

# Unit 1

## **Introduction to Computer Networks**

Modern world scenario is ever changing. Data Communication and network have changed the way business and other daily affair works. Now, they highly rely on computer networks and internetwork.

A set of devices often mentioned as nodes connected by media link is called a Network.

A node can be a device which is capable of sending or receiving data generated by other nodes on the network like a computer, printer etc. These links connecting the devices are called **Communication channels**.

Computer network is a telecommunication channel using which we can share data with other computers or devices, connected to the same network. It is also called Data Network. The best example of computer network is Internet.

Computer network does not mean a system with one Control Unit connected to multiple other systems as its slave. That is Distributed system, not Computer Network.

A network must be able to meet certain criterias, these are mentioned below:

- **Performance**
- **Reliability**
- **Scalability**

## **Computer Networks: Performance**

It can be measured in the following ways:

- **Transit time** : It is the time taken to travel a message from one device to another.
- **Response time** : It is defined as the time elapsed between enquiry and response.

Other ways to measure performance are :

- Efficiency of software
- Number of users
- Capability of connected hardware

## **Computer Networks: Reliability**

It decides the frequency at which network failure take place. More the failures are, less is the network's reliability.

## **Computer Networks: Security**

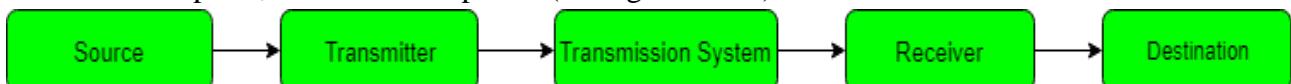
It refers to the protection of data from any unauthorised user or access. While travelling through network, data passes many layers of network, and data can be traced if attempted. Hence security is also a very important characteristic for Networks.

## **Properties of a Good Network**

- **Interpersonal Communication:** We can communicate with each other efficiently and easily. Example: emails, chat rooms, video conferencing etc, all of these are possible because of computer networks.
- **Resources can be shared:** We can share physical resources by making them available on a network such as printers, scanners etc.
- Authorised users are allowed to share the files on the network.

### **Basic Communication Model**

A Communication model is used to exchange data between two parties. For example: communication between a computer, server and telephone (through modem).



#### **Communication Model: Source**

Data to be transmitted is generated by this device, example: telephones, personal computers etc.

#### **Communication Model: Transmitter**

The data generated by the source system is not directly transmitted in the form its generated. The transmitter transforms and encodes the data in such a form to produce electromagnetic waves or signals.

#### **Communication Model: Transmission System**

A transmission system can be a single transmission line or a complex network connecting source and destination.

#### **Communication Model: Receiver**

Receiver accepts the signal from the transmission system and converts it into a form which is easily managed by the destination device.

#### **Communication Model: Destination**

Destination receives the incoming data from the receiver.

### **Data Communication**

The exchange of data between two devices through a transmission medium is called **Data Communication**. The data is exchanged in the form of **0's** and **1's**. The transmission medium used is wire cable. For data communication to occur, the communication device must be a part of a communication system. Data Communication has two types - **Local** and **Remote** which are discussed below:

#### **Data Communication: Local**

Local communication takes place when the communicating devices are in the same geographical area, same building, or face-to-face etc.

#### **Data Communication: Remote**

Remote communication takes place over a distance i.e. the devices are farther. The effectiveness of a data communication can be measured through the following features

1. **Delivery:** Delivery should be done to the correct destination.
2. **Timeliness:** Delivery should be on time.
3. **Accuracy:** Data delivered should be accurate.

## **Components of Data Communication**

1. **Message:** It is the information to be delivered.
2. **Sender:** Sender is the person who is sending the message.
3. **Receiver:** Receiver is the person to whom the message is being sent to.
4. **Medium:** It is the medium through which the message is sent. For example: A Modem.
5. **Protocol:** These are some set of rules which govern data communication.

## **Uses of Computer networks**

Computer networks have become invaluable to organizations as well as individuals. Some of its main uses are as follows –

- **Information and Resource Sharing** – Computer networks allow organizations having units which are placed apart from each other, to share information in a very effective manner. Programs and software in any computer can be accessed by other computers linked to the network. It also allows sharing of hardware equipment, like printers and scanners among varied users.
- **Retrieving Remote Information** – Through computer networks, users can retrieve remote information on a variety of topics. The information is stored in remote databases to which the user gains access through information systems like the World Wide Web.
- **Speedy Interpersonal Communication** – Computer networks have increased the speed and volume of communication like never before. Electronic Mail (email) is extensively used for sending texts, documents, images, and videos across the globe. Online communications have increased by manifold times through social networking services.
- **E-Commerce** – Computer networks have paved way for a variety of business and commercial transactions online, popularly called e-commerce. Users and organizations can pool funds, buy or sell items, pay bills, manage bank accounts, pay taxes, transfer funds and handle investments electronically.
- **Highly Reliable Systems** – Computer networks allow systems to be distributed in nature, by the virtue of which data is stored in multiple sources. This makes the system highly reliable. If a failure occurs in one source, then the system will still continue to function and data will still be available from the other sources.
- **Cost-Effective Systems** – Computer networks have reduced the cost of establishment of computer systems in organizations. Previously, it was imperative for organizations to set up expensive mainframes for computation and storage. With the advent of networks, it is sufficient to set up interconnected personal computers (PCs) for the same purpose.
- **VoIP** – VoIP or Voice over Internet protocol has revolutionized telecommunication systems. Through this, telephone calls are made digitally using Internet Protocols instead of the regular analog phone lines.

## **Line Configuration in Computer Networks**

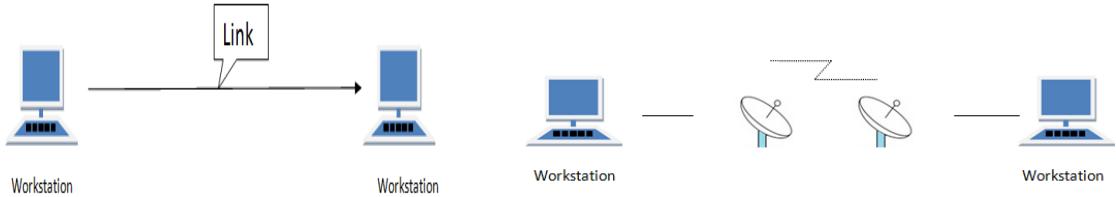
A Network is nothing but a connection made through connection links between two or more devices. Devices can be a computer, printer or any other device that is capable to send and receive data. There are two ways to connect the devices :

1. Point-to-Point connection
2. Multipoint connection

### **Point-To-Point Connection**

It is a protocol which is used as a communication link between two devices. It is simple to establish. The most common example for Point-to-Point connection (PPP) is a computer connected by telephone line. We can connect the two devices by means of a pair of wires or using a microwave or satellite link.

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

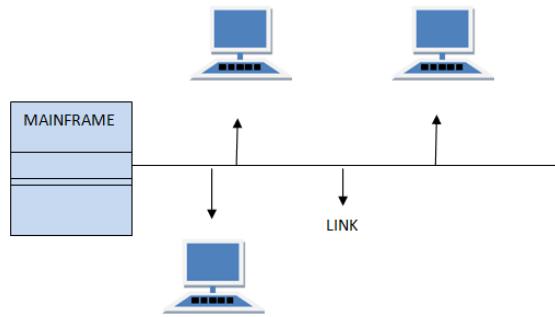


### **MultiPoint Connection**

It is also called Multidrop configuration. In this connection two or more devices share a single link.

There are two kinds of Multipoint Connections :

- If the links are used simultaneously between many devices, then it is spatially shared line configuration.
- If user takes turns while using the link, then it is time shared (temporal) line configuration.



### **Network topology:**

Network topology is the layout of a network. It consists of two parts; physical and logical. The physical part describes the physical layout of a network while the logical part describes how the data flows in that network. Both, physical and logical parts are also known as the physical topology and the logical topology.

$$\text{Physical part (topology)} + \text{Logical part (topology)} = \text{Network topology}$$

### **History of Computer Networking:**

A computer network is a group of computers that has the potential to transmit, receive and exchange voice, data, and video traffic. A network connection can be set up with the help of

either cable or wireless media. In modern times, computer networks are very important as information technology is increasing rapidly all over the world. The network and data communication are the essential factors to rise information technology in the world as technology's advancement is on the system, including the gadgets. ARPANET began the networking long ago.

In 1957, when SPUTNIK Satellite was launched by Russia. An agency named ADVANCED RESEARCH PROJECT AGENCY (ARPA) was started by American, and its first satellite was launched within 18 months after establishment. Then they used ARPANET to share the information on another computer. America's Dr. LIED LIEDER has this all responsibility. Then, ARPANET came to India in 1969, and its name changed from Indian to NETWORK.

For the United States Department of Defense, the funding of the design of the Advanced Research Projects Agency Network (ARPANET) was began by ARPA. In 1969, the network began to develop on the basis of the developed designs in the 1960s. The below table contains a complete history of computer networking:

Year	Event
1961	In this year, Leonard Kleinrock proposed the earliest computer networks, which was the idea of ARPANET.
1965	In 1965, Donald Davies coined the term "packet" to describe how to send data between computers on a network.
1969	Although In 1966, the development of ARPANET began, officially started ARPANET in 1969. It was considered one of the first computer networks in which first two nodes, UCLA and SRI (Stanford Research Institute) were connected, and to use packet switching. To provide and define information about network protocols, procedures, and computer communications, the first RFC surfaced as a document in April 1969.
1969	On 29 August 1969, the first IMP and network switch were sent to UCLA. On ARPANET, the first data transmission was sent by using it.
1970	NCP, stands for NetWare Core Protocol, released by Steve Crocker and a team at UCLA for use with NetWare.
1971	In 1971, the first e-mail was sent to across a network to other users by Ray Tomlinson.

<b>1973</b>	While working at Xerox PARC, Robert Metcalfe developed the Ethernet in 1973. In the same year, ARPA deployed the first international network connection, known as SATNET. In 1973, VoIP technology and capabilities were officially introduced, which made a VoIP call. However, until 1995, the software was not available for users that could make VoIP calls.
<b>1974</b>	In this year, the use of first router was began, but they were not considered true IP routers.
<b>1976</b>	Originally called a gateway, Ginny Strazisar develop the first true IP router.
<b>1978</b>	In 1978, the TCP/IP protocol was developed and invented by Bob Kahn for networks; it was developed with help from Vint Cerf.
<b>1981</b>	In the United States, between IBM mainframe systems, BITNET was created in 1981 as a network. The U.S. National Science Foundation developed the CSNET (Computer Science Network) in the same year 1981.
<b>1983</b>	For using TCP/IP, ARPANET finished the transition. The first DNS implement by Jon Postel and Paul Mockapetris in 1983.
<b>1986</b>	This is the year in which a backbone for ARPANET, the National Science Foundation Network was came online, which finally took the place of ARPANET in 1990s. In the same year, with the original BITNET, BITNET II was introduced to deal with bandwidth issues.
<b>1988</b>	In 1988, the first T1 backbone was included with ARPANET. AT&T, Lucent, and NCR introduced the WaveLAN network technology in 1988. In 1988, for the first time, the explanation of network firewall technology was published. In the same year, Digital Equipment Corporation developed it. This paper had the detail about the first firewall, known as a packet filter firewall.
<b>1990</b>	The first network switch was developed and introduced by a U.S. network hardware company named Kalpana in 1990.
<b>1996</b>	In 1996, an IPv6 was introduced as an improvement over IPv4, as well as embedded encryption, improved routing.
<b>1997</b>	In June 1997, the 802.11 standards, containing transmission speeds up to 2 Mbps, for Wi-Fi were introduced.

<b>1999</b>	The 802.11a standard, containing transmission speeds up to 25 Mbps to use the 5 GHz band, was officially made in 1999. Another standard 802.11b was available to use for the public in mid-1999, which offered transmission speeds up to 11 Mbps. In September 1999, for use with 802.11b, the WEP encryption protocol was released.
<b>2003</b>	802.11g devices, contained transmission speeds up to 20 Mbps, were available to the public in January 2003. In the same year, for use with 802.11g, the WPA encryption protocol is released.
<b>2004</b>	In 2004, as a replacement for WPA, the WPA2 encryption protocol was introduced. By 2006, WPA2 certification was compulsory for all Wi-Fi devices.
<b>2009</b>	The 802.11n standard can operate on the 2.4 GHz and 5 GHz bandwidths and offers higher transfer speeds over 802.11a and 802.11g. Officially, it was made in 2009.
<b>2018</b>	In January 2018, WPA3 encryption was released by the Wi-Fi Alliance, which comprises security enhancements over WPA2.

## PROTOCOLS AND STANDARDS

### Protocols:

In computer networks, communication occurs between entities in different systems. An entity is anything capable of sending or receiving information. However, two entities cannot simply send bit streams to each other and expect to be understood. For communication to occur, the entities must agree on a protocol. A protocol is a set of rules that govern data communications. A protocol defines what is communicated, how it is communicated, and when it is communicated. The key elements of a protocol are syntax, semantics, and timing.

□ Syntax. The term *syntax* refers to the structure or format of the data, meaning the order in which they are presented. For example, a simple protocol might expect the first 8 bits of data to be the address of the sender, the second 8 bits to be the address of the receiver, and the rest of the stream to be the message itself.

□ Semantics. The word *semantics* refers to the meaning of each section of bits. How is a particular pattern to be interpreted, and what action is to be taken based on that interpretation? For example, does an address identify the route to be taken or the final destination of the message?

□ Timing. The term *timing* refers to two characteristics: when data should be sent and how fast they can be sent. For example, if a sender produces data at 100 Mbps but the receiver can process data at only 1 Mbps, the transmission will overload the receiver and some data will be lost.

## **Standards**

Standards are essential in creating and maintaining an open and competitive market for equipment manufacturers and in guaranteeing national and international interoperability of data and telecommunications technology and processes. Standards provide guidelines to manufacturers, vendors, government agencies, and other service providers to ensure the kind of interconnectivity necessary in today's marketplace and in international communications.

Data communication standards fall into two categories: de facto (meaning "by fact" or "by convention") and de jure (meaning "by law" or "by regulation").

- De facto. Standards that have not been approved by an organized body but have been adopted as standards through widespread use are de facto standards. De facto standards are often established originally by manufacturers who seek to define the functionality of a new product or technology.
- De jure. Those standards that have been legislated by an officially recognized body are de jure standards.

## **LAYERED TASKS**

We use the concept of layers in our daily life. As an example, let us consider two friends who communicate through postal mail the process of sending a letter to a friend would be complex if there were no services available from the post office. Below Figure shows the steps in this task.

Sender, Receiver, and Carrier

In Figure we have a sender, a receiver, and a carrier that transports the letter. There is a hierarchy of tasks.

### *At the Sender Site*

Let us first describe, in order, the activities that take place at the sender site.

- Higher layer. The sender writes the letter, inserts the letter in an envelope, writes the sender and receiver addresses, and drops the letter in a mailbox.
- Middle layer. The letter is picked up by a letter carrier and delivered to the post office.
- Lower layer. The letter is sorted at the post office; a carrier transports the letter.

*On the Way:* The letter is then on its way to the recipient. On the way to the recipient's local post office, the letter may actually go through a central office. In addition, it may be transported by truck, train, airplane, boat, or a combination of these.

### *At the Receiver Site*

- Lower layer. The carrier transports the letter to the post office.
- Middle layer. The letter is sorted and delivered to the recipient's mailbox.
- Higher layer. The receiver picks up the letter, opens the envelope, and reads it.

## **Reference Models:**

In computer networks, reference models give a conceptual framework that standardizes communication between heterogeneous networks.

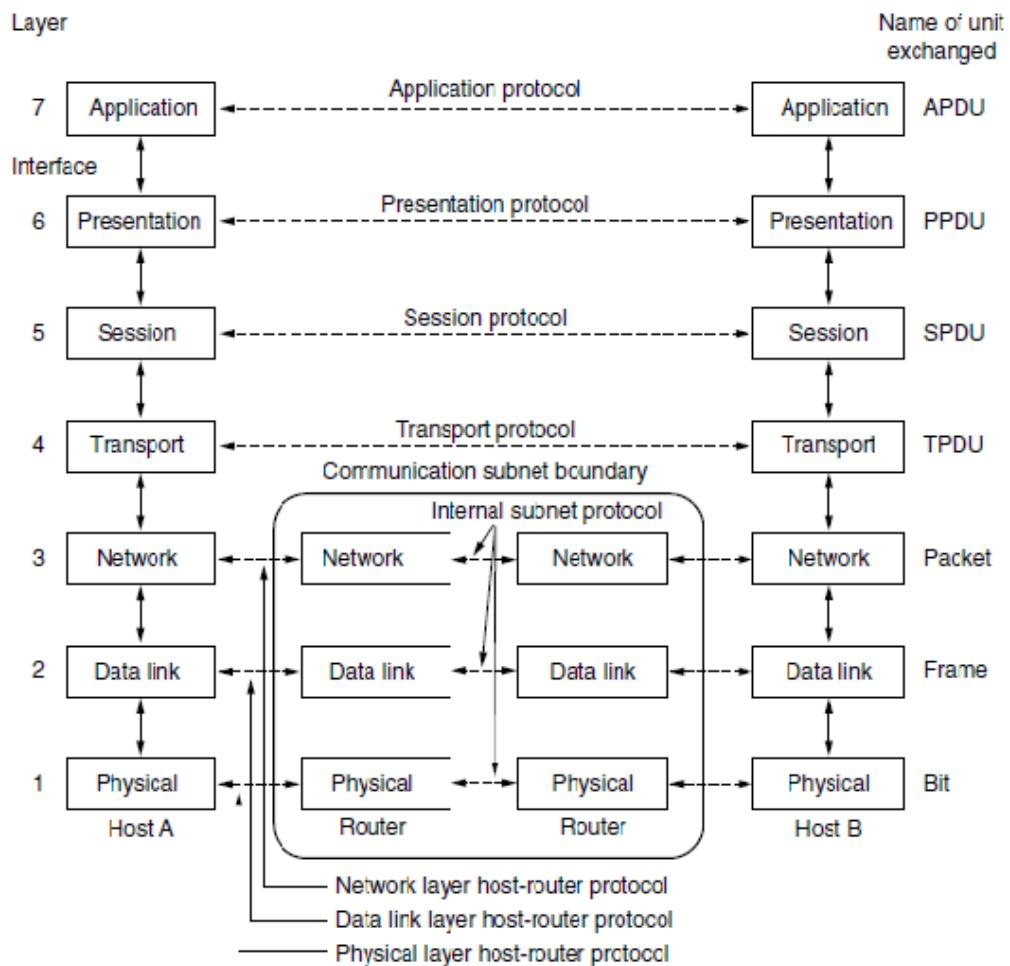
The two popular reference models are –

- OSI Model
- TCP/IP Protocol Suite

## 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:



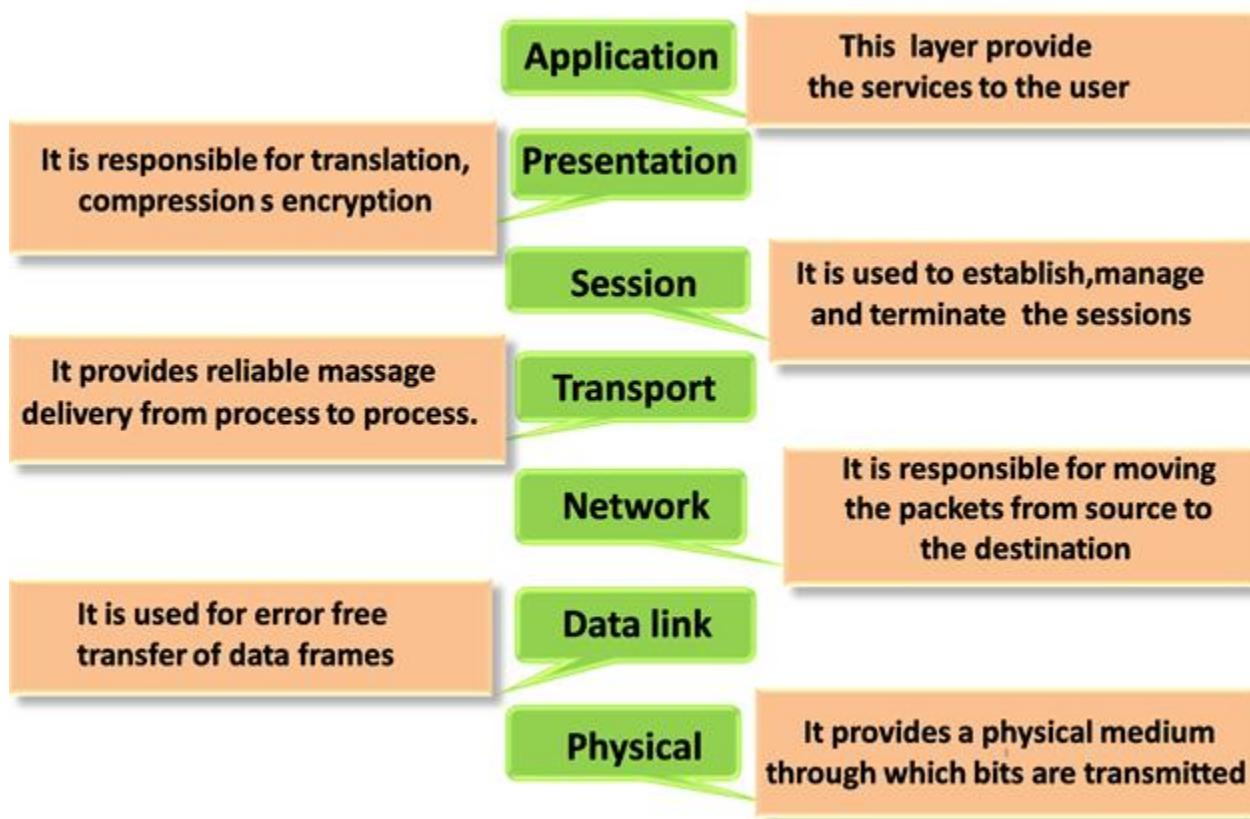
- The OSI model is divided into two layers: upper layers and lower layers.

- 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.

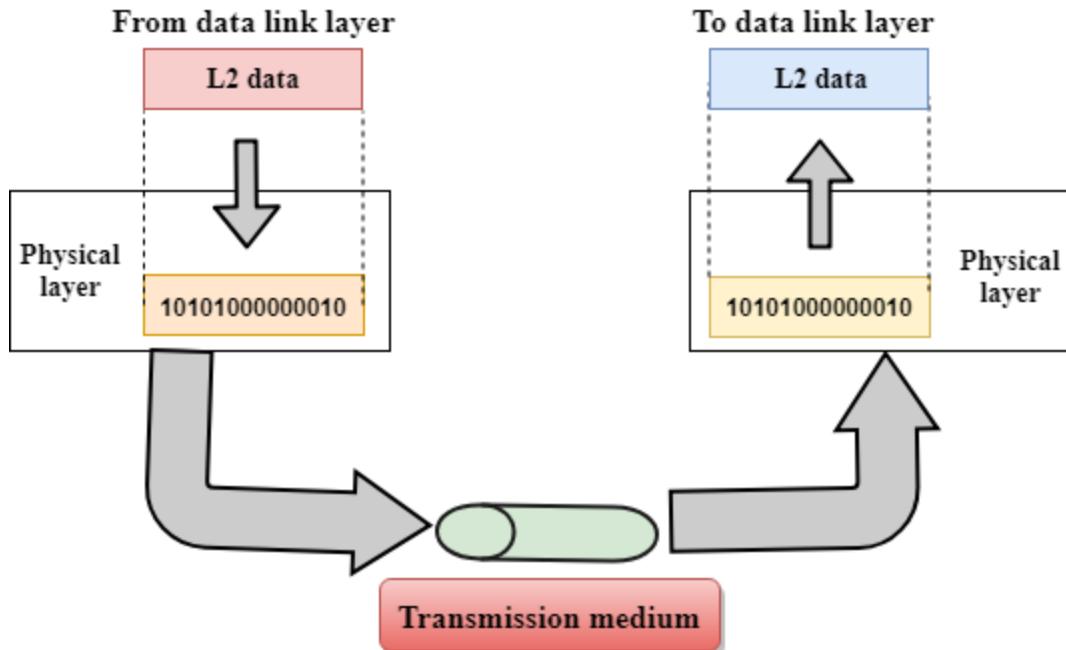
### Functions of the OSI Layers

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

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



### Physical layer

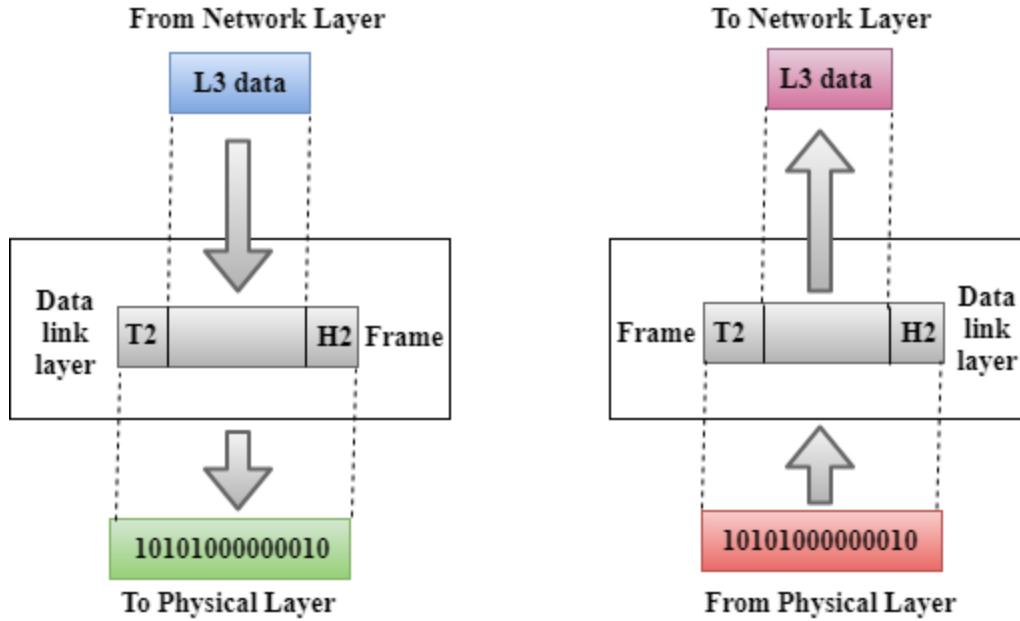


- The main functionality of the physical layer is to transmit the individual bits from one node to another node.
- It is the lowest layer of the OSI model.
- It establishes, maintains and deactivates the physical connection.
- It specifies the mechanical, electrical and procedural network interface specifications.

#### **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.

#### **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

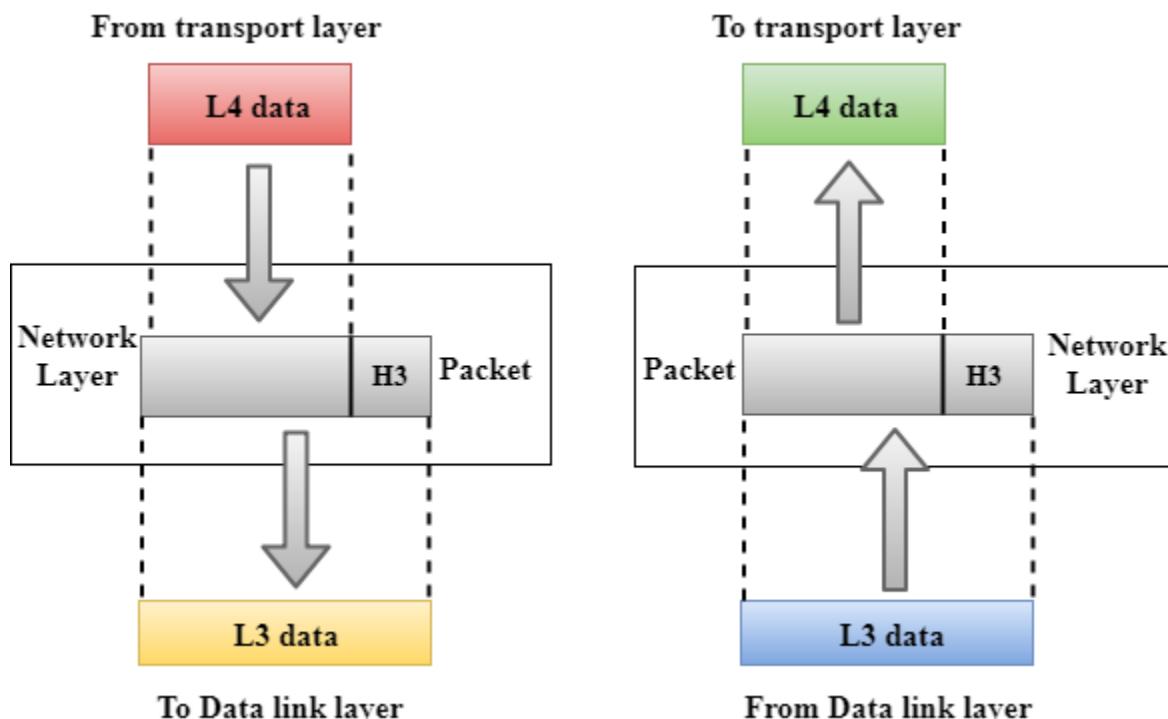
- **Framing:** The data link layer translates the physical's raw bit stream into packets known as Frames. The Data link layer adds the header and trailer to the frame. The header which is added to the frame contains the hardware destination and source address.



- **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.

## Network Layer

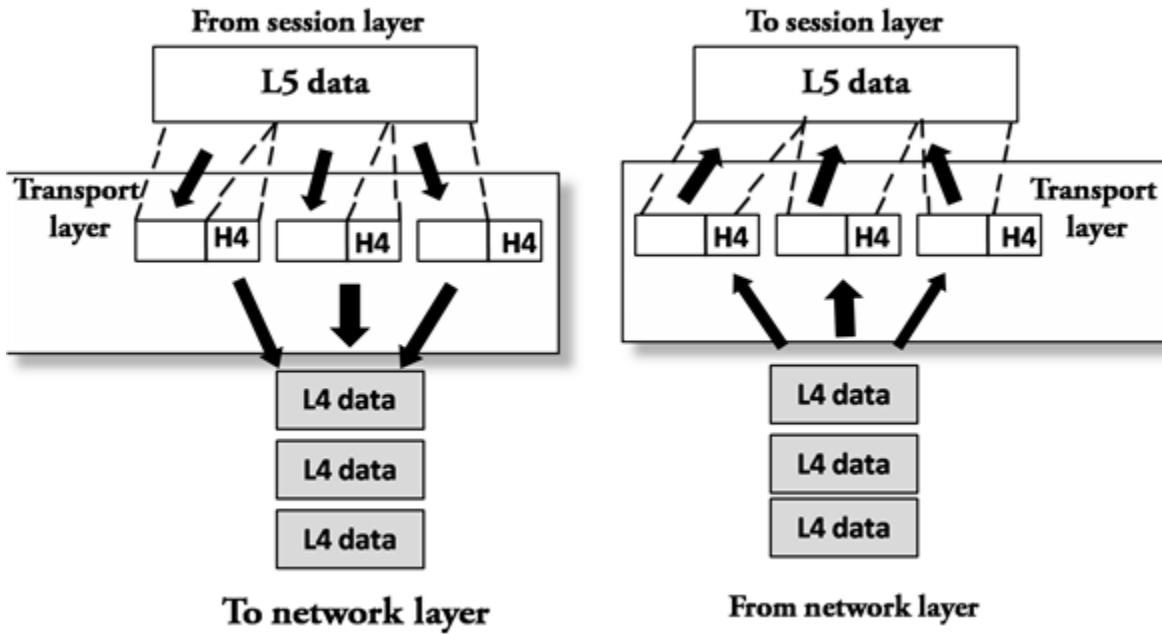


- It is a layer 3 that manages device addressing, tracks the location of devices on the network.
- It determines the best path to move data from source to the destination based on the network conditions, the priority of service, and other factors.
- The network layer is responsible for routing and forwarding 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).

## 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.

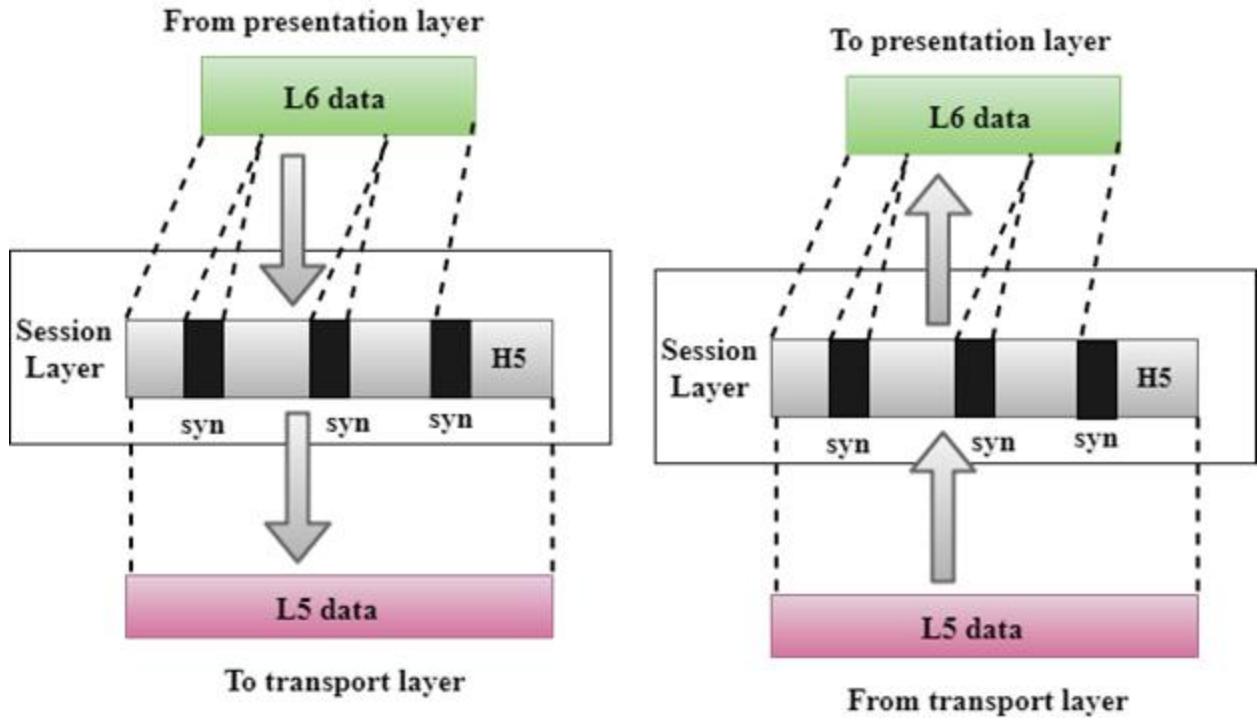
- **User Datagram Protocol**

- 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.

### **Session Layer**

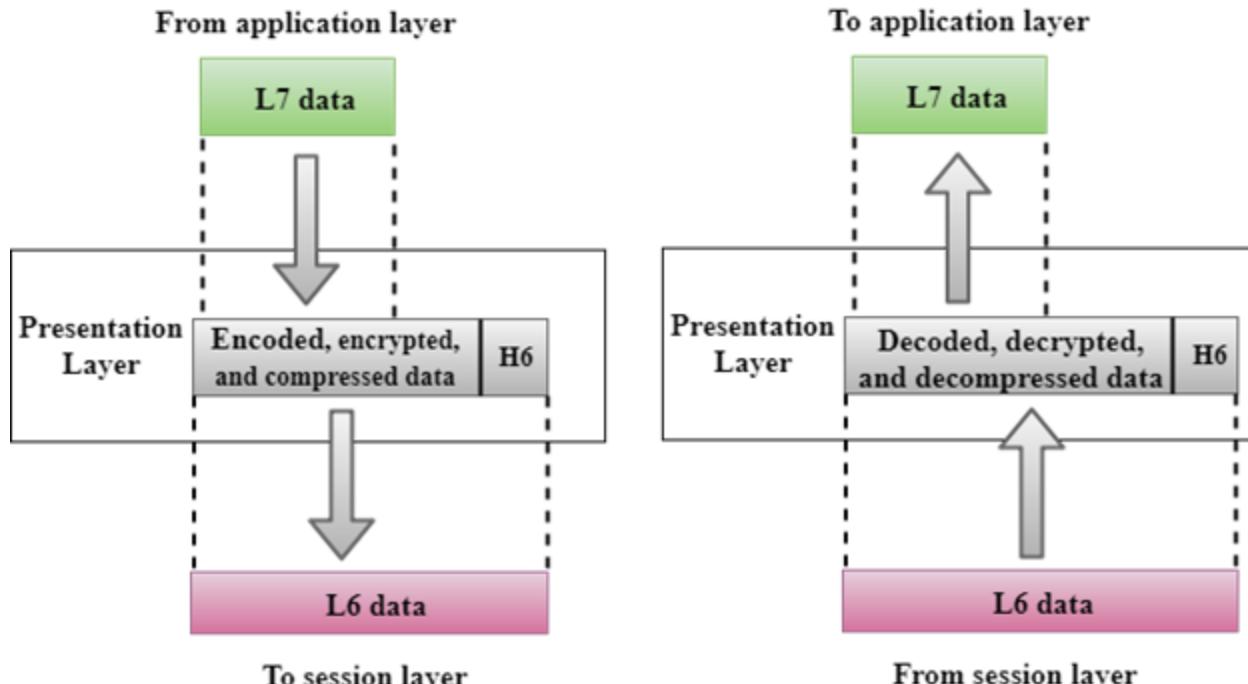


- It is a layer 3 in the OSI model.
- The Session layer is used to establish, maintain and synchronizes the interaction between communicating devices.

#### 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.

#### Presentation Layer

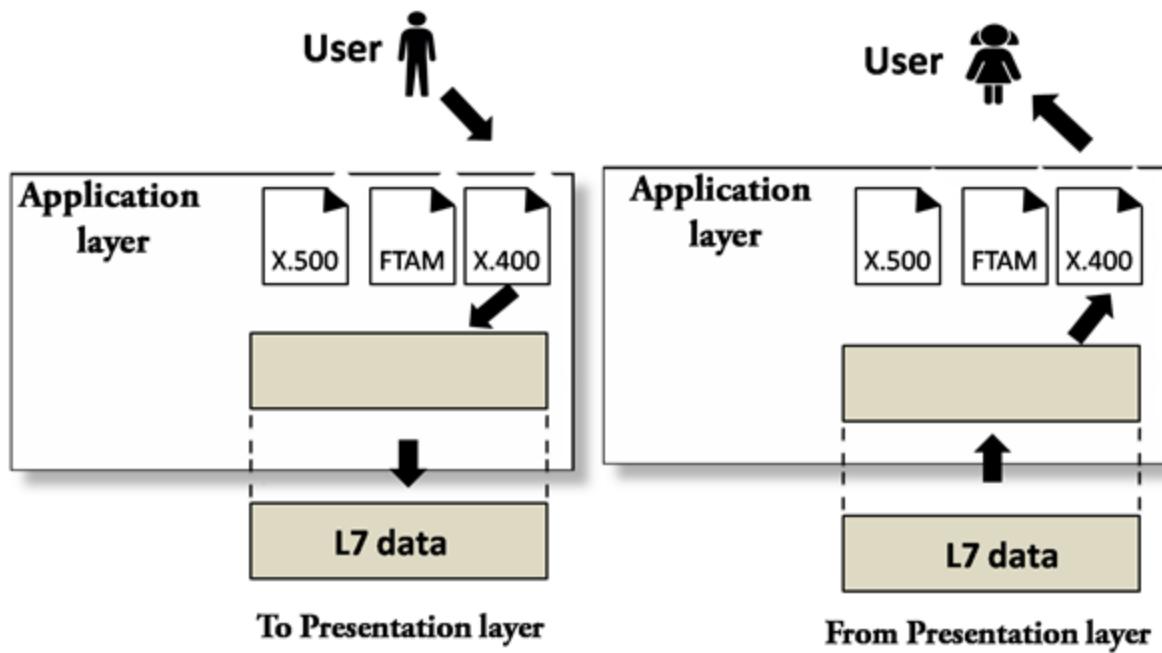


- A Presentation layer is mainly concerned with the syntax and semantics of the information exchanged between the two systems.
- It acts as a data translator for a network.
- This layer is a part of the operating system that converts the data from one presentation format to another format.
- The Presentation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

#### 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.

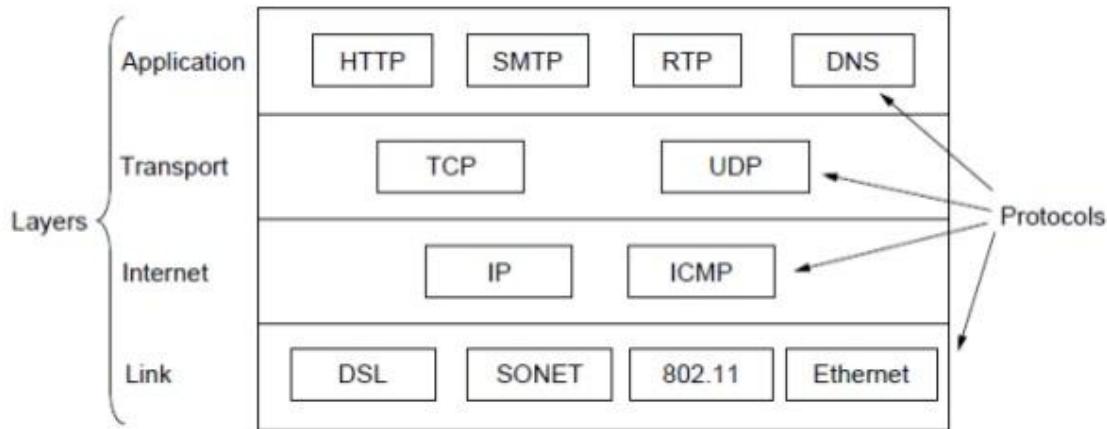
#### TCP/IP model

- The TCP/IP model was developed prior to the OSI model.
- The TCP/IP model is not exactly similar to the OSI model.
- The TCP/IP model consists of five layers: the application layer, transport layer, network layer, data link layer and physical layer.
- 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.
- 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:

## The TCP/IP Reference Model (2)



The TCP/IP reference model with some protocols we will study

### 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.

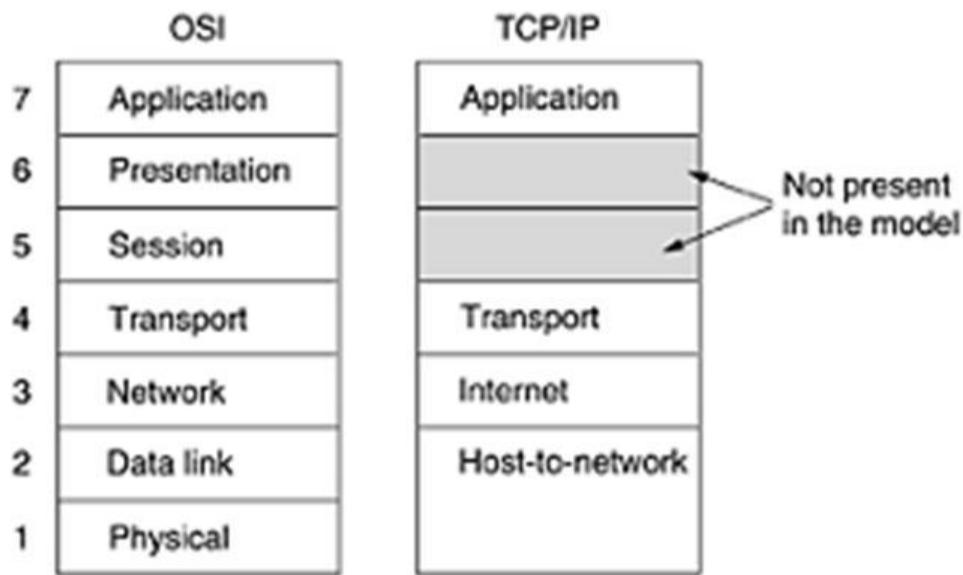
### Internet Layer

- 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 sends back its physical address in the form of ARP reply. The recipient adds the physical address both to its cache memory and to the datagram header

### **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**.

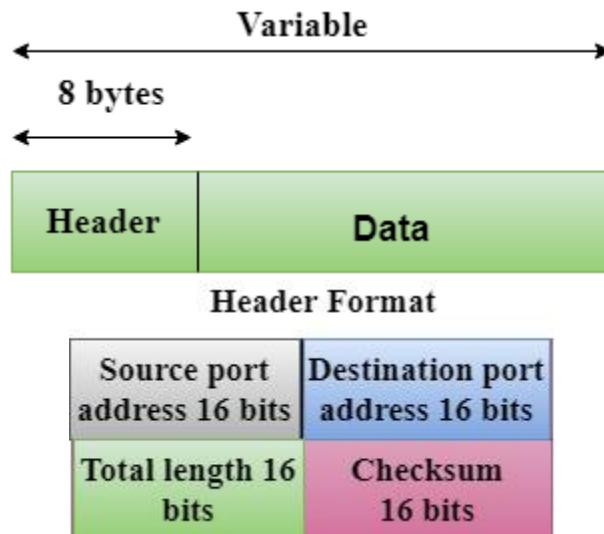
- **User Datagram Protocol (UDP)**
    - It provides connectionless service and end-to-end delivery of transmission.
    - It is an unreliable protocol as it discovers the errors but not specify the error.
    - User Datagram Protocol discovers the error, and ICMP protocol reports the error to the sender 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.



- **Transmission Control Protocol (TCP)**

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

---

## 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.

#### **Comparison of OSI Reference Model and TCP/IP Reference Model**

<b>OSI(Open System Interconnection)</b>	<b>TCP/IP(Transmission Control Protocol / Internet Protocol)</b>
1. OSI is a generic, protocol independent standard, acting as a communication gateway between the network and end user.	1. TCP/IP model is based on standard protocols around which the Internet has developed. It is a communication protocol, which allows connection of hosts over a network.
2. In OSI model the transport layer guarantees the delivery of packets.	2. In TCP/IP model the transport layer does not guarantees delivery of packets. Still the TCP/IP model is more reliable.
3. Follows vertical approach.	3. Follows horizontal approach.
4. OSI model has a separate Presentation layer and Session layer.	4. TCP/IP does not have a separate Presentation layer or Session layer.
5. OSI is a reference model around which the networks are built. Generally it is used as a guidance tool.	5. TCP/IP model is, in a way implementation of the OSI model.
6. Network layer of OSI model provides both connection oriented and connectionless service.	6. The Network layer in TCP/IP model provides connectionless service.

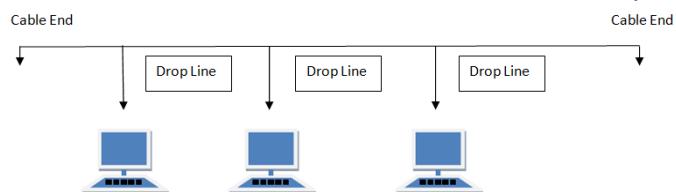
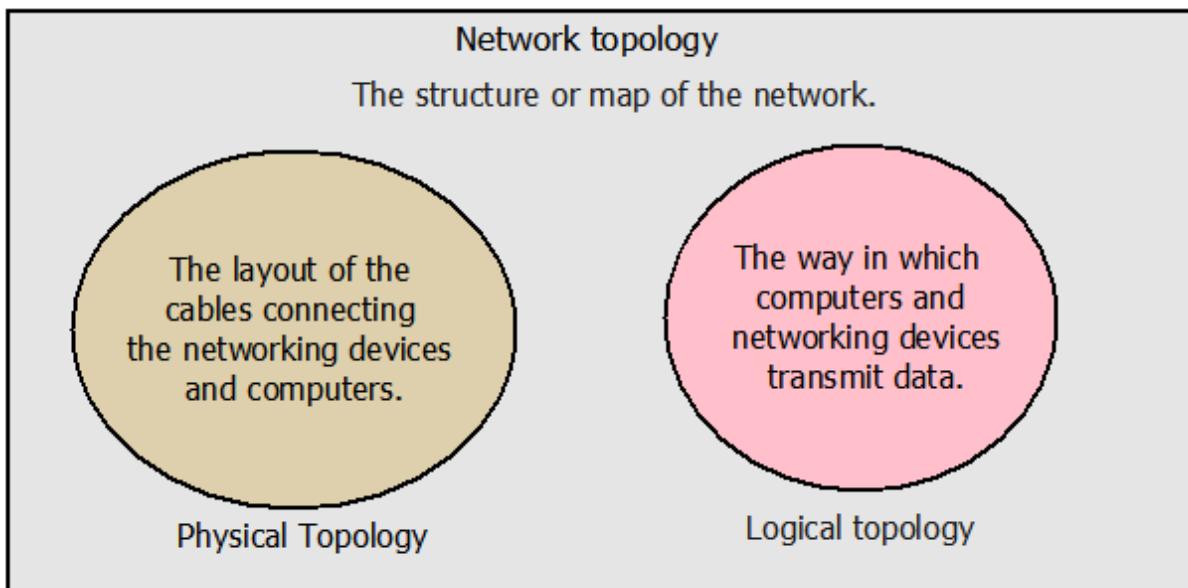
7. OSI model has a problem of fitting the protocols into the model.	7. TCP/IP model does not fit any protocol
8. Protocols are hidden in OSI model and are easily replaced as the technology changes.	8. In TCP/IP replacing protocol is not easy.

### Types of Network Topology:

Network Topology is the schematic description of a network arrangement, connecting various nodes(sender and receiver) through lines of connection.

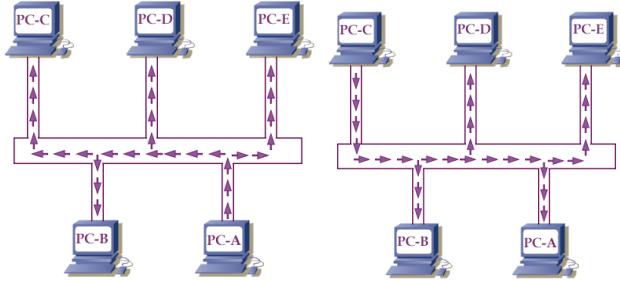
#### BUS Topology

Bus topology is a network type in which every computer and network device is connected to single cable. When it has exactly two endpoints, then it is called **Linear Bus topology**.



When a computer transmits data in this topology, all computers see that data over the wire, but only that computer accepts the data to which it is addressed. It is just like an announcement that is heard by all but answered only by the person to whom the announcement is made.

For example, if in the above network, **PC-A** sends data to the **PC-C** then all computers of the network receive this data but only the **PC-C** accepts it. The following image shows this process.



If **PC-C** replies, only the **PC-A** accepts the return data. The following image shows this process.

### Features of Bus Topology

1. It transmits data only in one direction.
2. Every device is connected to a single cable

### Advantages of Bus Topology

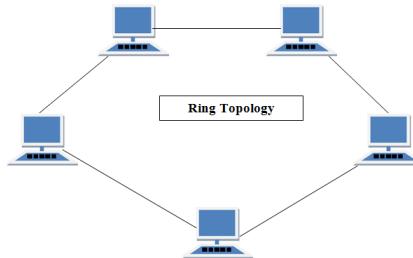
1. It is cost effective.
2. Cable required is least compared to other network topology.
3. Used in small networks.
4. It is easy to understand.
5. Easy to expand joining two cables together.

### Disadvantages of Bus Topology

1. Cables fails then whole network fails.
2. If network traffic is heavy or nodes are more the performance of the network decreases.
3. Cable has a limited length.
4. It is slower than the ring topology.

### RING Topology

It is called ring topology because it forms a ring as each computer is connected to another computer, with the last one connected to the first. Exactly two neighbours for each device.



### Features of Ring Topology

1. A number of repeaters are used for Ring topology with 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.
2. The transmission is unidirectional, but it can be made bidirectional by having 2 connections between each Network Node, it is called **Dual Ring Topology**.
3. In Dual Ring Topology, two ring networks are formed, and data flow is in opposite direction in them. Also, if one ring fails, the second ring can act as a backup, to keep the network up.

4. Data is transferred in a sequential manner that is bit by bit. Data transmitted, has to pass through each node of the network, till the destination node.

### **Advantages of Ring Topology**

1. Transmitting network is not affected by high traffic or by adding more nodes, as only the nodes having tokens can transmit data.
2. Cheap to install and expand

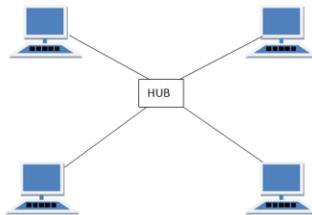
### **Disadvantages of Ring Topology**

1. Troubleshooting is difficult in ring topology.
2. Adding or deleting the computers disturbs the network activity.
3. Failure of one computer disturbs the whole network.

### **STAR Topology**

In this topology, all computers connect to a centralized networking device. Usually, a networking switch or a Hub (in earlier days) is used as the centralized device. Each computer in the network uses its own separate twisted pair cable to connect to the switch. Twisted pair cable uses **RJ-45** connectors on both ends.

The following image shows an example of the star topology.



To transmit data, the star topology uses the same concept which the bus topology uses. It means, if you build a network using the star topology, then that network will use the bus topology to transmit the data.

### **Features of Star Topology**

1. Every node has its own dedicated connection to the hub.
2. Hub acts as a repeater for data flow.
3. Can be used with twisted pair, Optical Fibre or coaxial cable.

### **Advantages of Star Topology**

1. Fast performance with few nodes and low network traffic.
2. Hub can be upgraded easily.
3. Easy to troubleshoot.
4. Easy to setup and modify.
5. Only that node is affected which has failed, rest of the nodes can work smoothly.

### **Disadvantages of Star Topology**

1. Cost of installation is high.
2. Expensive to use.
3. If the hub fails then the whole network is stopped because all the nodes depend on the hub.
4. Performance is based on the hub that is it depends on its capacity

### **MESH Topology**

It is a point-to-point connection to other nodes or devices. All the network nodes are connected to each other. Mesh has  $n(n-1)/2$  physical channels to link  $n$  devices.

$$\text{Required connections} = n * (n-1)/2$$

Here,  $n$  is the number of end devices or locations.

For example, to make a fully meshed network of 4 end devices, we need  $4*(4-1)/2 = 6$  connections.

There are two techniques to transmit data over the Mesh topology, they are :

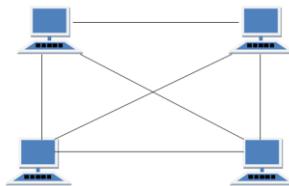
1. Routing
2. Flooding

### **MESH Topology: Routing**

In routing, the nodes have a routing logic, as per the network requirements. Like routing logic to direct the data to reach the destination using the shortest distance. Or, routing logic which has information about the broken links, and it avoids those node etc. We can even have routing logic, to re-configure the failed nodes.

### **MESH Topology: Flooding**

In flooding, the same data is transmitted to all the network nodes, hence no routing logic is required. The network is robust, and it's very unlikely to lose the data. But it leads to unwanted load over the network.



### **Types of Mesh Topology**

1. **Partial Mesh Topology** : In this topology some of the systems are connected in the same fashion as mesh topology but some devices are only connected to two or three devices.
2. **Full Mesh Topology** : Each and every nodes or devices are connected to each other.

### **Features of Mesh Topology**

1. Fully connected.
2. Robust.
3. Not flexible.

### **Advantages of Mesh Topology**

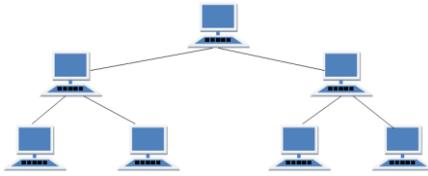
1. Each connection can carry its own data load.
2. It is robust.
3. Fault is diagnosed easily.
4. Provides security and privacy.

### **Disadvantages of Mesh Topology**

1. Installation and configuration is difficult.
2. Cabling cost is more.
3. Bulk wiring is required.

## **TREE Topology**

It has a root node and all other nodes are connected to it forming a hierarchy. It is also called hierarchical topology. It should at least have three levels to the hierarchy.



## **Features of Tree Topology**

1. Ideal if workstations are located in groups.
2. Used in Wide Area Network.

## **Advantages of Tree Topology**

1. Extension of bus and star topologies.
2. Expansion of nodes is possible and easy.
3. Easily managed and maintained.
4. Error detection is easily done.

## **Disadvantages of Tree Topology**

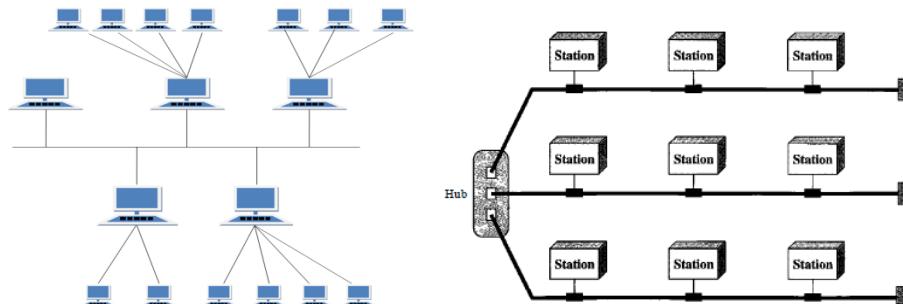
1. Heavily cabled.
2. Costly.
3. If more nodes are added maintenance is difficult.
4. Central hub fails, network fails.

## **HYBRID Topology**

This topology is a mix of two or more topologies. For example, there are two networks; one is built from the star topology and another is built from the bus topology. If we connect both networks to build a single large network, the topology of the new network will be known as the hybrid topology.

You are not restricted to the bus and star topologies. You can combine any topology with another topology. In modern network implementations, the hybrid topology is mostly used to mix the wired network with the wireless network.

The following image shows an example of the hybrid network topology.



## **Features of Hybrid Topology**

- It is a combination of two or more topologies
- Inherits the advantages and disadvantages of the topologies included

## **Advantages of Hybrid Topology**

- Reliable as Error detecting and trouble shooting is easy.
- Effective.
- Scalable as size can be increased easily.
- Flexible.

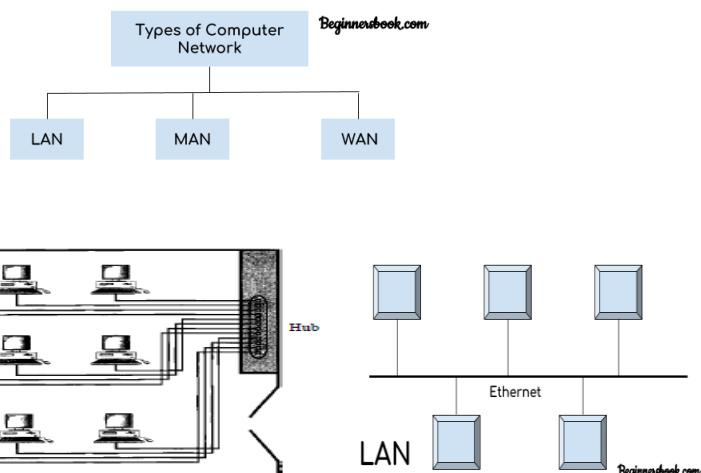
### Disadvantages of Hybrid Topology

- Complex in design.
- Costly.

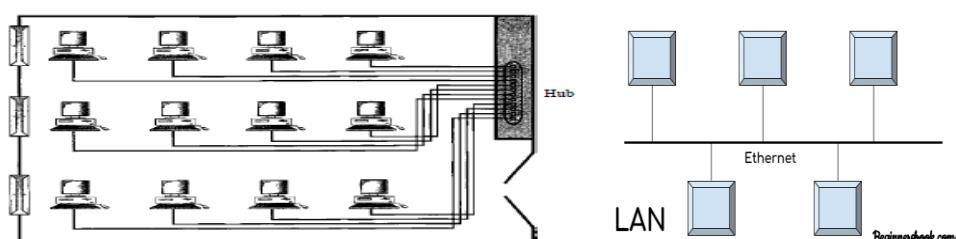
### Types of Computer Network: LAN, MAN and WAN

The **Network** allows computers to **connect and communicate** with different computers via any medium. LAN, MAN and WAN are the three major types of the network designed to operate over the area they cover. There are some similarities and dissimilarities between them. One of the major differences is the geographical area they cover, i.e. **LAN** covers the smallest area; **MAN** covers an area larger than LAN and **WAN** comprises the largest of all. There are other types of Computer Networks also, like :

- **PAN (Personal Area Network)**
- **SAN (Storage Area Network)**
- **EPN (Enterprise Private Network)**
- **VPN (Virtual Private Network)**



#### 1. Local Area Network (LAN)



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

## Topologies used in LANs

Various topologies are possible to form a LANs but three core forms can be identified easily as follows:

**Bus topology:** All devices are connected to a backbone cable, called the bus. The Bus networks are relatively less costly and very easy to install for small networks. Ethernet systems use a bus topology.

**Ring topology:** All devices are connected to one another in the shape of a closed loop, so that each device is connected directly to the neighboring device, one on either side of it. Ring topologies are relatively expensive and difficult to install, but they offer high bandwidth and can cover large distances.

**Star topology:** All devices are connected to a central hub device. Star networks are relatively easy to install and manage, but bottlenecks can occur because all data must pass through the hub.

These topologies can also be mixed to perform better. For example, a bus-star network consists of a high-bandwidth bus, which connects a collection of slower-bandwidth star segments.

## Characteristics of Local Area Network

- LANs are private owned-network, can be extended up to a few kilometers.
- LANs operate at relatively high speed as compared to the typical WAN
- It connects computers within a single office, building, block or campus, i.e. they work in a relatively small geographical area.

## Advantages of LAN

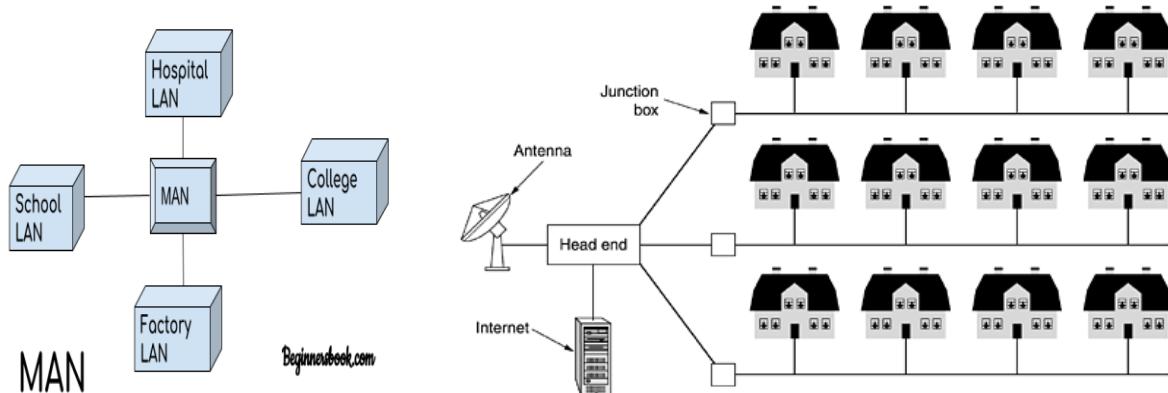
1. **Resource Sharing:** LAN provides resource sharing such as computer resources like printers, scanners, modems, DVD-ROM drives, and hard disks can be shared within the connected devices. This reduces cost and hardware purchases.
2. **Software Applications Sharing:** In a Local Area Network, it is easy to use the same software in a number of computers connected to a network instead of purchasing the separately licensed software for each client a network.
3. **Easy and Cheap Communication:** Data and messages can easily be shared with the other computer connected to the network.
4. **Centralized Data:** The data of all network users can be stored on a hard disk of the central/server computer. This help users to use any computer in a network to access the required data.
5. **Data Security:** Since data is stored on the server computer, it will be easy to manage data at only one place and the data will be more secure too.
6. **Internet Sharing:** Local Area Network provides the facility to share a single internet connection among all the LAN users. In school labs and internet Cafes, single internet connection is used to provide internet to all connected computers.

## Disadvantages of LAN

1. **High Setup Cost:** The initial setup costs of installing Local Area Networks is high because there is special software required to make a server. Also, communication devices like an ethernet cable, switches, hubs, routers, cables are costly.
2. **Privacy Violations:** The LAN administrator can see and check personal data files of each and every LAN user. Moreover, he can view the computer and internet history of the LAN user.
3. **Data Security Threat:** Unauthorised users can access important data of an office or campus if a server hard disk is not properly secured by the LAN administrator.

4. **LAN Maintenance Job:** Local Area Network requires a LAN Administrator because there are problems such as software installations, program faults or hardware failures or cable disturbances in Local Area Network. A LAN Administrator is required to maintain these issues.
5. **Covers Limited Area:** LANs are restricted in size they cover a small area like a single office, single building or a group of nearby buildings.

## 2. Metropolitan Area Network (MAN)



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

A **metropolitan area network (MAN)** is a large computer network that usually spans a city or a large campus. A MAN Network is optimized for a larger geographical area than a LAN, ranging from several blocks of buildings to entire cities.

MAN Networks are formed by connecting multiple LANs. Thus, MAN Networks are larger than LANs but smaller than wide-area networks (WAN).

The purpose of MAN (Metropolitan Area Network) is to provide the link to the internet in the long run. MAN Network provides Internet connectivity for LANs in a metropolitan region, and connect them to wider area networks like the Internet.” **It can also be used in cable television.**

The primary use of metropolitan area networks is the customer that has high-capacity needs in a metropolitan area. A MAN is intended to provide the required capacity at a lower cost and greater efficiency than obtaining an equivalent service from the local telephone company

### How Does a Metropolitan Area Network Work?

Metropolitan Area Network is larger than LAN and smaller than WAN. It is generally applied to connect geographically dispersed LANs. Therefore the goal of MAN is to develop a communication link between two independent LAN nodes.

A MAN Network is usually established using optical fiber. The network is established using routers and switches. A switch is a port which is active in handling the filtration of data usually coming in the form of frames. Any switch acts as a dual-port, at one end it is handling filtration of data and at the other end managing connections.

The router is another device for facilitating the network connection. A router helps the data packets to identify the path to be taken. Hence, in other words, it keeps an eye on the data transfer. MAN (Metropolitan Area Network) is usually operated over an area of up to 5 to 50kms.

#### Characteristics of Metropolitan Area Network

1. Network size generally ranges from 5 to 50 km. It may be as small as a group of buildings on campus to as large as covering the whole city.
2. In general, a MAN is either owned by a user group or by a network provider who sells service to users, rather than a single organization as in LAN.
3. Data rates are moderate to high.
4. It facilitates the sharing of regional resources.
5. They provide uplinks for connecting LANs to WANs and the Internet.

#### Uses of Metropolitan Area Network (MAN)

Some of the Uses of MAN are:-

- Digital cable television
- Used in government agencies
- University campuses
- Cable broadband
- Used to connect several branches of the local school
- In hospital (for communication between doctors, research offices, labs)
- A network of fire stations
- In airports
- Networking between community colleges within the country
- Used in public libraries

#### Advantages of a MAN Network

There are many advantages of the MAN network, some of them given below.

##### **1: Less Expensive:**

It is less expensive to attach MAN with WAN Network. MAN gives you good efficiency of data. All data on MAN is easily manageable in a centralized way.

##### **2: Sending Local Emails:**

You can send local emails fast and free on MAN.

##### **3: High Speed than WAN:**

The speed of data can easily reach 1000 Mbps, as MAN uses fiber optics. Files and database transfer rates are fast.

##### **4: Sharing of the Internet:**

With the installation of MANs, users can share their internet connection. In this way, multiple users can get the same high-speed internet.

##### **5: Conversion of LAN to MAN is Easy:**

MAN is a combination of two or more LAN network. So it is a faster way to connect two LAN networks together. It is possible by the fast configuration of links.

## **6: High Security:**

MAN's has a high-security level than WAN.

Disadvantages of MAN Network

### **1: Difficult To Manage:**

It is very difficult to manage if the size and number of LANs network increase. This is due to security and extra configuration problems.

### **2: Internet Speed Difference:**

As it cannot work on phone copper wires. Copper wires affect the speed of MAN. So high cost is needed for fiber optics.

### **3: Hackers Attack:**

In this network, there is a high risk of attacking hackers as compared to LAN. So data may be a leak.

Highly security staff is the need in MAN.

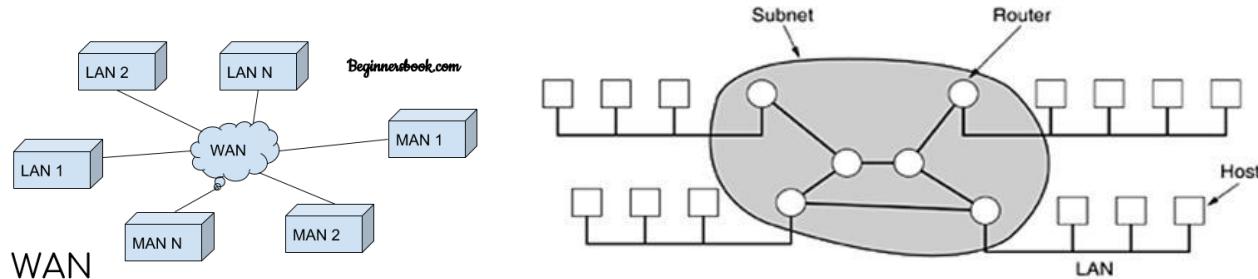
### **4: Technical Staff Requires to Set up:**

Highly technical people require to setup MAN. The technical people are network administrators and troubleshooters.

### **5: Need More wires:**

In MAN more than LAN network, cables require. As you know, it is a combination of two LANs.

## **3. Wide area network (WAN)**



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

- A Wide Area Network is a network that extends over a large geographical area such as states or countries.
- A Wide Area Network is quite bigger network than the LAN.
- A Wide Area Network is not limited to a single location, but it spans over a large geographical area through a telephone line, fibre optic cable or satellite links.
- The internet is one of the biggest WAN in the world.
- A Wide Area Network is widely used in the field of Business, government, and education.

### **Advantages of WAN:**

**Centralized infrastructure:** One of the main advantage of WAN is the that we do not need to maintain the backup and store data on local system as everything is stored online on a data centre, from where we can access the data through WAN.

**Privacy:** We can setup the WAN in such a way that it encrypts the data that we share online that way the data is secure and minimises the risk of unauthorized access.

**Increased Bandwidth:** With the WAN we get to choose the bandwidth based on the need, a large organization can have larger bandwidth that can carry large amount of data faster and efficiently.

**Area:** A WAN can cover a large area or even a whole world though internet connection thus we can connect with the person in another country through WAN which is not possible in other type of computer networks.

### Disadvantages of WAN:

**Antivirus:** Since our systems are connected with the large amount of systems, there is possibility that we may unknowingly download the virus that can affect our system and become threat to our privacy and may lead to data loss.

**Expensive:** Cost of installation is very high.

**Issue resolution:** Issue resolution takes time as the WAN covers large area, it is really difficult to pin point the exact location where the issues raised and causing the problem.

Sr. No.	Key	LAN	MAN	WAN
1	Definition	LAN stands for Local Area Network.	MAN stands for Metropolitan Area Network.	WAN stands for Wide Area Network.
2	Ownership	LAN is often owned by private organizations.	MAN ownership can be private or public.	WAN ownership can be private or public.
3	Speed	LAN speed is quite high.	MAN speed is average.	WAN speed is lower than that of LAN.
4	Delay	Network Propagation Delay is short in LAN.	Network Propagation Delay is moderate in MAN.	Network Propagation Delay is longer in WAN.
5	Congestion	LAN has low congestion as compared to WAN.	MAN has higher congestion than LAN.	WAN has higher congestion than both MAN and LAN.
6	Fault Tolerance	Fault Tolerance of LAN is higher than WAN.	Fault Tolerance of MAN is lower than LAN.	Fault Tolerance of WAN is lower than both LAN and MAN.

Sr. No.	Key	LAN	MAN	WAN
7	Maintenance	Designing and maintaining LAN is easy and less costly than WAN.	Designing and maintaining WAN is complex and more costly than LAN and MAN.	Designing and maintaining WAN is complex and more costly than both LAN and MAN.

## Switching

- When a user accesses the internet or another computer network outside their immediate location, messages are sent through the network of transmission media. This technique of transferring the information from one computer network to another network is known as **switching**.
- Switching in a computer network is achieved by using switches. A switch is a small hardware device which is used to join multiple computers together with one local area network (LAN).
- Network switches operate at layer 2 (Data link layer) in the OSI model.
- Switching is transparent to the user and does not require any configuration in the home network.
- Switches are used to forward the packets based on MAC addresses.
- A Switch is used to transfer the data only to the device that has been addressed. It verifies the destination address to route the packet appropriately.
- It is operated in full duplex mode.
- Packet collision is minimum as it directly communicates between source and destination.
- It does not broadcast the message as it works with limited bandwidth.

## Why is Switching Concept required?

Switching concept is developed because of the following reasons:

- **Bandwidth:** It is defined as the maximum transfer rate of a cable. It is a very critical and expensive resource. Therefore, switching techniques are used for the effective utilization of the bandwidth of a network.
- **Collision:** Collision is the effect that occurs when more than one device transmits the message over the same physical media, and they collide with each other. To overcome this problem, switching technology is implemented so that packets do not collide with each other.

Advantages of Switching:

- Switch increases the bandwidth of the network.
- It reduces the workload on individual PCs as it sends the information to only that device which has been addressed.
- It increases the overall performance of the network by reducing the traffic on the network.
- There will be less frame collision as switch creates the collision domain for each connection.

Disadvantages of Switching:

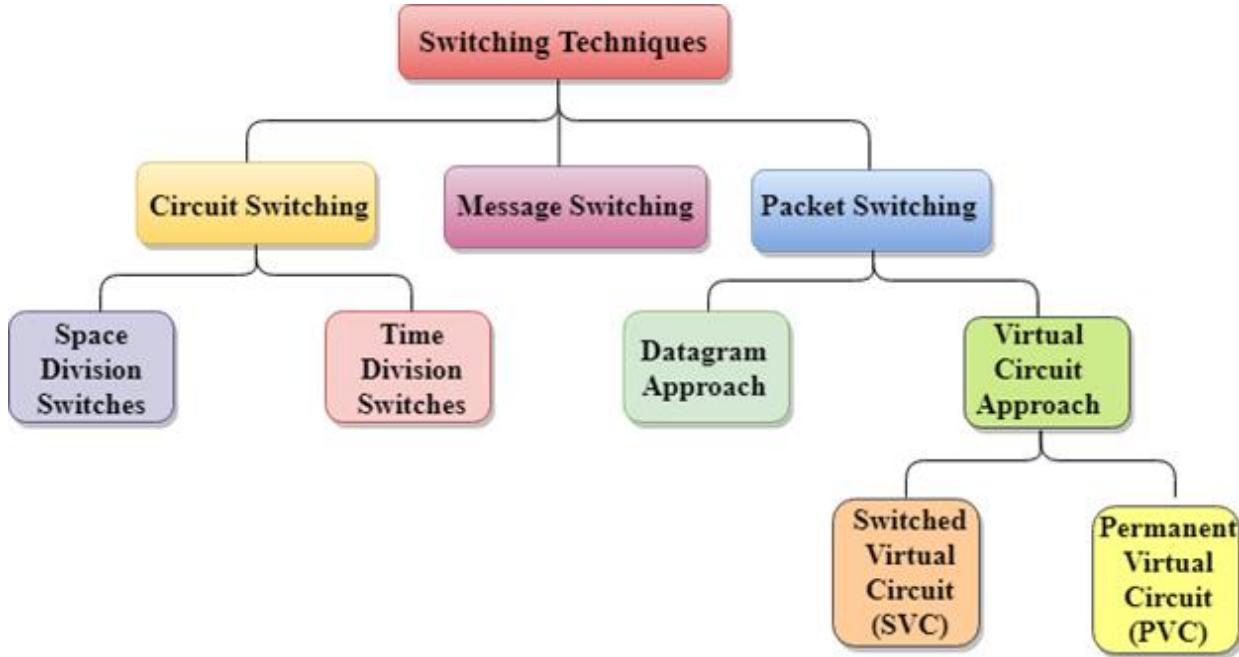
- A Switch is more expensive than network bridges.
- A Switch cannot determine the network connectivity issues easily.
- Proper designing and configuration of the switch are required to handle multicast packets.

## **Switching techniques**

In large networks, there can be multiple paths from sender to receiver. The switching technique will decide the best route for data transmission.

Switching technique is used to connect the systems for making one-to-one communication.

### **Classification Of Switching Techniques**



## Circuit Switching

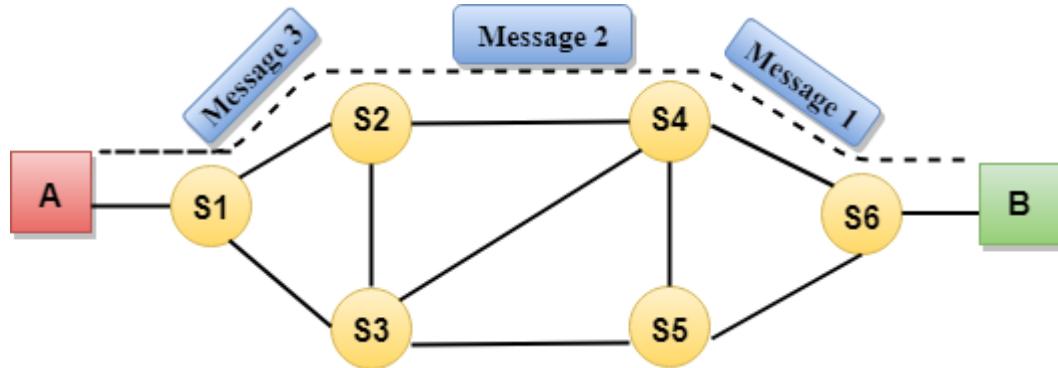
- Circuit switching is a switching technique that establishes a dedicated path between sender and receiver.
- In the Circuit Switching Technique, once the connection is established then the dedicated path will remain to exist until the connection is terminated.
- Circuit switching in a network operates in a similar way as the telephone works.
- A complete end-to-end path must exist before the communication takes place.
- In case of circuit switching technique, when any user wants to send the data, voice, video, a request signal is sent to the receiver then the receiver sends back the acknowledgment to ensure the availability of the dedicated path. After receiving the acknowledgment, dedicated path transfers the data.
- Circuit switching is used in public telephone network. It is used for voice transmission.
- Fixed data can be transferred at a time in circuit switching technology.

**Communication through circuit switching has 3 phases:**

Features of Java - Javatpoint

- Circuit establishment

- Data transfer
- Circuit Disconnect



Circuit Switching can use either of the two technologies:

### **Space Division Switches:**

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

**Space Division Switches can be categorized in two ways:**

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

### **Crossbar Switch**

The Crossbar switch is a switch that has  $n$  input lines and  $n$  output lines. The crossbar switch has  $n^2$  intersection points known as **crosspoints**.

#### **Disadvantage of Crossbar switch:**

The number of crosspoints increases as the number of stations is increased. Therefore, it becomes very expensive for a large switch. The solution to this is to use a multistage switch.

## **Multistage Switch**

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

### **Advantages Of Circuit Switching:**

- In the case of Circuit Switching technique, the communication channel is dedicated.
- It has fixed bandwidth.

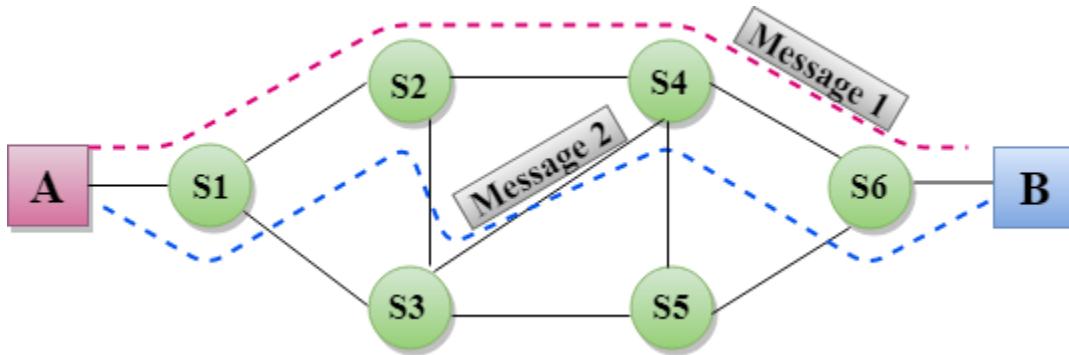
### **Disadvantages Of Circuit Switching:**

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

## **Message Switching**

- Message Switching is a switching technique in which a message is transferred as a complete unit and routed through intermediate nodes at which it is stored and forwarded.
- In Message Switching technique, there is no establishment of a dedicated path between the sender and receiver.
- The destination address is appended to the message. Message Switching provides a dynamic routing as the message is routed through the intermediate nodes based on the information available in the message.

- Message switches are programmed in such a way so that they can provide the most efficient routes.
- Each and every node stores the entire message and then forward it to the next node. This type of network is known as **store and forward network**.
- Message switching treats each message as an independent entity.



### **Advantages Of Message Switching**

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

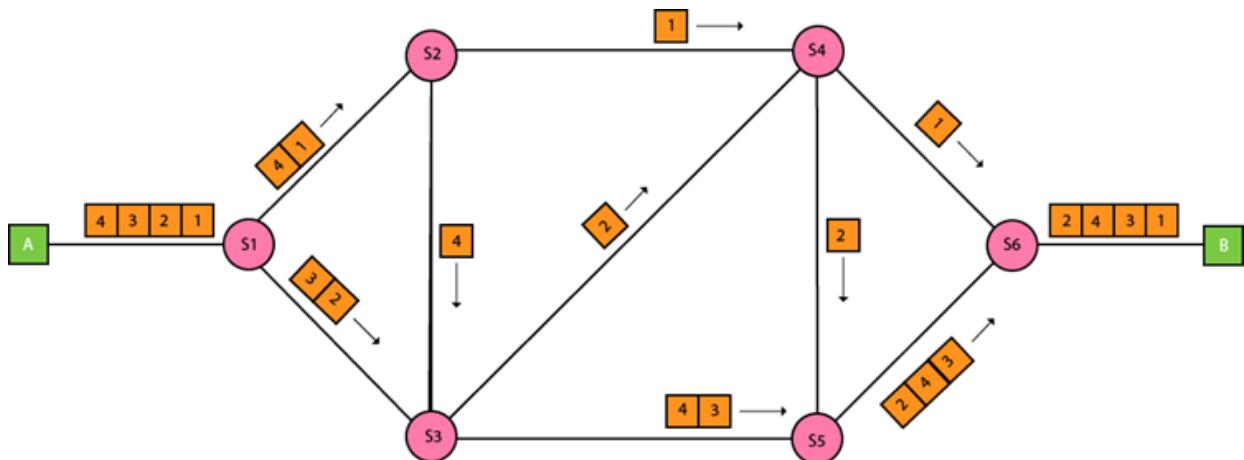
### **Disadvantages Of Message Switching**

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

## **Packet Switching**

- The packet switching is a switching technique in which the message is sent in one go, but it is divided into smaller pieces, and they are sent individually.

- The message splits into smaller pieces known as packets and packets are given a unique number to identify their order at the receiving end.
- Every packet contains some information in its headers such as source address, destination address and sequence number.
- Packets will travel across the network, taking the shortest path as possible.
- All the packets are reassembled at the receiving end in correct order.
- If any packet is missing or corrupted, then the message will be sent to resend the message.
- If the correct order of the packets is reached, then the acknowledgment message will be sent.



## Approaches Of Packet Switching:

There are two approaches to Packet Switching:

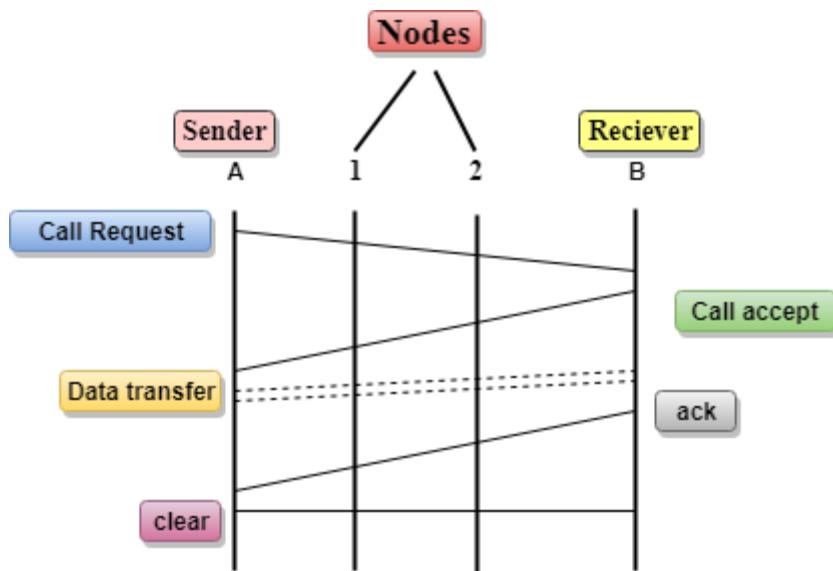
### Datagram Packet switching:

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

## Virtual Circuit Switching

- Virtual Circuit Switching is also known as connection-oriented switching.
- In the case of Virtual circuit switching, a preplanned route is established before the messages are sent.
- Call request and call accept packets are used to establish the connection between sender and receiver.
- In this case, the path is fixed for the duration of a logical connection.

Let's understand the concept of virtual circuit switching through a diagram:



- In the above diagram, A and B are the sender and receiver respectively. 1 and 2 are the nodes.
- Call request and call accept packets are used to establish a connection between the sender and receiver.
- When a route is established, data will be transferred.
- After transmission of data, an acknowledgment signal is sent by the receiver that the message has been received.
- If the user wants to terminate the connection, a clear signal is sent for the termination.

Differences b/w Datagram approach and Virtual Circuit approach

<b>Datagram approach</b>	<b>Virtual Circuit approach</b>
Node takes routing decisions to forward the packets.	Node does not take any routing decision.
Congestion cannot occur as all the packets travel in different directions.	Congestion can occur when the node is busy, and it does not allow other packets to pass through.
It is more flexible as all the packets are treated as an independent entity.	It is not very flexible.

### **Advantages Of Packet Switching:**

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

### **Disadvantages Of Packet Switching:**

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

### **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:

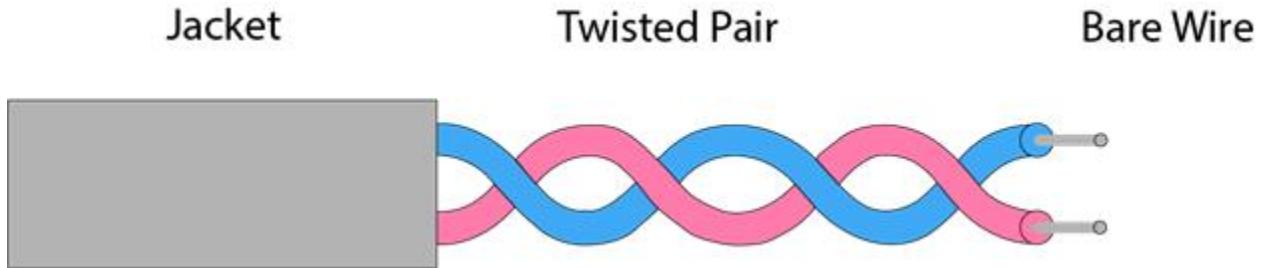
Twisted pair:

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.

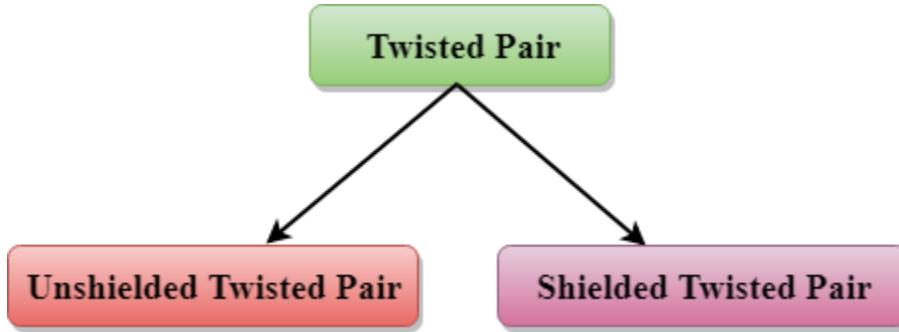
A twisted pair consists of two insulated copper wires arranged in a regular spiral pattern.

Hello Java Program for Beginners

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:

- It is cheap.
- Installation of the unshielded twisted pair is easy.
- 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.

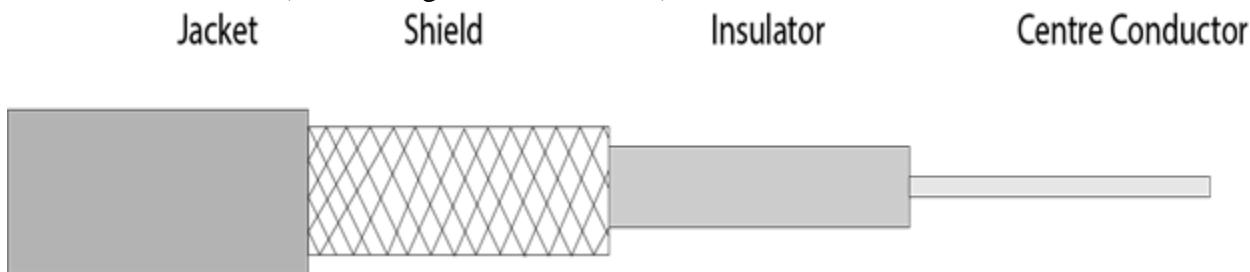
### **Disadvantages**

- 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 provide faster data transmission than copper wires.

### Diagrammatic representation of fibre optic cable:



### Basic elements of Fibre optic cable:

- **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.
- **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.
- **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 to 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 obstruction 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.

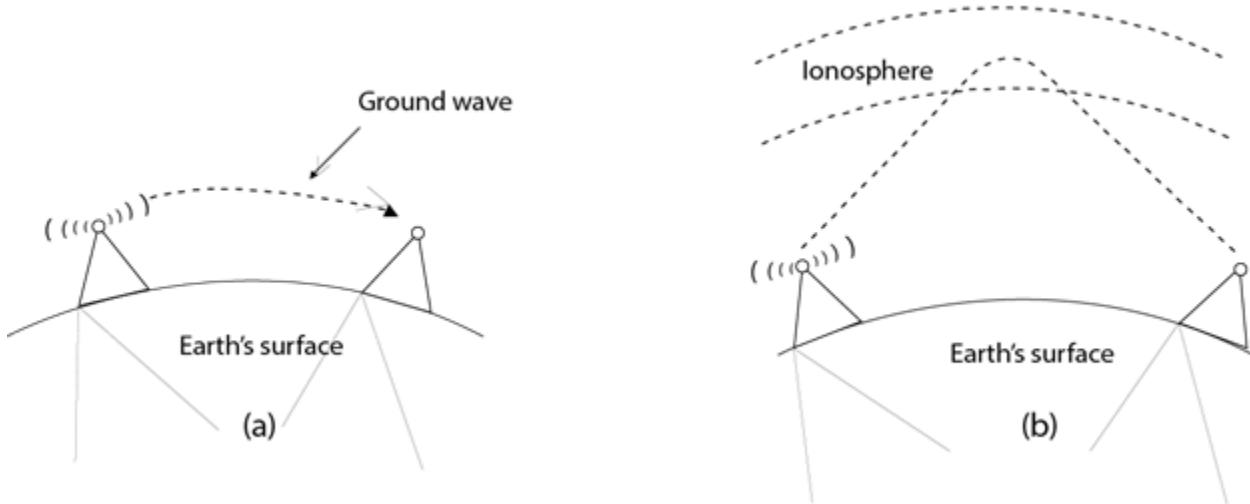
## UnGuided Transmission

- 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:

### Radio waves

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



### Applications Of Radio waves:

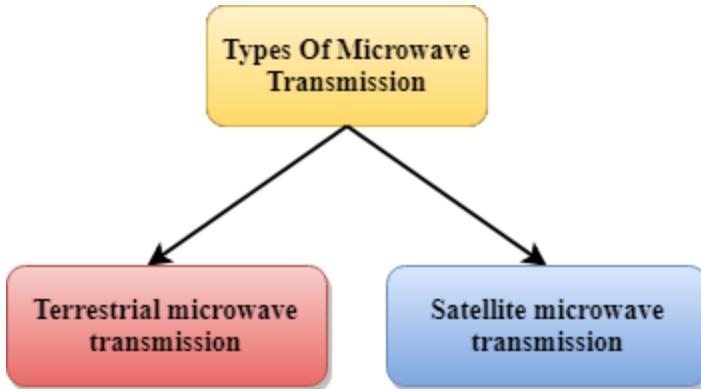
- A Radio wave is useful for multicasting when there is one sender and many receivers.
- An FM radio, television, cordless phones are examples of a radio wave.

### 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.

---

## Microwaves



Microwaves are of two types:

- Terrestrial microwave
- 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 focussed.
- 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:

- The coverage area of a satellite microwave is more than the terrestrial microwave.
- The transmission cost of the satellite is independent of the distance from the centre of the coverage area.
- Satellite communication is used in mobile and wireless communication applications.
- It is easy to install.
- 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

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

## **Network Devices (Hub, Repeater, Bridge, Switch, Router, Gateways and Brouter)**

**1. Repeater** – A repeater operates at the physical layer. Its job is to regenerate the signal over the same network before the signal becomes too weak or corrupted so as to extend the length to which the signal can be transmitted over the same network. An important point to be noted about repeaters is that they do not amplify the signal. When the signal becomes weak, they copy the signal bit by bit and regenerate it at the original strength. It is a 2 port device.

**2. Hub** – A hub is basically a multiport repeater. A hub connects multiple wires coming from different branches, for example, the connector in star topology which connects different stations. Hubs cannot filter data, so data packets are sent to all connected devices. In other words, the collision domain of all hosts connected through Hub remains one. Also, they do not have the intelligence to find out the best path for data packets which leads to inefficiencies and wastage.

### **Types of Hub**

- **Active Hub**:- These are the hubs that have their own power supply and can clean, boost, and relay the signal along with the network. It serves both as a repeater as well as a wiring center. These are used to extend the maximum distance between nodes.
- **Passive Hub** :- These are the hubs that collect wiring from nodes and power supply from the active hub. These hubs relay signals onto the network without cleaning and boosting them and can't be used to extend the distance between nodes.
- **Intelligent Hub** :- It works like active hubs and includes remote management capabilities. They also provide flexible data rates to network devices. It also enables an administrator to monitor the traffic passing through the hub and to configure each port in the hub.

**3. Bridge** – A bridge operates at the data link layer. A bridge is a repeater, with add on the functionality of filtering content by reading the MAC addresses of source and destination. It is also used for interconnecting two LANs working on the same protocol. It has a single input and single output port, thus making it a 2 port device.

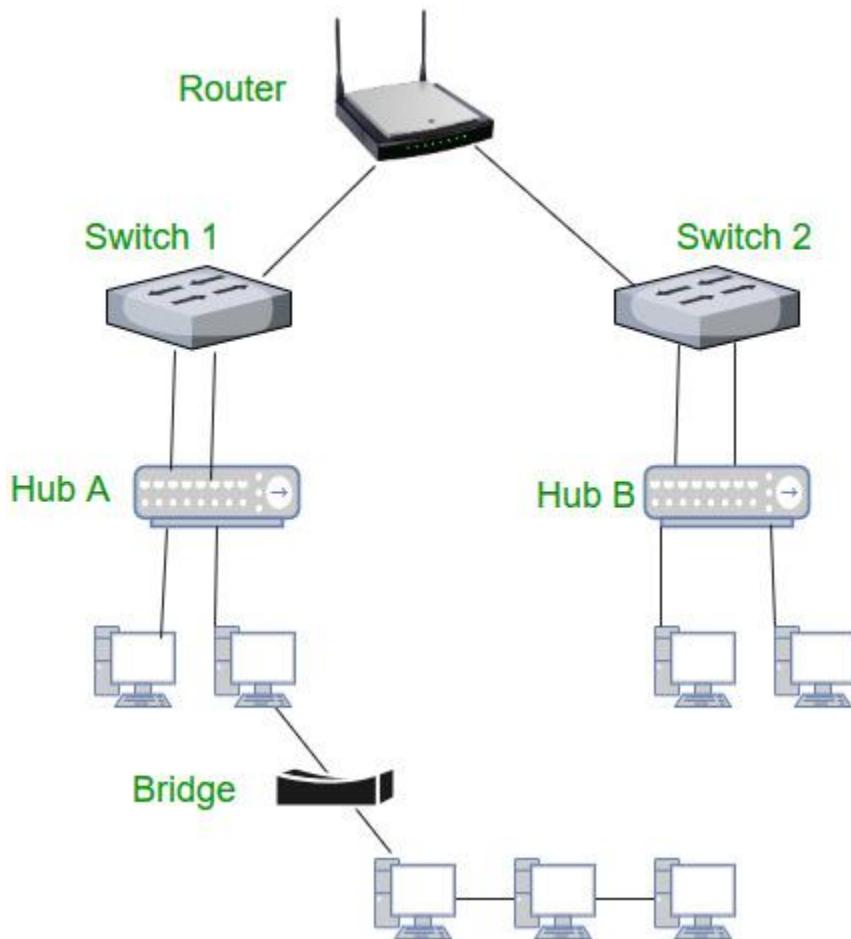
### **Types of Bridges**

- **Transparent Bridges**:- These are the bridge in which the stations are completely unaware of the bridge's existence i.e. whether or not a bridge is added or deleted from the network, reconfiguration of the stations is unnecessary. These bridges make use of two processes i.e. bridge forwarding and bridge learning.

- **Source Routing Bridges:-** In these bridges, routing operation is performed by the source station and the frame specifies which route to follow. The host can discover the frame by sending a special frame called the discovery frame, which spreads through the entire network using all possible paths to the destination.

**4. Switch** – A switch is a multiport bridge with a buffer and a design that can boost its efficiency(a large number of ports imply less traffic) and performance. A switch is a data link layer device. The switch can perform error checking before forwarding data, which makes it very efficient as it does not forward packets that have errors and forward good packets selectively to the correct port only. In other words, the switch divides the collision domain of hosts, but broadcast domain remains the same.

**5. Routers** – A router is a device like a switch that routes data packets based on their IP addresses. The router is mainly a Network Layer device. Routers normally connect LANs and WANs together and have a dynamically updating routing table based on which they make decisions on routing the data packets. Router divide broadcast domains of hosts connected through it.



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

**7. Brouter** – It is also known as the bridging router is a device that combines features of both bridge and router. It can work either at the data link layer or a network layer. Working as a router, it is capable of routing packets across networks, and working as the bridge, it is capable of filtering local area network traffic.

**8. NIC** – NIC or network interface card is a network adapter that is used to connect the computer to the network. It is installed in the computer to establish a LAN. It has a unique id that is written on the chip, and it has a connector to connect the cable to it. The cable acts as an interface between the computer and router or modem. NIC card is a layer 2 device which means that it works on both physical and data link layer of the network model.