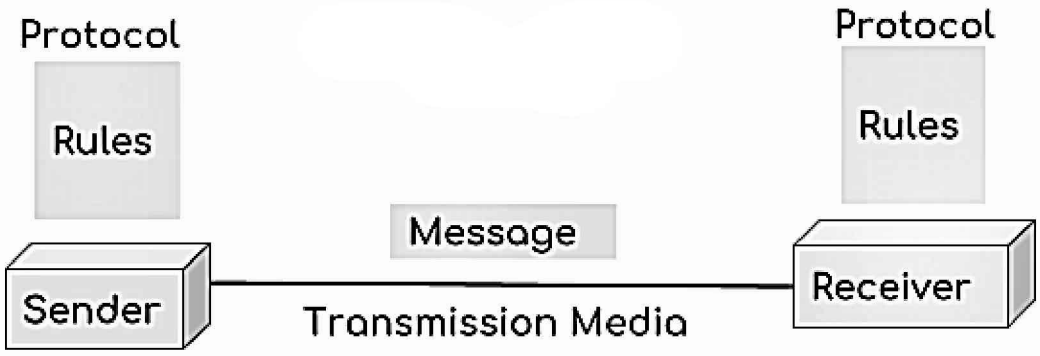
Introduction to Computer Network

A computer network is a group of devices connected with each other through a transmission medium such as wires, cables etc. These devices can be computers, printers, scanners, Fax machines etc.

The purpose of having computer network is to send and receive data stored in other devices over the network. These devices are often referred as nodes.

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



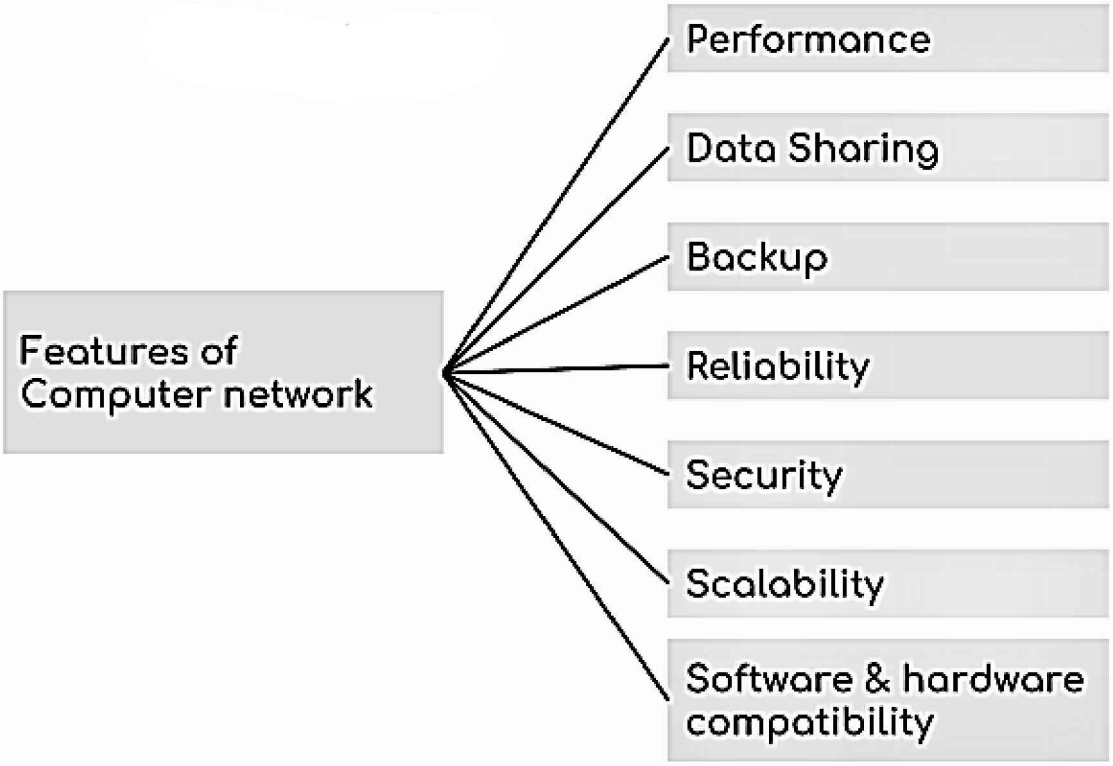
Message: It is the data or information which needs to be transferred from one device to another device over a computer network.

Sender: Sender is the device that has the data and needs to send the data to other device connected to the network.

Receiver: A receiver is the device which is expecting the data from other device on the network.
Transmission media: In order to transfer data from one device to another device we need a transmission media such as wires, cables, radio waves etc.

Protocol: A protocol is a set of rules that are agreed by both sender and receiver, without a protocol two devices can be connected to each other but they cannot communicate. In order to establish a reliable communication or data sharing between two different devices we need set of rules that are called protocol. For example, http and https are the two protocols used by web browsers to get and post the data to internet, similarly smtp protocol is used by email services connected to the internet.

Computer Network Features



A computer network has following features:

Performance: Performance of a computer network is measured in terms of response time. The response time of sending and receiving data from one node (computer in a computer network are often referred as node) to another should be minimal.

Data Sharing: One of the reason why we use a computer network is to share the data between different systems connected with each other through a transmission media.

Backup: A computer network must have a central server that keeps the backup of all the data that is to be shared over a network so that in case of a failure it should be able to recover the data faster.

Software and hardware compatibility: A computer network must not limit all the computers in a computer network to use same software and hardware, instead it should allow the better compatibility between the different software and hardware configuration.

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

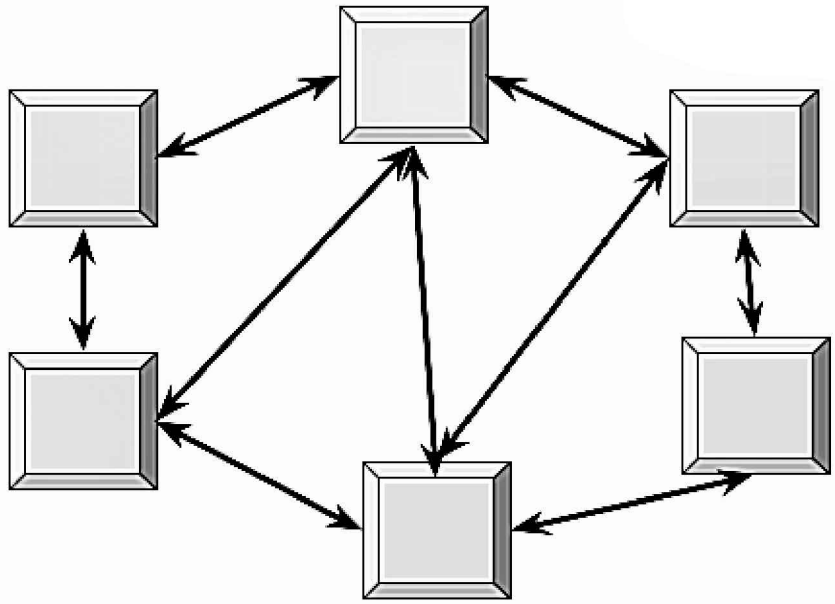
Security: A computer network should be secure so that the data transmitting over a network should be safe from unauthorized access. Also, the sent data should be received as it is at the receiving node, which means there should not be any loss of data during transmission.

Scalability: A computer network should be scalable which means it should always allow to add new computers (or nodes) to the already existing computer network. For example, a company runs 100 computers over a computer network for their 100 employees, let's say they hire another 100 employees and want to add new 100 computers to the already existing LAN then in that case the local area computer network should allow this.

Computer Network Architecture

A **Computer Architecture** is a design in which all computers in a computer network are organized. A architecture defines how the computers should get connected to get the maximum advantages of a computer network such as better response time, security, scalability etc. The two most popular computer architectures are **P2P (Peer to Peer)** and **Client-Server architecture**.

Peer to Peer Architecture



In peer to peer architecture all the computers in a computer network are connected with every computer in the network. Every computer in the network use the same resources as other computers. There is no central computer that acts as a server rather all computers acts as a server for the data that is stored in them.

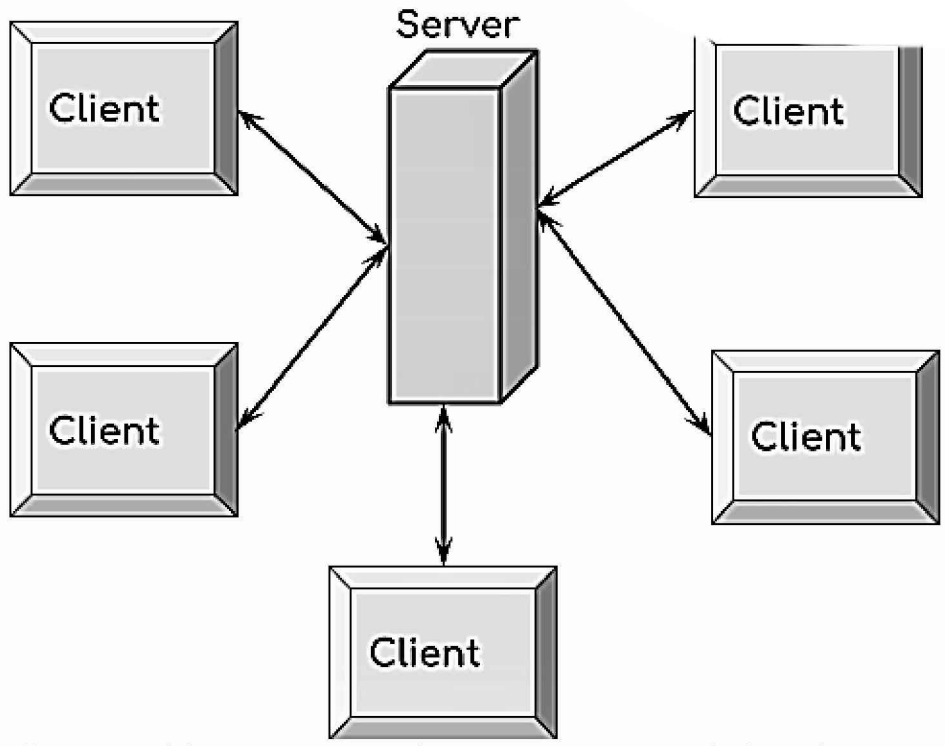
Advantages of a Peer to Peer Architecture

1. Less costly as there is no central server that has to take the backup.
2. In case of a computer failure all other computers in the network are not affected and they will continue to work as same as before the failure.
3. Installation of peer to peer architecture is quite easy as each computer manages itself.

Disadvantages of a Peer to Peer Architecture

1. Each computer has to take the backup rather than a central computer and the security measures are to be taken by all the computers separately.
2. Scalability is a issue in a peer to Peer Architecture as connecting each computer to every computer is a headache on a very large network.

Client Server Architecture



In Client Server architecture a central computer acts as a hub and serves all the requests from client computers. All the shared data is stored in the server computer which is shared with the client computer when a request is made by the client computer.

All the communication takes place through the server computer, for example if a client computer wants to share the data with other client computer then it has to send the data to server first and then the server will send the data to other client.

Advantages of Client Server Architecture

1. Data backup is easy and cost effective as there is no need to manage the backup on each computer.
2. Performance is better as the response time is greatly improves because the server is more powerful computer than the other computers in the network.
3. Security is better as unauthorized access are denied by server computer and all the data goes through the server.
4. Scalability is not an issue in this Architecture as large number of computers can be connected with server.

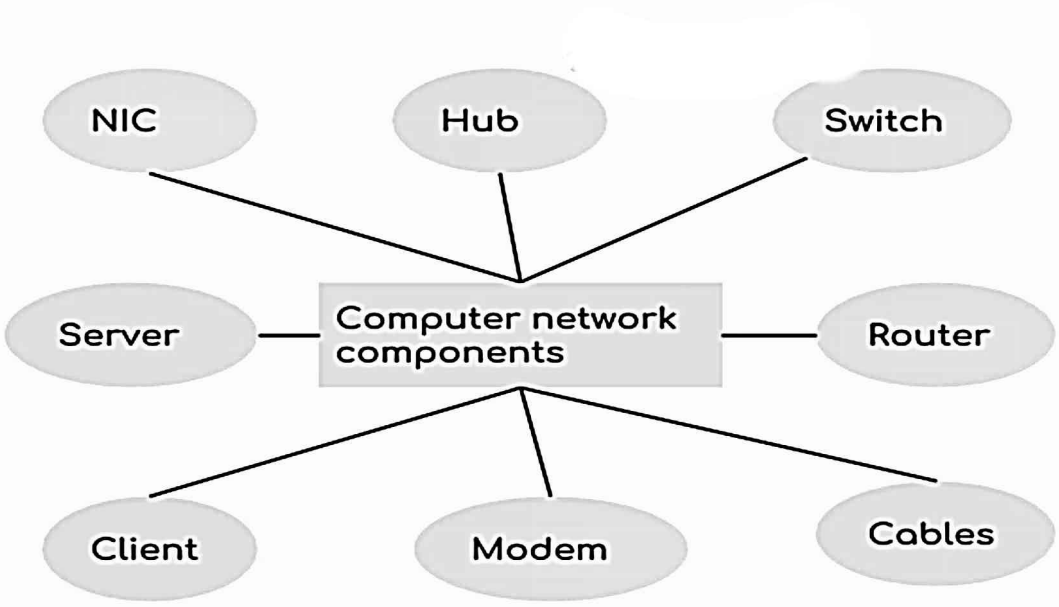
Disadvantages of Client Server Architecture

1. In case of server failure entire network is down.
2. Server maintenance cost is high as the server is the main component in this Architecture
3. Cost is high as the server needs more resources to handle that many client requests and to be able to hold large amount of data.

Computer Network Components

A computer network is build up from several components. These components together makes it possible to transfer data from one device to another and makes smooth communication between two different devices. In this guide, we will discuss the main components of a computer network.

Basic components of a computer network



Server: Servers are computers that runs operating system and hold data that can be shared over a computer network.

Client: A client is a computer that is connected to other computers in the network and can receive data sent by other computers.

Transmission Media: All computers in a computer network are connected with each other through a transmission media such as wires, optical fiber cables, coaxial cables etc.

Network Interface card: Each system or computer in a computer network must have a card called network interface card (NIC). The main purpose of NIC is to format the data, send the data and receive the data at the receiving node.

Hub: Hub acts as a device that connects all the computer in a network to each other. Any request that comes from a client computer first received by Hub and then hub transmit this request over a network so that the correct server receives and respond to it.

Switch: Switch is similar to hub however instead of broadcasting a incoming data request it uses the physical device address in the incoming request to transfer the request to correct server computer.

Router: Router joins multiple computer networks to each other. For example lets say a company runs 100 computers over a local area network(LAN) and another company runs another LAN of 150 computers. These both LANs can be connected with each other through a internet connection which is provided by the router.

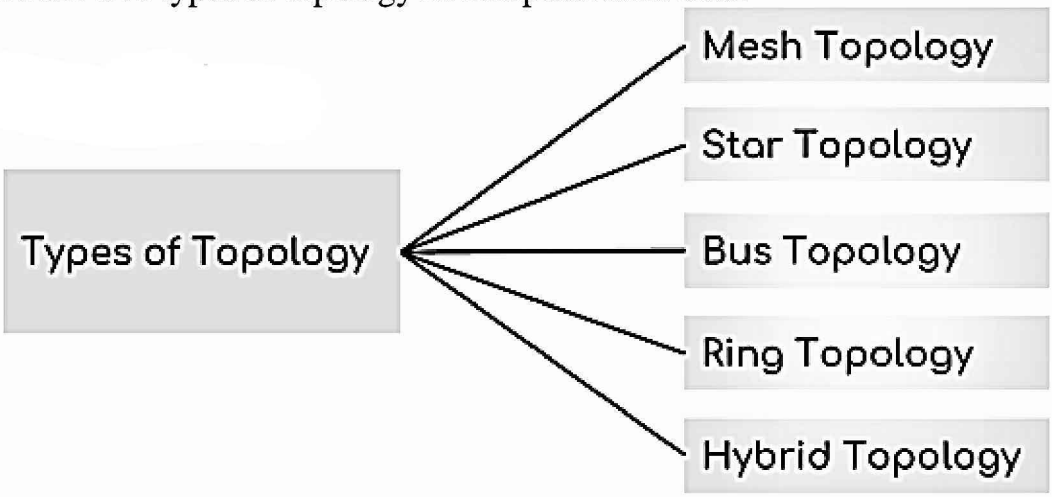
LAN cable: A wire that is used to connect more than one computers or other devices such as printers and scanner to each other.

Computer Network Topology – Mesh, Star, Bus, Ring and Hybrid

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

Types of Topology

There are five types of topology in computer networks:



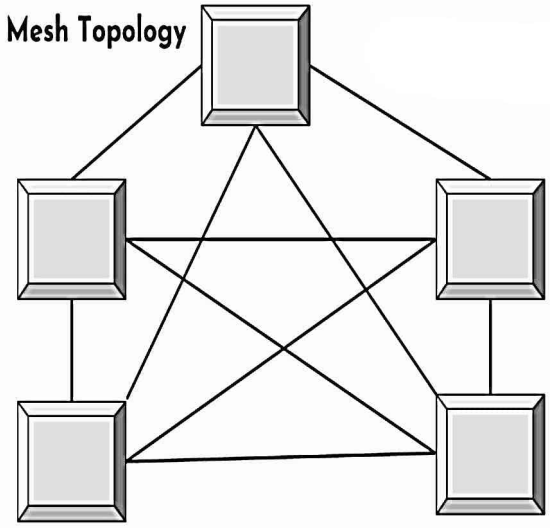
1. Mesh Topology
2. Star Topology
3. Bus Topology
4. Ring Topology
5. Hybrid Topology

Mesh Topology

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

Advantages of Mesh topology

1. No data traffic issues as there is a dedicated link between two devices which means the link is only available for those two devices.
2. Mesh topology is reliable and robust as failure of one link doesn't affect other links and the communication between other devices on the network.
3. Mesh topology is secure because there is a point to point link thus unauthorized access is not possible.
4. Fault detection is easy.

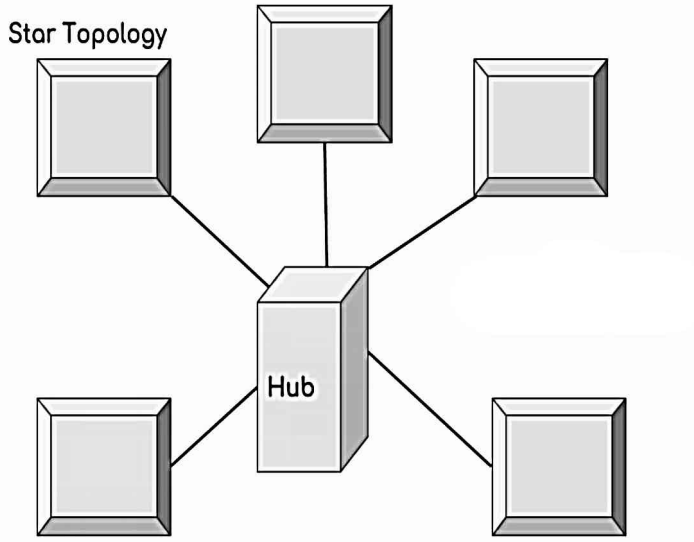


Disadvantages of Mesh topology

1. Amount of wires required to connected each system is tedious and headache.
2. Since each device needs to be connected with other devices, number of I/O ports required must be huge.
3. Scalability issues because a device cannot be connected with large number of devices with a dedicated point to point link.

Star Topology

In star topology each device in the network is connected to a central device called hub. Unlike Mesh topology, star topology doesn't allow direct communication between devices, a device must have to communicate through hub. If one device wants to send data to other device, it has to first send the data to hub and then the hub transmit that data to the designated device.



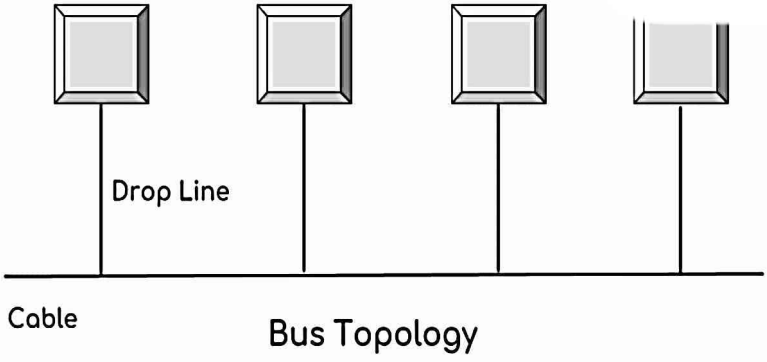
Advantages of Star topology

1. Less expensive because each device only need one I/O port and needs to be connected with hub with one link.
2. Easier to install
3. Less amount of cables required because each device needs to be connected with the hub only.
4. Robust, if one link fails, other links will work just fine.
5. Easy fault detection because the link can be easily identified.

Disadvantages of Star topology

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

Bus Topology



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

Advantages of bus topology

1. Easy installation, each cable needs to be connected with backbone cable.
2. Less cables required than Mesh and star topology

Disadvantages of bus topology

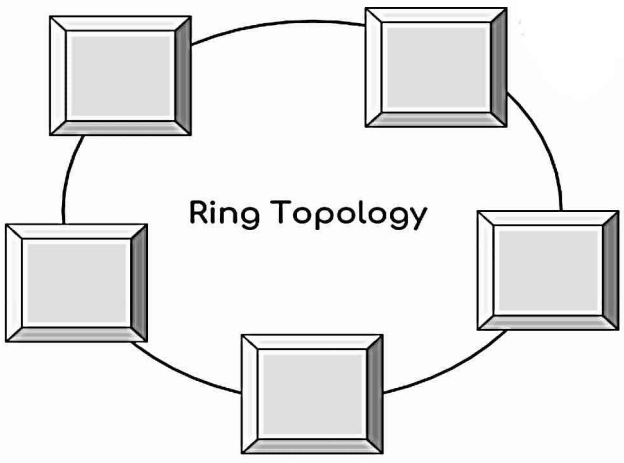
1. Difficultly in fault detection.
2. Not scalable as there is a limit of how many nodes you can connect with backbone cable.

Ring Topology

In ring topology each device is connected with the two devices on either side of it. There are two dedicated point to point links a device has with the devices on the either side of it. This structure forms a ring thus it is known as ring topology. If a device wants to send data to another device then it sends the data in one direction, each device in ring topology has a repeater, if the received data is intended for other device then repeater forwards this data until the intended device receives it.

Advantages of Ring Topology

1. Easy to install.
2. Managing is easier as to add or remove a device from the topology only two links are required to be changed.



Disadvantages of Ring Topology

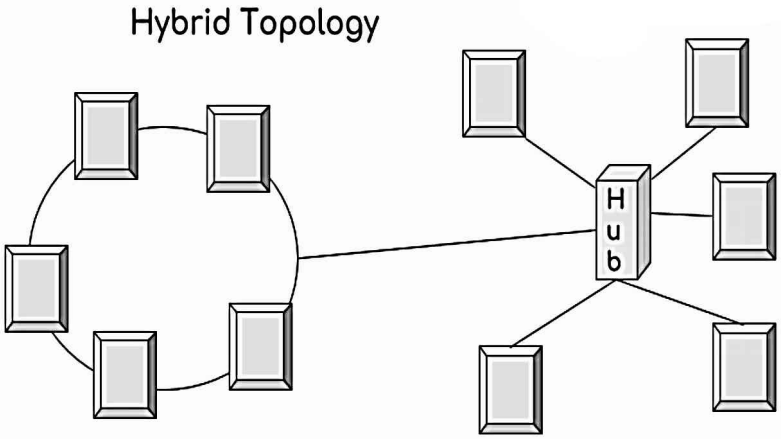
1. A link failure can fail the entire network as the signal will not travel forward due to failure.
2. Data traffic issues, since all the data is circulating in a ring.

Hybrid topology

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

Advantages of Hybrid topology

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



Disadvantages of Hybrid topology

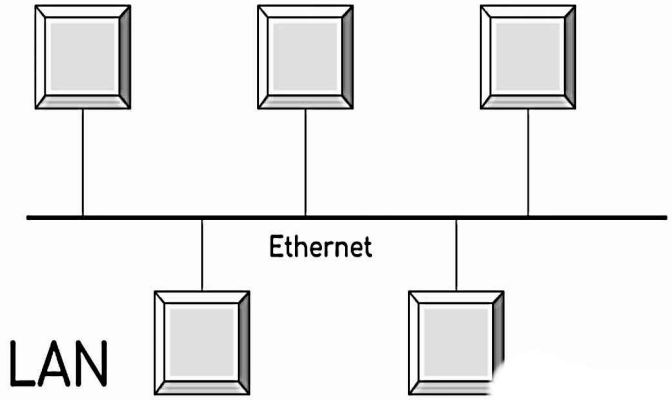
1. Fault detection is difficult.
2. Installation is difficult.
3. Design is complex so maintenance is high thus expensive.

Types of Computer Network: LAN, MAN and WAN

A computer network is a group of computers connected with each other through a transmission medium such as cable, wire etc.

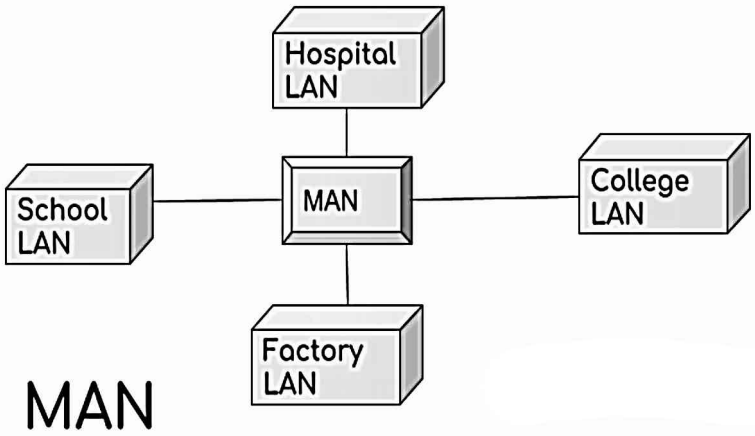
There are mainly three types of computer networks based on their size:
1. Local Area Network (LAN)
2. Metropolitan Area Network (MAN)
3. Wide area network (WAN)

1. Local Area Network (LAN)



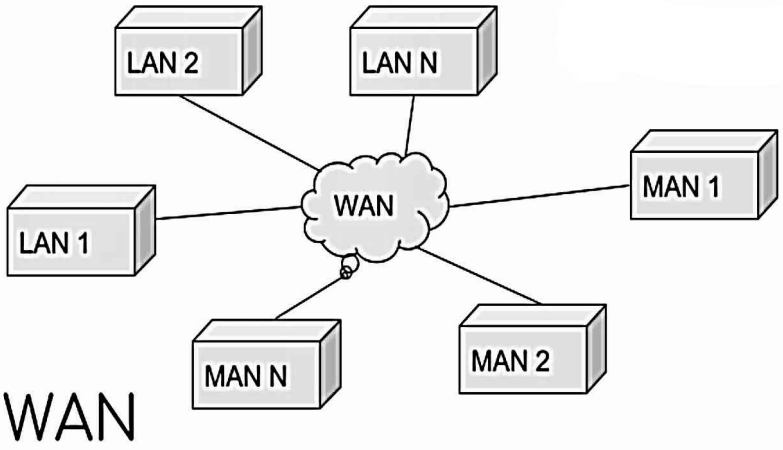
1. Local area network is a group of computers connected with each other in a small places such as school, hospital, apartment etc.
2. LAN is secure because there is no outside connection with the local area network thus the data which is shared is safe on the local area network and can't be accessed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

2. Metropolitan Area Network (MAN)



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

3. Wide area network (WAN)



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

Advantages of WAN:

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

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

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

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

Disadvantages of WAN:

virus: 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 becomes 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.

Computer Network Transmission Modes

The data is transmitted from one device to another device through a **transmission mode**. The transmission mode decides the direction of data in which the data needs to travel to reach the receiver system or node.

The transmission mode is divided in **three** categories:

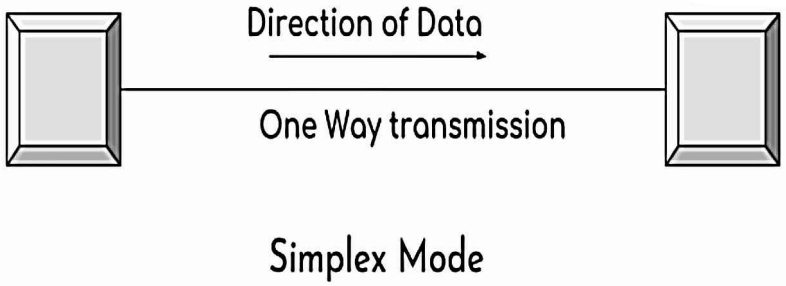
1. Simplex
2. Half-Duplex
3. Full-Duplex

Simplex Mode

1. In simplex mode the data transmits in one direction only, from one system to another system.
2. The sender device that sends data can only send data and cannot receive it. On the other hand the receiver device can only receive the data and cannot send it.
3. Television is an example of simplex mode transmission as the broadcast sends signals to our TV but never receives signals back from our TV. This is a unidirectional transmission.

Advantages of Simplex Mode:
The full capacity of the transmission medium is utilised as the transmission is one way and cannot have traffic issues.

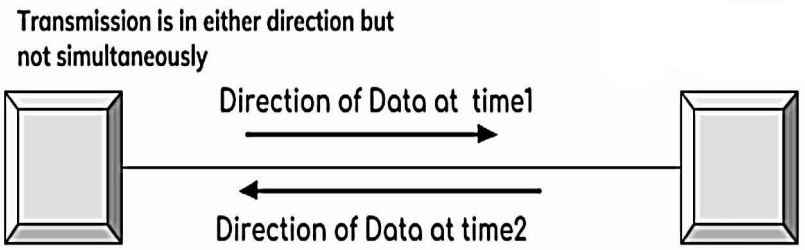
Disadvantages of Simplex Mode:
No bidirectional communication is possible. Two devices cannot communicate with each other using simplex mode of transmission.



Simplex Mode

Half-Duplex Mode

1. In half duplex mode transmission can be done both ways which means if two systems are connected with half-duplex mode of transmission, they both can send and receive data but not at the same time.
2. If one device is sending data then other device cannot send data until it receives the data which is already in transmission. You can say that the communication is not simultaneous.
3. The radio communication device that our soldiers use at the battle fields are the examples of



Half-Duplex Mode

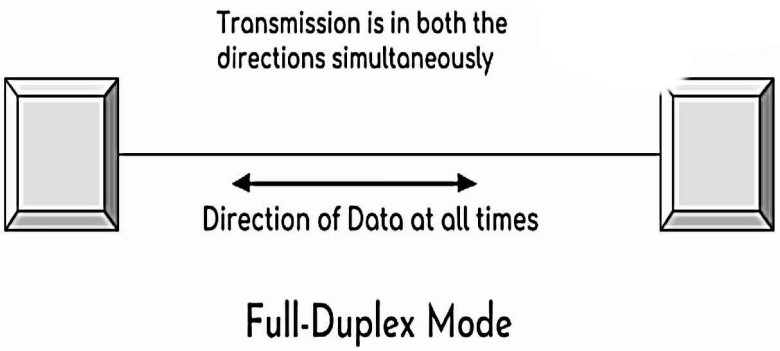
half duplex mode transmission as they send message and then say over and then the person on other hand send his message and this way they communicate but not simultaneously like we used to do on mobile.

Advantages of Half-Duplex mode:
Both devices can send and receive data.
Whole bandwidth can be utilized as at a time only one signal transmits.

Disadvantages of Half-Duplex mode:
The disadvantage in half duplex mode is that the other device cannot send data until it receives the data which is already in transmission, this can cause delays to the communication.

Full Duplex Mode

1. In full duplex mode both the connected devices can send and receive data simultaneously. The mobile phone we use is an example of full duplex mode where we can communicate simultaneously.
2. Both the devices can send and receive the data at the same time.



Full-Duplex Mode

Advantages of Full Duplex mode:
No delays in communication as both can send and receive data simultaneously.

Disadvantages of Full Duplex mode:
No proper bandwidth utilization as the same line is used for sending and receiving data at the same time.

Computer Network Models

A simple transmission of data consists several steps at various layers of computer network. In computer network models we will discuss the models in detail to **understand how the data is actually transferred and received at a computer level**.

Let's have a basic idea of layers involved in data communication.

Layers of a computer network models

1. The main purpose of having several layers in a computer network model is to divide a process of sending and receiving data into small small tasks.

2. These layers are connected with each other, each layer provide certain data to its immediate higher and immediate lower layer and receives certain data from the same.

3. Dividing a model is layers makes the structure quite simple that makes it easy to identify the issue if it occurs. There are three main components of a computer network model. Sender, receiver and carrier.

At sender Side:

Higher layer: Higher layer serves the middle layer, directs the message (or data) to middle layer
Middle layer: Middle layer picks up the data from higher layer and transfer it to the lower layer
lower layer: The data is transmitted to the lower layer of the receiver side.

At receiver Side:

lower layer: Receives the data from the lower layer of sender side and transfer it to middle layer.
Middle layer: Middle layer picks up the data from lower layer and transfer to higher layer.
Higher layer: Higher layer transfers the data to the receiver.
4. We will discuss more than one computer models here, each model has different set and design of layers.

The most important computer network models are:
1. OSI Model
2. TCP/IP Model

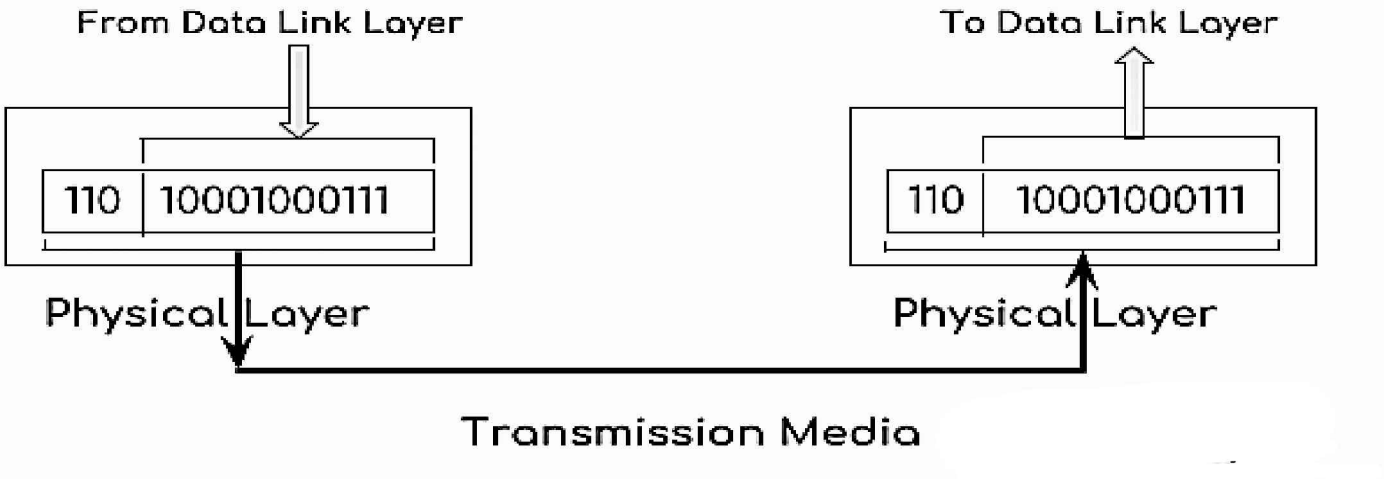
OSI Model in Computer Network

1. **OSI Model** stands for Open System interconnection model.
2. **OSI Model** defines how data is transferred from one computer to another computer.
3. In a very basic scenario two computers connected with a LAN and connectors transfer data using the NIC. This forms a computer network, however if both the system uses different operating systems, for example one system runs on windows and other one runs on MacOS then how can data be transferred between these two different systems, here comes the role of a OSI model which is a seven layered model that defines how a data can be transferred between different systems.

4. **OSI model** was introduced by International Organisation for standardisation (ISO) in 1984.
5. There are **seven layers** in a OSI model

- Application layer
- Presentation Layer
- Session layer
- Transport layer
- Network Layer
- DataLink layer
- Physical layer

Physical Layer



Transport layer converts the data into segments, network layer converts the segments into packets and data link layer converts the packets into frames. A frame is nothing but a sequence of bits such as 1001011.
Physical layer converts these binary sequences into signals and transfer it through a transmission media such as cables etc.

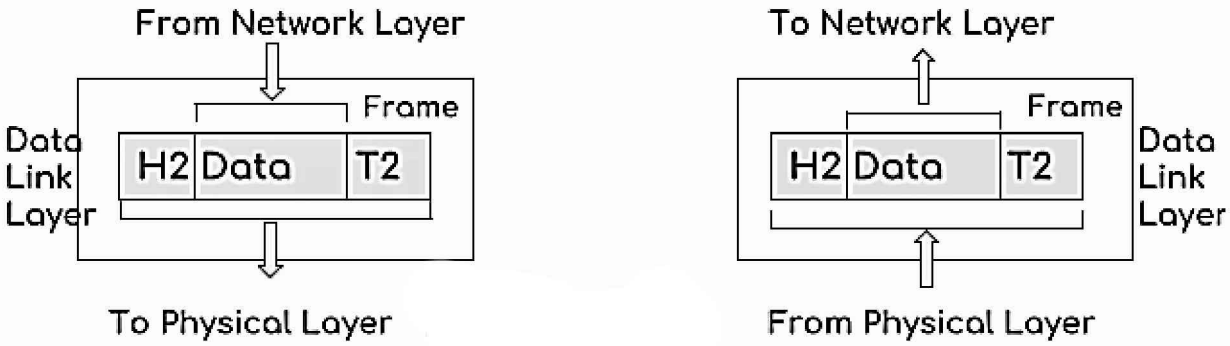
The signals generated by physical layer is based on the transmission media. For example an electrical signal is generated if the media is copper cable, light signal if media is optical fibre and radio signal in case of transmission media is air. This generated signal is received by the physical layer at the receiver side and converts it into bits.

Main functions of Physical Layer:

Digital Transmission:
One of the main functions of physical layer is to transfer data in form of signals. A data can be either analog or digital. To transfer the data over a transmission media such as wire, cable etc. physical layer must need to convert the data to its digital signal.

Digital data to Digital signal conversion:
It uses two techniques to do this conversion: Line coding and block coding.

Data Link Layer



Data link layer receives the data from network layer.

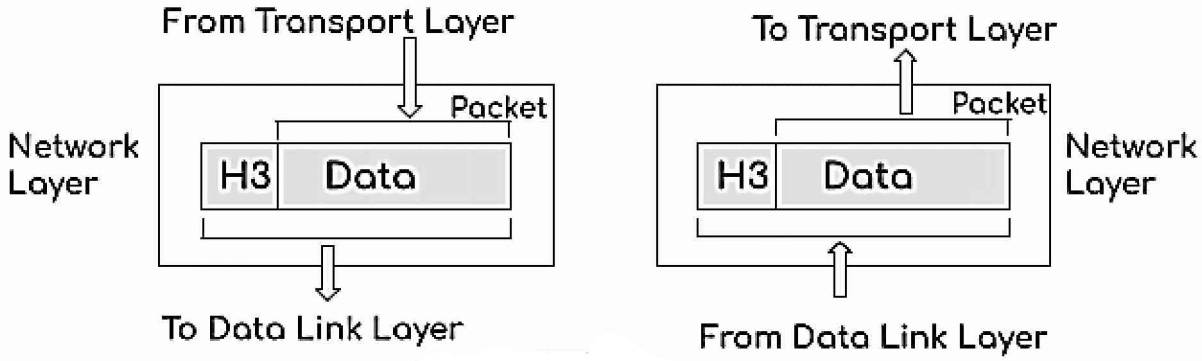
There are two types of addressing done to the packets transfers from one computer to another computer.
Logical addressing: Logical addressing is assigning sender and receiver IP addresses to data packets. This is done at the network layer.

Physical addressing: Physical addressing is done at data link layer where MAC addresses of sender and receiver are assigned to each data packets.

Data unit in the data link layer is called frame. A frame is transferred from one computer to another computer and transmission is done through a transmission media such as wire, cable etc. Both sender and receiver computer has NIC that helps in sending and receiving frame. These NICs presents at sender and receiver provides a physical link between sender and receiver.

Main functions of data link layer:
Access the Media: Allows upper layers of OSI model to use the media using a technique called framing
Media Access control: How data is placed and received from the media.
Error Detection: Tail of the each frame transferred contains certain bits to check whether the data received on the side is corrupted or not.

Network layer



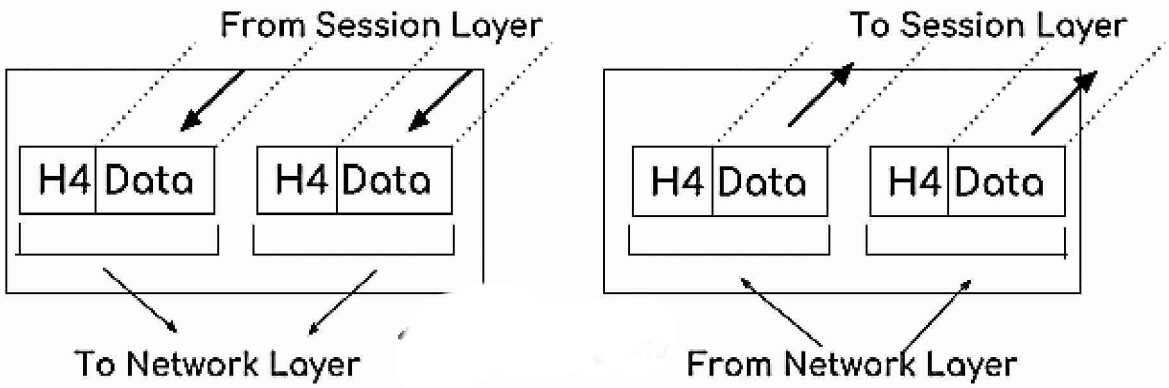
The main purpose of network layer is to receive the data segments from transport layer and transfer them from one computer to another computer on different network.

The main functions of network layer:
Logical Addressing: Every computer on a network has a unique IP address. Network layer assigns the sender and receiver IP address to the data packets before transmitting them so that the data packet reach the correct destination.

Routing: It is a method of transferring data packets from source to destination. It uses the combination of Mask and IP address to transfer the data to correct destination. Each data packets contains three addition components mask, sender IP, receiver IP. The Mask determines the computer network to which the data needs to be delivered and then the IP address determines which computer on that particular network needs to receive the data packet.

Path determination: A computer can be connected to another computer in number of ways. Network layer determines the optimal path for data transmission so that the data can be transmitted faster to the receiver. OSPF, BGP, IS-IS protocols are used to determine best possible path for data delivery.

Transport layer



The main role of transport layer is to check the reliability of data communication.

The main functions of transport layer are:
Segmentation: Data received from session layer is divided into small data units called segments. Each segment contains the sender and receiver port number along with the sequence number. Port number helps to direct the data segments to the correct application and the sequence number helps to reassemble the data from data segments in correct order.

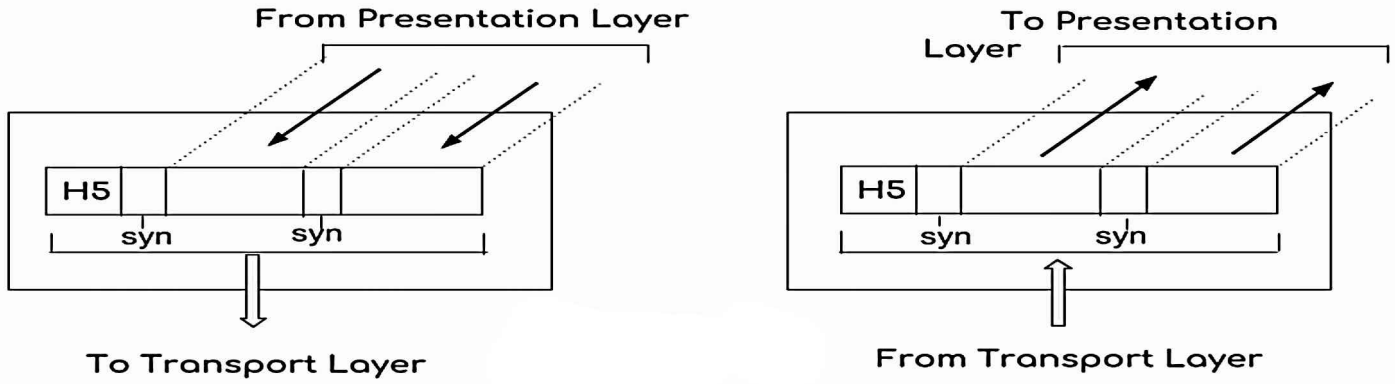
Flow control: It controls the flow of data. It checks the capability of the receiver device receiving capability before transmitting data. For example a sender server can send the data at a rate of 200Mbps but a receiving data can only receive data at a rate of 10 Mbps then it controls the flow of data to 10Mbps so that the data doesn't get lost during transmission.

Error control: Transport layer also performs error control using Automatic Repeat Request, if a data is lost during transmission, it is send again using automatic repeat request. Transport layer also adds a group of bits called checksum with each segment to check whether the data received at receiver side is not corrupt.

Connection oriented transmission: Connection oriented transmission is done using transmission control protocol (TCP). TCP is considerably slower than UDP because it provides the feedback that the data is received or not, thus a data can be sent again if it is not received.

Connectionless transmission: Connectionless transmission is done using User Datagram protocol (UDP). UDP is faster than TCP because it doesn't provide the feedback that the data is actually received at the receiver side or not.

Session Layer



The main role of session layer is to setup and maintain the connection between different systems.

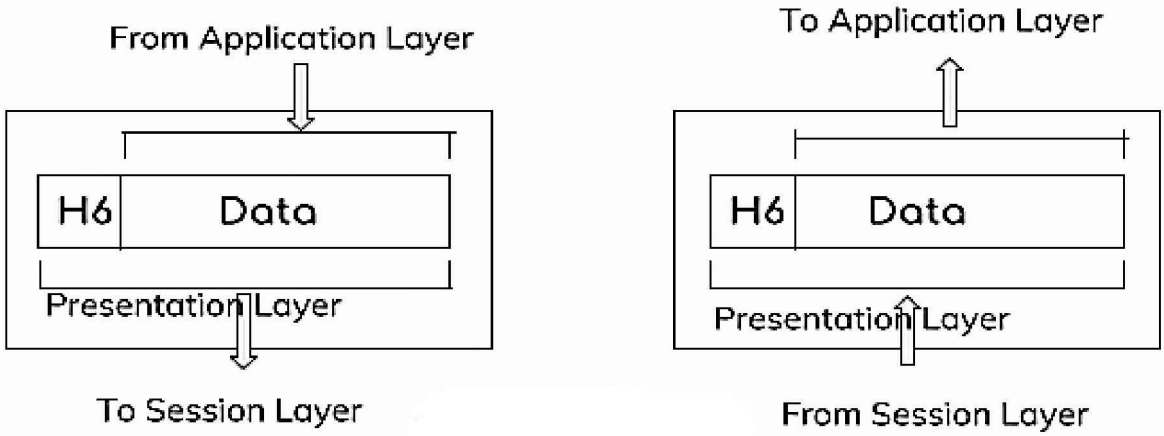
Main functions of session layer:
Authentication: Before a computer can be connected to a server, the computer has to provide

user name and password for the authentication. The function of authentication and setting up a connection after authentication is performed by session layer.

Authorization: Once a connection is established, session layer checks whether the connected computer is authorized to access the data, this function of authorization checking is also performed by session layer.

Session management: Session layer also checks that the data which is received from the server in form of data packets belongs to which application for example when you access Facebook profile through your browser, the data transferred from the Facebook server is transferred to your web browser application, thus the session layer helps in session management.

Presentation Layer



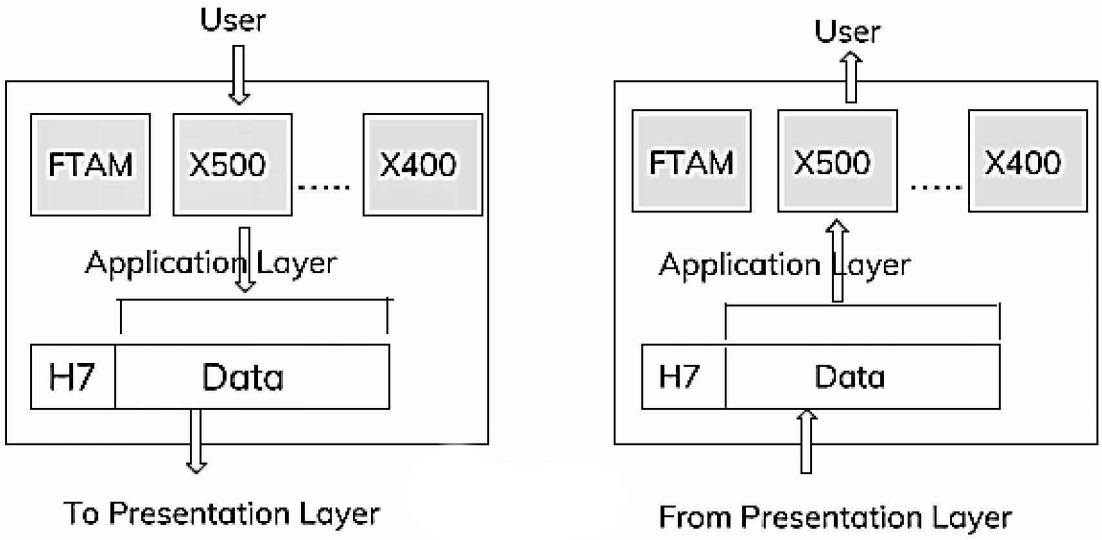
Presentation layer receives the data from top most layer which is application layer.

Functions of Presentation layer:
Translation: The data received from application layer is in form of characters and numbers such as 1234, ERFF etc. The presentation layer converts these characters and numbers into machine understandable format which is known as binary format for example 100111101.

Encryption: To protect the sensitivity of data, presentation layer encrypts the data at the sender side before the transmission and the receiver side this data is decrypted by the presentation layer at the receiver side. Secure sockets layer protocol (SSL) is used by the presentation layer for encryption and decryption.

Compression: Compress the data to small size so that it can be transferred faster over a network. This compression can be lossy or lossless compression.

Application layer



1. Application layer is used by computer applications such as google chrome, outlook, FireFox, Skype etc.
2. Application layer defines the protocols that are used by computer applications for example: HTTP and HTTPS protocols are used by web browsers such as google chrome, FireFox, Safari etc.

FTP protocol is used for file transfer between two or more computers.

SMTP protocol is used for emails

Telnet is used for virtual terminals.

There are dozens of other protocol that forms the application layer, such as NFS, FMTP, DHCP, SNMP, POP3, IRC, NNTP etc.

3. In short you can say that application layer provides the services to computer applications with the help of protocols that are defined in it.

Computer Network TCP/IP model

The TCP/IP Model is developed before than OSI Model. The layers in TCP/IP Model are different than OSI Model.

Layers in TCP/IP Model

The TCP/IP Model has four layers:
1. Physical Layer and data link layer – combined known as host-to-network layer
2. Network layer
3. Transport
4. Application

1. Physical and Data Link Layer

Physical and Data Link Layers in TCP/IP model does not define any protocols, they support all the standard protocols. They are combined known as **host-to-network layer**. A network in TCP/IP internetwork can be LAN or WAN.

2. Network Layer

In the network layer, the TCP/IP model supports internetworking protocol in short known as IP. The IP uses four protocols internally: ARP, RARP, ICMP & IGMP.

Internetworking protocol(IP):

1. It is an unreliable connectionless protocol used by TCP/IP Model.
2. This protocol is used for data transmission.
3. This protocol doesn't do error checking or tracking of data, thus we cannot be sure that the data is actually reached its destination. This is why it is also known as best effort delivery service which means this protocol tries it best to send the data to its destination but doesn't take an guarantee.
4. IP protocol transmits the data in form of small packets known as datagrams. Each of these datagrams are transmitted separately, thus they can take different routes and sometime duplicate datagrams can be reached to destination, also they are reached in no particular order at the destination.

Lets discuss the **four protocol** this Internetworking protocol(IP) uses:

Address Resolution Protocol (ARP)

ARP finds the physical address by using the IP address. In a network, each device is known as physical address usually imprinted on Network interface card (NIC).

ARP protocol is used to find the physical address of a device whose internet address (IP address) is known.

Reverse Address Resolution Protocol (RARP)

RARP protocol helps to find the internet address of a device whose physical address is known.

Internet Control Message Protocol (ICMP)

IP in network layer sends data in form of small packets known as datagrams. ICMP protocol sends the datagrams problems back to sender. It is used for query and error reporting messages.

Internet Group Message Protocol (IGMP)

This protocol is used for simultaneous transmission of a message to a group of recipients.

3. Transport Layer

Transport layer in TCP/Model can be represented by three protocols: Transmission control protocol (TCP), User data gram protocol (UDP) and Stream Control Transmission Protocol (SCTP).

These three protocols in transport layer are responsible for delivery of messages from one process to another. The SCTP protocol was later introduced to meet the needs of newer applications.

User Datagram protocol (UDP)

1. UDP is a process to process protocol used for data transmission.

2. It takes the data from upper layer of TCP/IP Model and adds following information to the data:
a) **Port Address** – Source port address of 16 bits and destination port address of 16 bits added to the data so that it reaches to correct destination and displays the correct source of data.
b) **checksum error control** – 16 bits of checksum data is added to the data received from upper layer, this is used for error control.
c) **length of data** – Length defines the total bytes of data in datagram.

3. Although this protocol finds the error in the transmission of data, it doesn't specify the error which makes it hard to identify the actual error in transmission.

Transmission control protocol (TCP)

1. Unlike UDP which is a connectionless protocol, the TCP is a connection oriented protocol.

2. A connection must be made between sender and receiver before the transmission of data.

3. TCP protocol divides the data in small units called **segments**. Each segment contains the sequence number which makes it possible to rearrange the segments in correct order at the receiver side to make the complete data.

4. It also adds acknowledgement number to the segments to verify that the data is actually reached its destination or not.

5. Unlike UDP which is unable to specify the exact error in transmission, this protocol does error control and specifies the exact error which makes TCP a reliable protocol.

Stream Control Transmission Protocol (SCTP)

1. This protocol combines the best features of TCP and UDP protocols.

2. It was discovered later to support newer applications such as voice data transmission over the internet.

4. Application Layer

1. This is the top most layer of TCP/IP model.

2. It is used for interaction between user and application.

3. There are several protocols used by the application layer for user interaction such as: HTTP, SNMP, SMTP, DNS, TELNET, FTP etc.

HTTP: HTTP stands for **Hypertext transfer protocol**, it allows the user to interact with world wide web through the browser application. HTTP can be used to transfer various types of data such as plain text, audio, video etc.

FTP: FTP stands for **File Transfer Protocol**. This protocol is used for transmitting files from one system to another system.

TELNET: TELNET is a client-server protocol. It is a reliable connection oriented protocol. This protocol is used on internet or on LAN to provide a bidirectional (both ways) text based communication through a virtual terminal connection.

DNS: DNS stands for Domain Name System. Each computer on a network has different IP address, a computer is known by its IP address. DNS provides a mapping to a name to the IP Address so a name can be used to identify a system on network rather than IP address itself.

SNMP: SNMP stands for Simple Network Management Protocol. It managers the devices connected to the internet using TCP/IP protocol.

SMTP: SMTP stands for Simple mail transfer protocol. It is used for email services, using this protocol a email containing data can be sent to another email address.