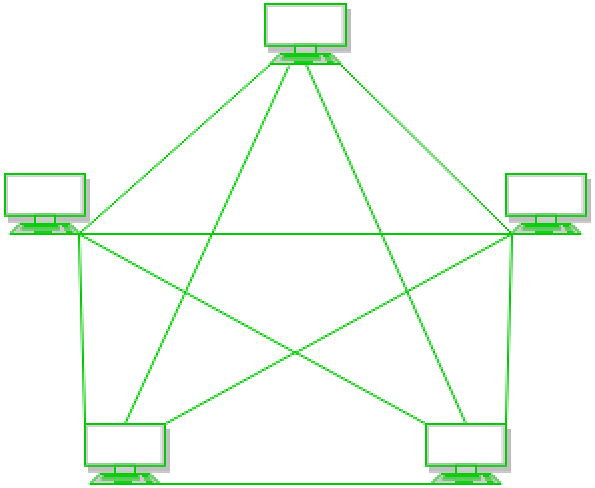
- The arrangement of a network that comprises nodes and connecting lines via sender and receiver is referred to as **Network Topology**. The various network topologies are:
- Point to Point Topology
- Mesh Topology
- Star Topology
- Bus Topology
- Ring Topology

# Point to Point Topology

- Point-to-point topology is a type of topology that works on the functionality of the sender and receiver. It is the simplest communication between two nodes, in which one is the sender and the other one is the receiver. Point-to-Point provides high bandwidth.
- 

# Mesh Topology

- In a mesh topology, every device is connected to another device via a particular channel. In Mesh Topology, the protocols used are AHCP (Ad Hoc Configuration Protocols), DHCP (Dynamic Host Configuration Protocol), etc.



**Advantages of Mesh Topology**

- Communication is very fast between the nodes.
- Mesh Topology is robust.
- The fault is diagnosed easily. Data is reliable because data is transferred among the devices through dedicated channels or links.
- Provides security and privacy.

**Disadvantages of Mesh Topology**

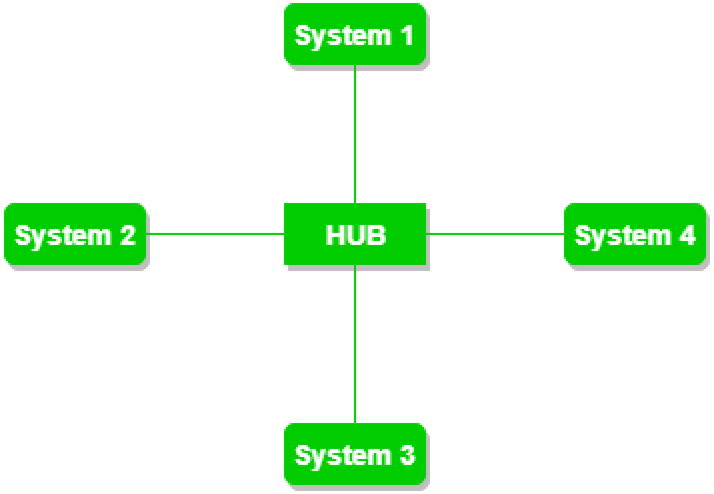
- Installation and configuration are difficult.
- The cost of cables is high as bulk wiring is required, hence suitable for less number of devices.
- The cost of maintenance is high.

- A common example of mesh topology is the internet backbone, where various internet service providers are connected to each other via dedicated channels.
- This topology is also used in military communication systems and aircraft navigation systems.

# Star Topology

- In Star Topology, all the devices are connected to a single hub through a cable.
- This hub is the central node and all other nodes are connected to the central node.
- The hub can be passive in nature i.e., not an intelligent hub such as broadcasting devices, at the same time the hub can be intelligent known as an active hub.
- Active hubs have repeaters in them. Coaxial cables or RJ-45 cables are used to connect the computers.

- In Star Topology, many popular Ethernet LAN protocols are used as CD(Collision Detection), CSMA (Carrier Sense Multiple Access), etc.



**Advantages of Star Topology**

- If N devices are connected to each other in a star topology, then the number of cables required to connect them is N. So, it is easy to set up.
- Each device requires only 1 port i.e. to connect to the hub, therefore the total number of ports required is N.
- It is Robust. If one link fails only that link will affect and not other than that.
- Easy to fault identification and fault isolation.
- Star topology is cost-effective as it uses inexpensive coaxial cable.

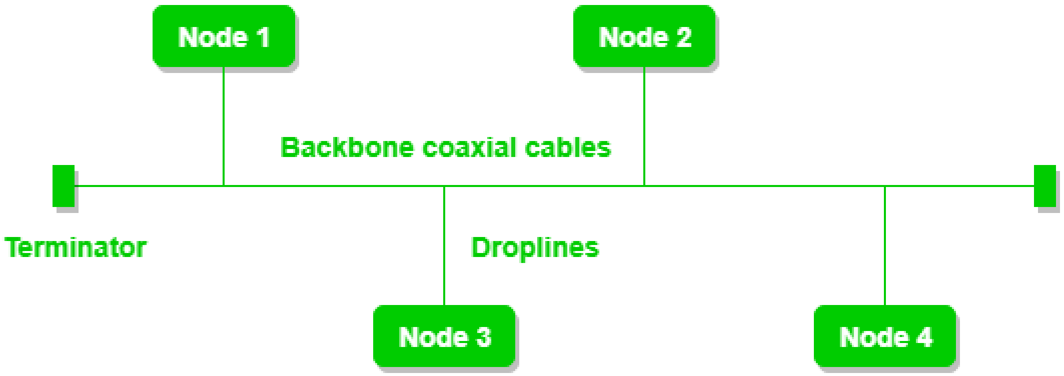
**Disadvantages of Star Topology**

- If the concentrator (hub) on which the whole topology relies fails, the whole system will crash down.
- The cost of installation is high.
- Performance is based on the single concentrator i.e. hub.

- A common example of star topology is a local area network (LAN) in an office where all computers are connected to a central hub. This topology is also used in wireless networks where all devices are connected to a wireless access point.

# Bus Topology

- Bus Topology is a network type in which every computer and network device is connected to a single cable.
- It is bi-directional.
- It is a multi-point connection and a non-robust topology because if the backbone fails the topology crashes.
- In Bus Topology, various MAC (Media Access Control) protocols are followed by LAN ethernet connections like TDMA, Pure Aloha, CDMA, Slotted Aloha, etc.


Node 1
Node 2
Backbone coaxial cables
Terminator
Droplines
Node 3
Node 4

- **Advantages of Bus Topology**
- If N devices are connected to each other in a bus topology, then the number of cables required to connect them is 1, known as backbone cable, and N drop lines are required.
- Coaxial or twisted pair cables are mainly used in bus-based networks that support up to 10 Mbps.
- The cost of the cable is less compared to other topologies, but it is used to build small networks.
- Bus topology is familiar technology as installation and troubleshooting techniques are well known.
- CSMA is the most common method for this type of topology.

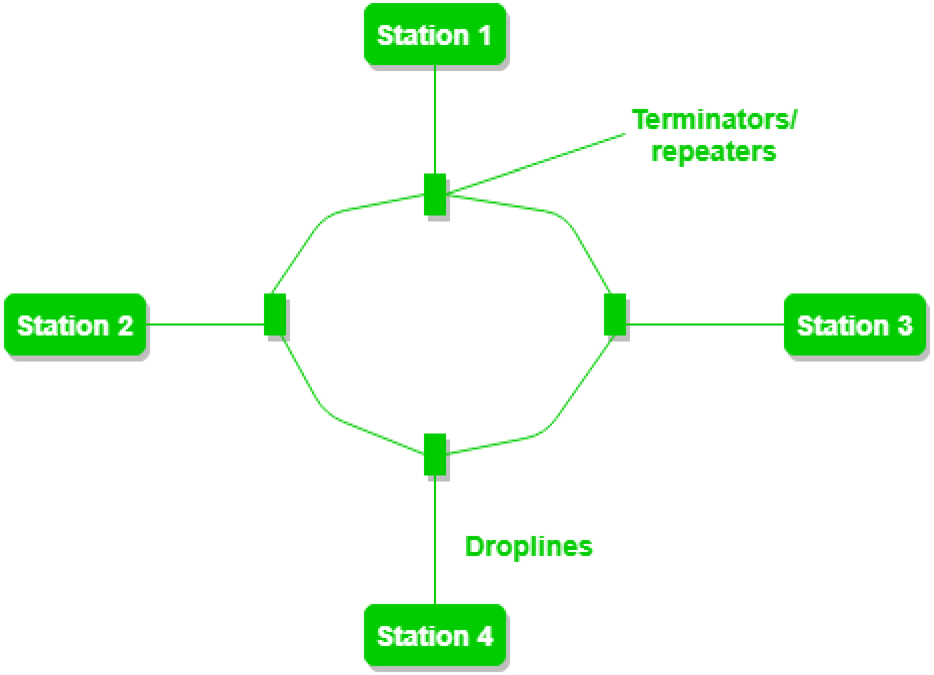
**Disadvantages of  Bus Topology**

- A bus topology is quite simpler, but still, it requires a lot of cabling.
- If the common cable fails, then the whole system will crash down.
- If the network traffic is heavy, it increases collisions in the network. To avoid this, various protocols are used in the MAC layer known as Pure Aloha, Slotted Aloha, CSMA/CD, etc.
- Adding new devices to the network would slow down networks.
- Security is very low.

- A common example of bus topology is the Ethernet LAN, where all devices are connected to a single coaxial cable or twisted pair cable. This topology is also used in cable television networks.

# Ring Topology

- In a Ring Topology, it forms a ring connecting devices with exactly two neighboring devices. A number of repeaters are used for Ring topology with a large number of nodes, because if someone wants to send some data to the last node in the ring topology with 100 nodes, then the data will have to pass through 99 nodes to reach the 100th node. Hence to prevent data loss repeaters are used in the network.
- The data flows in one direction, i.e. it is unidirectional, but it can be made bidirectional by having 2 connections between each Network Node, it is called Dual Ring Topology. In-Ring Topology, the Token Ring Passing protocol is used by the workstations to transmit the data.



- The most common access method of ring topology is token passing.
- **Token passing:** It is a network access method in which a token is passed from one node to another node.
- **Token:** It is a frame that circulates around the network.

**Advantages of Ring Topology**

- The data transmission is high-speed.
- The possibility of collision is minimum in this type of topology.
- Cheap to install and expand.
- It is less costly than a star topology.

**Disadvantages of Ring Topology**

- The failure of a single node in the network can cause the entire network to fail.
- Troubleshooting is difficult in this topology.
- The addition of stations in between or the removal of stations can disturb the whole topology.
- Less secure.

# Switching techniques

- **Switching** is the process of transferring data packets from one device to another in a network, or from one network to another, using specific devices called **switches**.
- Switching takes place at the Data Link layer of the OSI Model. This means that after the generation of data packets in the Physical Layer, switching is the immediate next process in data communication.

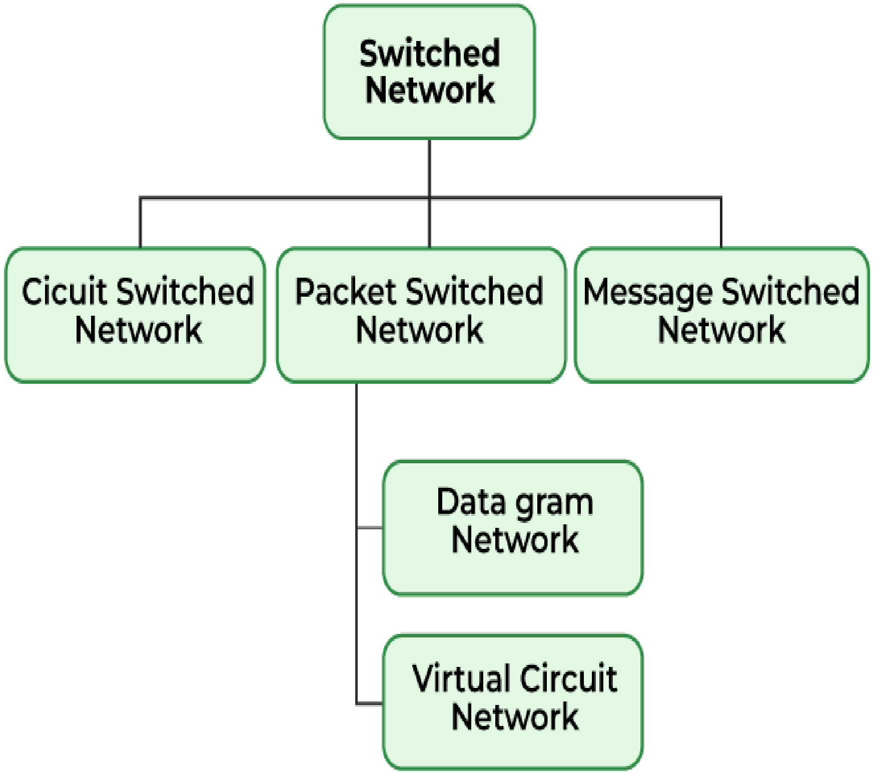
# Switch

- A switch is a hardware device in a network that connects other devices, like computers and servers. It helps multiple devices share a network without their data interfering with each other.

# Types of Switching

There are three types of switching methods:

- Message Switching
- Circuit Switching
- Packet Switching
  - Datagram Packet Switching
  - Virtual Circuit Packet Switching



- **Message Switching:** This is an older switching technique that has become obsolete. In message switching technique, the entire data block/message is forwarded across the entire network thus, making it highly inefficient.
- **Circuit Switching:** In this type of switching, a connection is established between the source and destination beforehand. This connection receives the complete bandwidth of the network until the data is transferred completely.

  This approach is better than message switching as it does not involve sending data to the entire network, instead of its destination only.

- **Packet Switching:** This technique requires the data to be broken down into smaller components, data frames, or packets. These data frames are then transferred to their destinations according to the available resources in the network at a particular time.
  This switching type is used in modern computers and even the Internet. Here, each data frame contains additional information about the destination and other information required for proper transfer through network components.

- **Datagram Packet Switching:** In Datagram Packet switching, each data frame is taken as an individual entity and thus, they are processed separately. Here, no connection is established before data transmission occurs. Although this approach provides flexibility in data transfer, it may cause a loss of data frames or late delivery of the data frames.

- **Virtual-Circuit Packet Switching:** In Virtual-Circuit Packet switching, a logical connection between the source and destination is made before transmitting any data. These logical connections are called virtual circuits. Each data frame follows these logical paths and provides a reliable way of transmitting data with less chance of data loss.