RIZVI COLLEGE OF ENGINEERING

Department Of Computer Engineering

Subject : Computer Network (CSC503)

Semester V (R-2019)

By Prof. Mohammed Juned

Module No : 1	Introduction to Networking	4Hrs
1.1 1.2	Introduction to computer network, network application, Network software and hardware components (Interconnection networking devices),Network topology, protocol hierarchies, design issues for the layers, connection oriented and connectionless services Reference models: Layer details of OSI, TCP/IP models. Communication between layers.	

Course Outcome Covered : CO1 : Demonstrate the concepts of data communication at physical layer and compare ISO - OSI model with TCP/IP model.

- Books to be referred :
- B.A. Forouzan, Data Communications and Networking, 5th edition, TMH

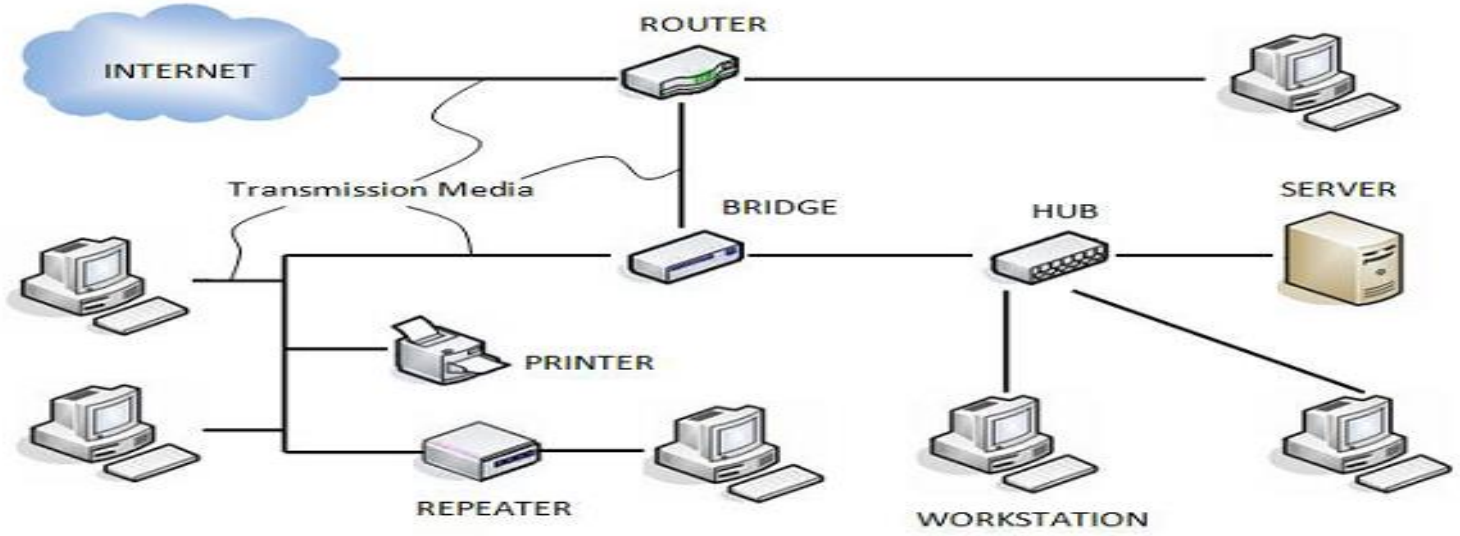
Introduction to computer network :

- A **computer network** is a system that connects numerous independent computers in order to share information (data) and resources. The integration of computers and other different devices allows users to communicate more easily.

Network application:

- A network application is **any application running on one host providing communication to another application running on a different host**.
- Network applications allow network operators to easily manage and monitor network traffic as well as analyze data that can be used to improve network systems.

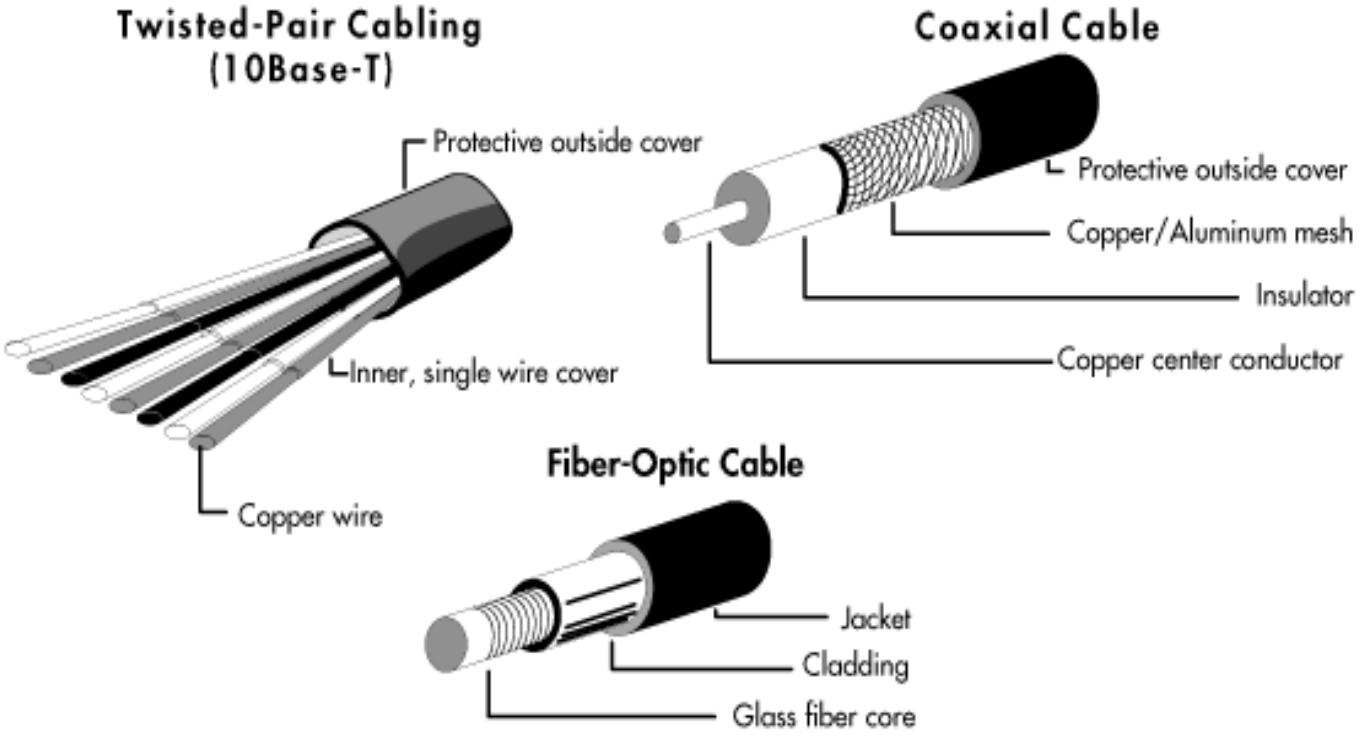
- **Network software and hardware components (Interconnection networking devices)**

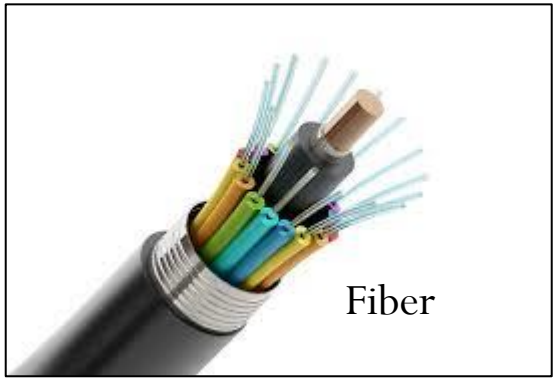


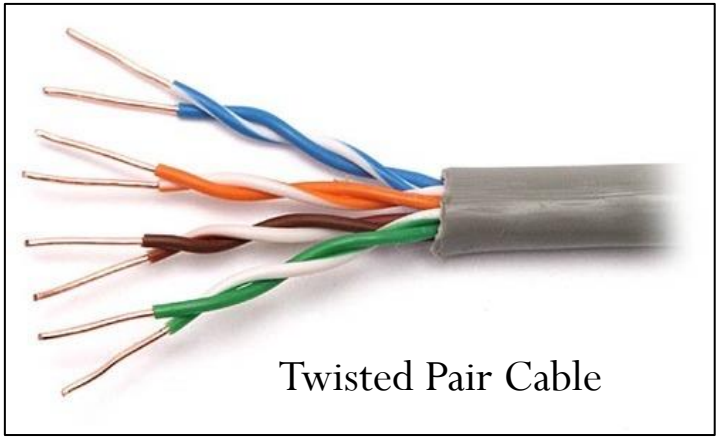
COMPUTER NETWORK COMPONENTS

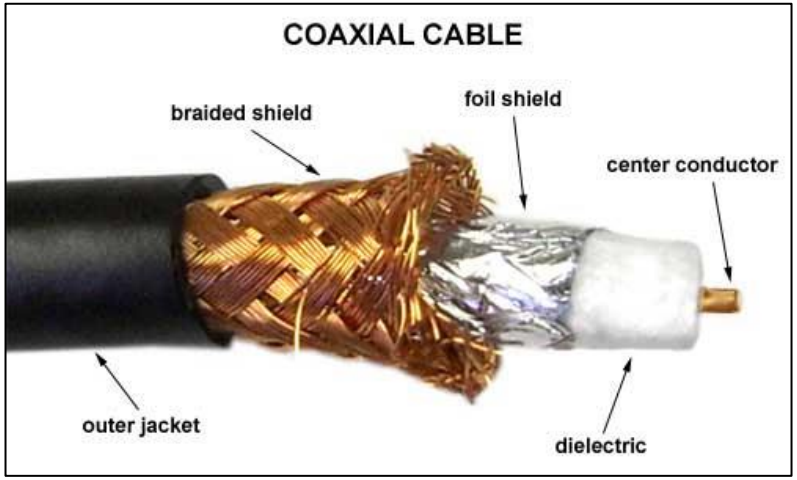
- **Network software and hardware components :**
- **Hardware Components**
- **Servers** –
- high-configuration computers that manage the resources of the network.
- N/W OS is typically installed in the server and so they give user accesses to the network resources. **Microsoft Windows Server 2003, Microsoft Windows Server 2008, UNIX etc.**
- Servers can be of various kinds: file servers, database servers, print servers etc.
- **Clients** – Clients are computers that request and receive service from the servers to access and use the network resources.

- **Transmission Media** –
- Transmission media are the channels through which data is transferred from one device to another in a network.
- Transmission media may be guided media like coaxial cable, fibre optic cables etc; or maybe unguided media like microwaves, infra-red waves etc.


Twisted-Pair Cabling
(10Base-T)
Protective outside cover
Inner, single wire cover
Copper wire
Coaxial Cable
Protective outside cover
Copper/Aluminum mesh
Insulator
Copper center conductor
Fiber-Optic Cable
Jacket
Cladding
Glass fiber core


Fiber


Twisted Pair Cable


COAXIAL CABLE
braided shield
foil shield
center conductor
outer jacket
dielectric

- **Connecting Devices** – Connecting devices act as middleware between networks or computers, by binding the network media together. Some of the common connecting devices are:

- Routers
- Bridges
- Hubs
- Repeaters
- Gateways
- Switches

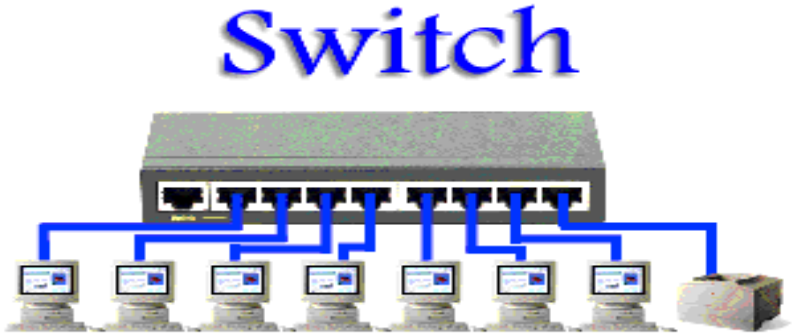
- Interconnection networking devices
- Hub
- Routers
- Switches
- Gateways
- Bridges
- Repeaters

Hub

Hub

- A Hub is a hardware device that divides the network connection among multiple devices. When computer requests for some information from a network, it first sends the request to the Hub through cable.
- Hub will broadcast this request to the entire network.
- All the devices will check whether the request belongs to them or not. If not, the request will be dropped.
- The process used by the Hub consumes more bandwidth and limits the amount of communication. Nowadays, the use of hub is obsolete, and it is replaced by more advanced computer network components such as Switches, Routers.

Switch

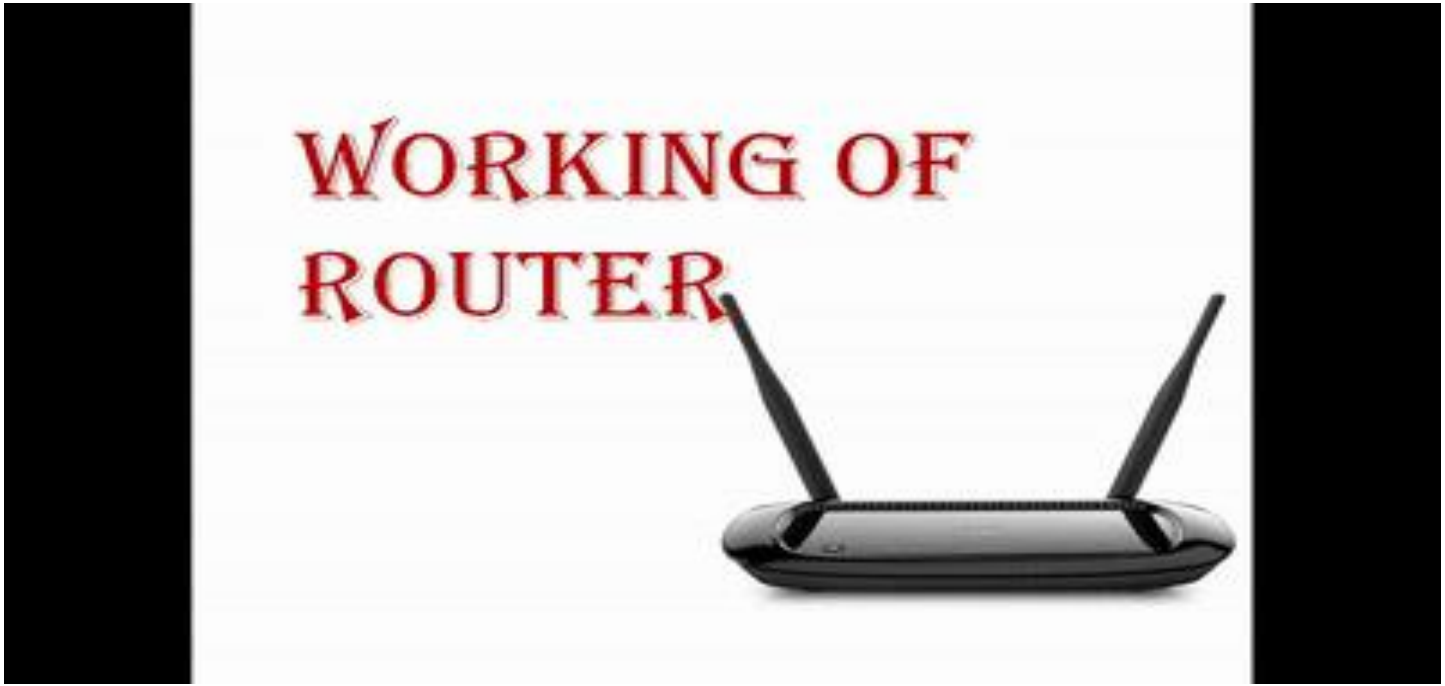


Switch :

- A switch is a hardware device that connects multiple devices on a computer network.
- A Switch contains more advanced features than Hub. The Switch contains the updated table that decides where the data is transmitted or not.
- Switch delivers the message to the correct destination based on the physical address present in the incoming message.
- A Switch does not broadcast the message to the entire network like the Hub. It determines the device to whom the message is to be transmitted.
- Therefore, we can say that switch provides a direct connection between the source and destination. It increases the speed of the network.

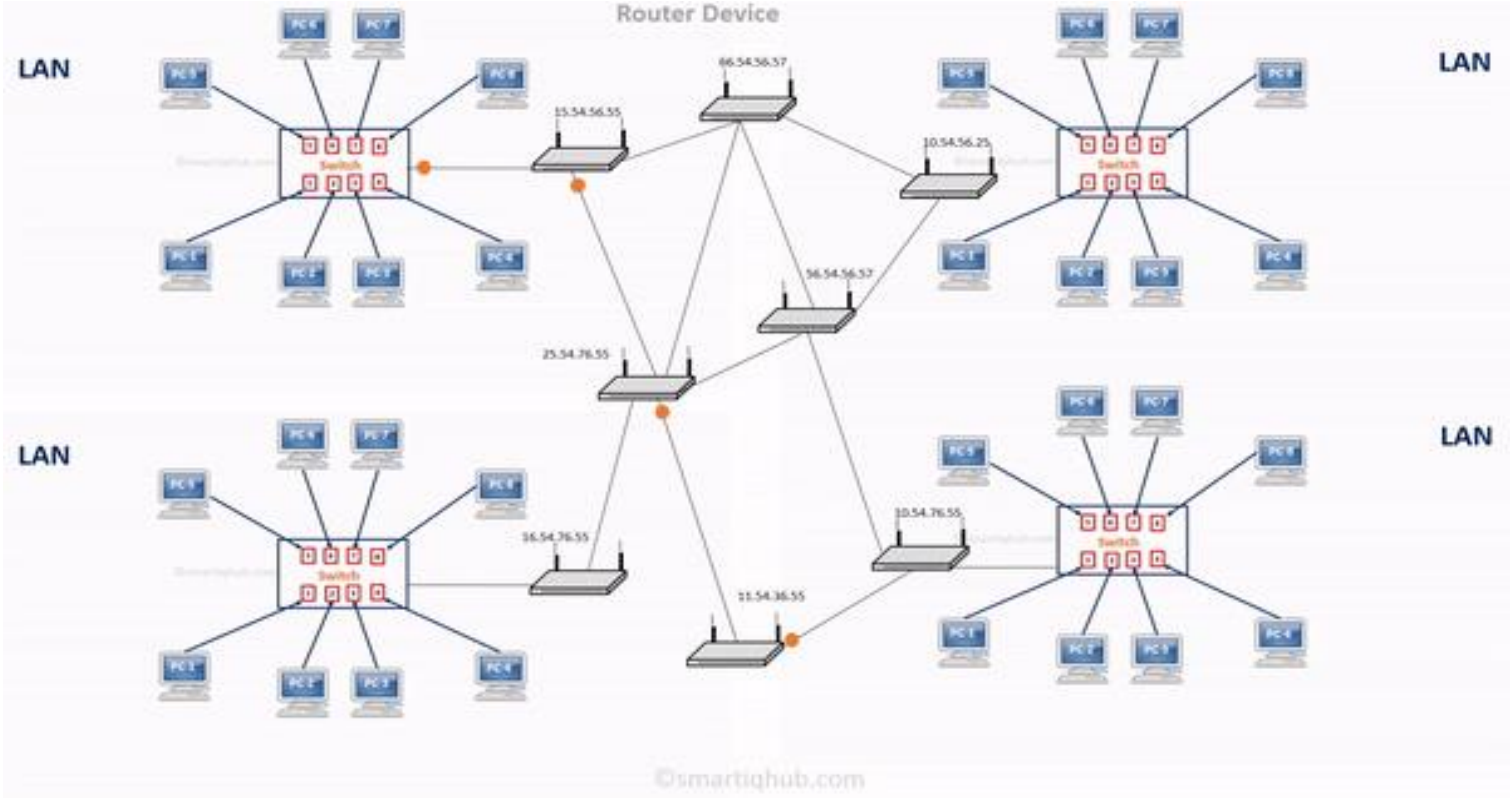

D-Link
D-Link
DES-1018MPV2
PoE
Combo

Router :



Router :

Router :


Router Device
LAN
LAN
LAN
LAN
66.54.56.57
15.54.56.55
10.54.56.25
56.54.56.57
25.54.76.55
16.54.76.55
10.54.76.55
11.54.36.55
Switch
©smartiqhub.com

Router :

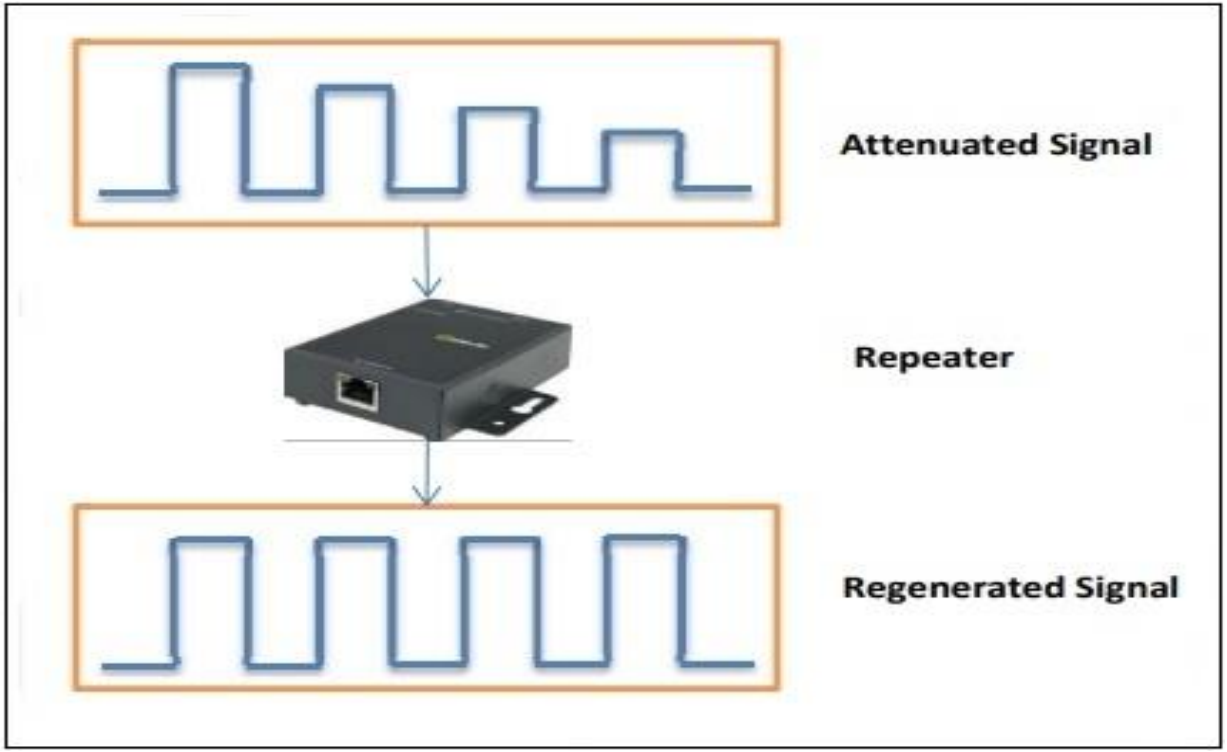
- A router is a hardware device which is used to connect a LAN with an internet connection. It is used to receive, analyses and forward the incoming packets to another network.
- A router works in a **Layer 3 (Network layer)** of the OSI Reference model.
- A router forwards the packet based on the information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

Advantages Of Router:

Security: The information which is transmitted to the network will traverse the entire cable, but the only specified device which has been addressed can read the data.

- **Reliability:** If the server has stopped functioning, the network goes down, but no other networks are affected that are served by the router.
- **Performance:** Router enhances the overall performance of the network. Suppose there are 24 workstations in a network generates a same amount of traffic.
- This increases the traffic load on the network. Router splits the single network into two networks of 12 workstations each, reduces the traffic load by half.
- **Network range**

Repeater :



- **Repeater :**
- Repeaters are network devices operating at physical layer of the OSI model that amplify or regenerate an incoming signal before retransmitting it.
- They are incorporated in networks to expand its coverage area.
- They are also known as signal boosters.

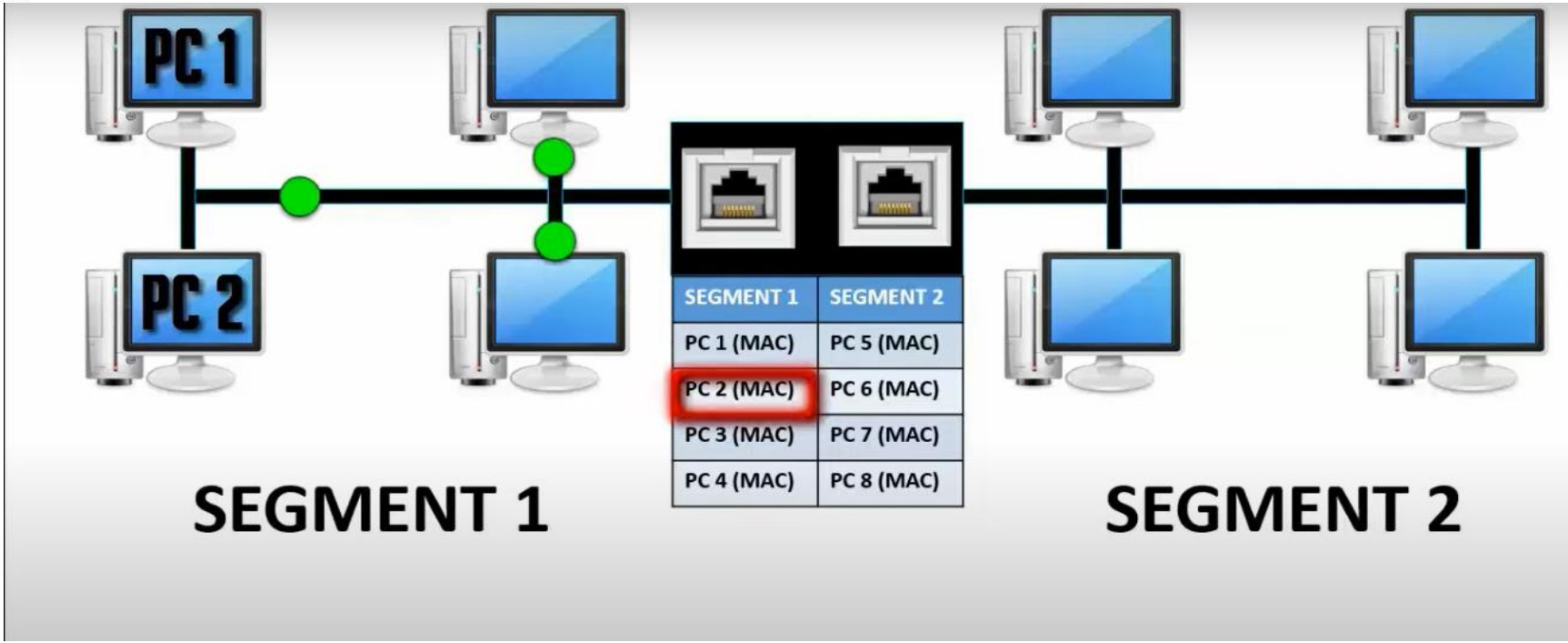
Advantages of Repeaters

- Repeaters are simple to install and can easily extend the length or the coverage area of networks.
- They are cost effective.
- Repeaters don’t require any processing overhead. The only time they need to be investigated is in case of degradation of performance.
- They can connect signals using different types of cables.

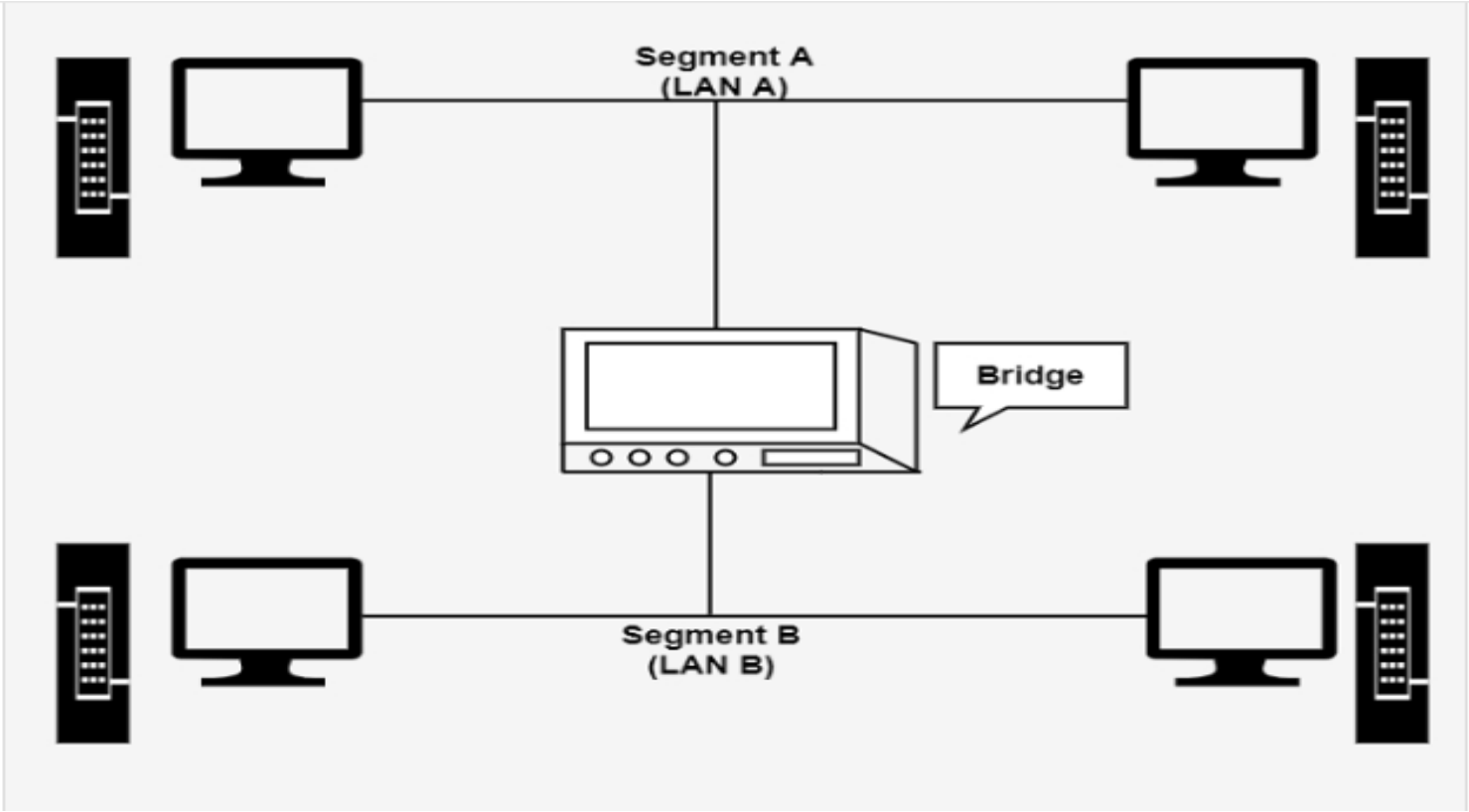
Disadvantages of Repeaters

- Repeaters cannot connect dissimilar networks.
- They cannot differentiate between actual signal and noise.
- They cannot reduce network traffic or congestion.
- Most networks have limitations upon the number of repeaters that can be deployed.

Bridges :


PC 1
PC 2
SEGMENT 1
SEGMENT 2
PC 1 (MAC)
PC 2 (MAC)
PC 3 (MAC)
PC 4 (MAC)
PC 5 (MAC)
PC 6 (MAC)
PC 7 (MAC)
PC 8 (MAC)
SEGMENT 1
SEGMENT 2

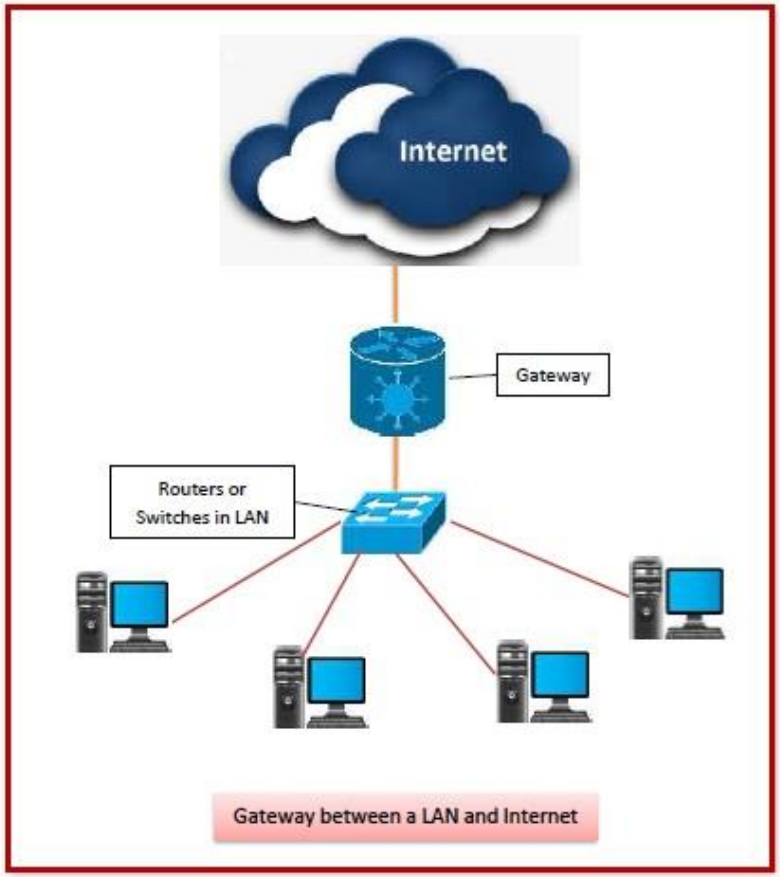
Bridges :


Segment A
(LAN A)
Bridge
Segment B
(LAN B)

- Bridges connects two or more different LANs that has a similar protocol and provides communication between the devices (nodes) in them.
- By joining multiple LANs, bridges help in multiplying the network capacity of a single LAN.
- **A bridge performs in the following aspect –**
- A bridge receives all the packets or frame from both LAN (segment) A and B.
- A bridge builds a table of addresses from which it can identify that the packets are sent from which LAN (or segment) to which LAN.
- The bridge reads the send and discards all packets from LAN A sent to a computer on LAN A and that packets from LAN A send to a computer on LAN B are retransmitted to LAN B.
- The packets from LAN B are considered in the same method.

- **Uses of Bridges**
- The main uses of bridges are –
- Bridges are used to divide large busy networks into multiple smaller and interconnected networks to improve performance.
- Bridges also can increase the physical size of a network.
- Bridges are also used to connect a LAN segment through a synchronous modem relation to another LAN segment at a remote area.

- **Gateways :**
- A gateway is a network node that forms a passage between two networks operating with different transmission protocols.
- A gateway is a hardware device that goes about as a “gate” between two networks. It very well might be a server, firewall, router, or another device that empowers traffic to stream all through the network.
- Gateways serve as an exit and entry point for a network as all data should go through or communication gateway before being routed.


Internet
Gateway
Routers or
Switches in LAN
Gateway between a LAN and Internet


1
2
3
4
5
6
7
8
PWR

- **Features of Gateways**
- Gateway is located at the boundary of a network and manages all data that inflows or outflows from that network.
- It forms a passage between two different networks operating with different transmission protocols.
- A gateway operates as a protocol converter, providing compatibility between the different protocols used in the two different networks.

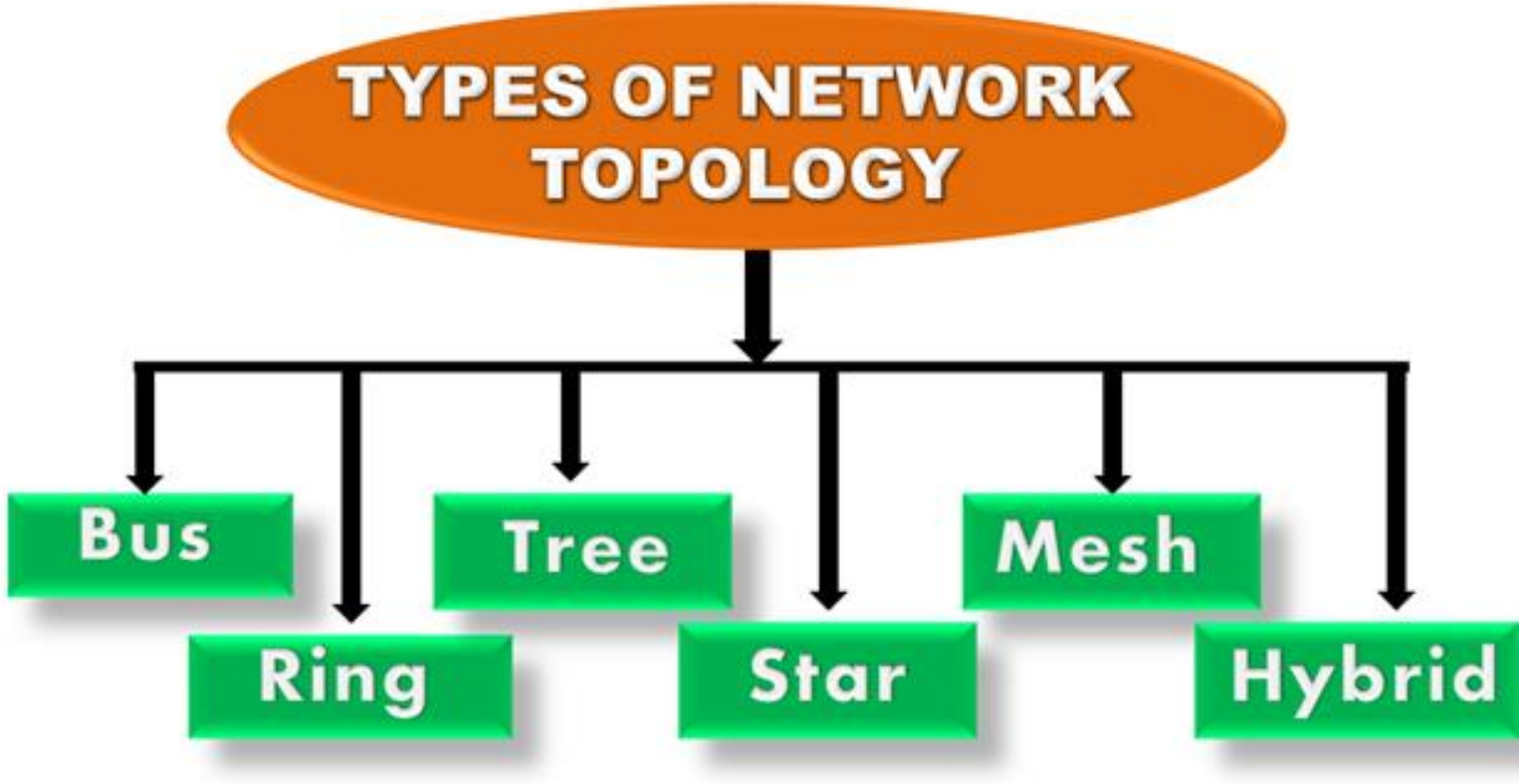
- **Types of Gateways**
- On basis of direction of data flow, gateways are broadly divided into two categories –
- **Unidirectional Gateways** – They allow data to flow in only one direction.
- **Bidirectional Gateways** – They allow data to flow in both directions. They can be used as synchronization tools.

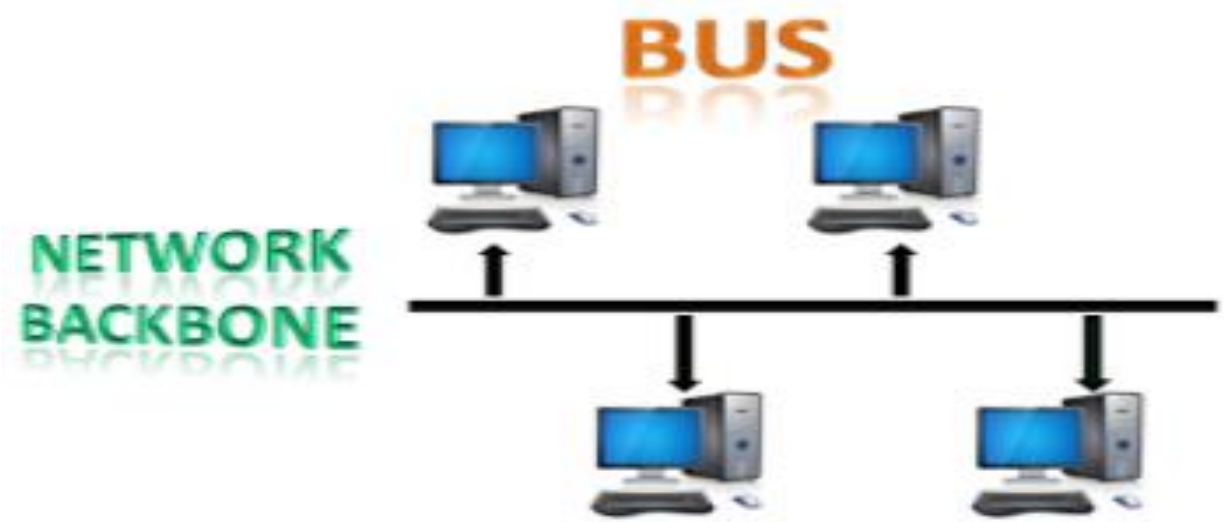
Network Topology :

- The arrangement of a network that comprises nodes and connecting lines via sender and receiver is referred to as network topology :
- Some of the factors that affect choice of topology for a network are :
- **Cost** – Installation cost is a very important factor in overall cost of setting up an infrastructure. Therefore, cable lengths, distance between nodes, location of servers, etc. must be considered when designing a network.
- **Flexibility** – Topology of a network should be flexible enough to allow reconfiguration of office set up, addition of new nodes and relocation of existing nodes.

Network Topology :

- **Reliability** – Network should be designed in such a way that it has minimum down time. Failure of one node or a segment of cabling should not render the whole network useless.
- **Scalability** – Network topology should be scalable, i.e., it can accommodate load of new devices and nodes without perceptible drop in performance.
- **Ease of installation** – Network should be easy to install in terms of hardware, software and technical personnel requirements.
- **Ease of maintenance** – Troubleshooting and maintenance of network should be easy.


TYPES OF NETWORK TOPOLOGY
Bus
Ring
Tree
Star
Mesh
Hybrid


BUS
NETWORK
BACKBONE

- The bus topology is designed in such a way that all the stations are connected through a single cable known as a backbone cable.
- Each node is either connected to the backbone cable by drop cable or directly connected to the backbone cable.
- When a node wants to send a message over the network, it puts a message over the network. All the stations available in the network will receive the message whether it has been addressed or not.
- The backbone cable is considered as a **"single lane"** through which the message is broadcast to all the stations.

- Advantages of Bus topology:
- **Low-cost cable:** In bus topology, nodes are directly connected to the cable without passing through a hub. Therefore, the initial cost of installation is low.
- **Moderate data speeds:** Coaxial or twisted pair cables are mainly used in bus-based networks that support upto 10 Mbps.
- **Familiar technology:** Bus topology is a familiar technology as the installation and troubleshooting techniques are well known, and hardware components are easily available.
- **Limited failure:** A failure in one node will not have any effect on other nodes.

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

Ring Topology :

- Ring topology is like a bus topology, but with connected ends.
- The node that receives the message from the previous computer will retransmit to the next node.
- The data flows in one direction, i.e., it is unidirectional.
- The data flows in a single loop continuously known as an endless loop.
- It has no terminated ends, i.e., each node is connected to other node and having no termination point.
- The data in a ring topology flow in a clockwise direction.

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

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

- **Advantages of Ring topology:**
- **Network Management:** Faulty devices can be removed from the network without bringing the network down.
- **Product availability:** Many hardware and software tools for network operation and monitoring are available.
- **Cost:** Twisted pair cabling is inexpensive and easily available. Therefore, the installation cost is very low.
- **Reliable:** It is a more reliable network because the communication system is not dependent on the single host computer.

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


STAR
CENTRAL
HUB

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

Advantages of Star topology

- **Efficient troubleshooting:** Troubleshooting is quite efficient in a star topology as compared to bus topology.
- In a bus topology, the manager has to inspect the kilometres of cable. In a star topology, all the stations are connected to the centralized network.
- Therefore, the network administrator has to go to the single station to troubleshoot the problem.
- **Network control:** Complex network control features can be easily implemented in the star topology. Any changes made in the star topology are automatically accommodated.
- **Limited failure:** As each station is connected to the central hub with its own cable, therefore failure in one cable will not affect the entire network.

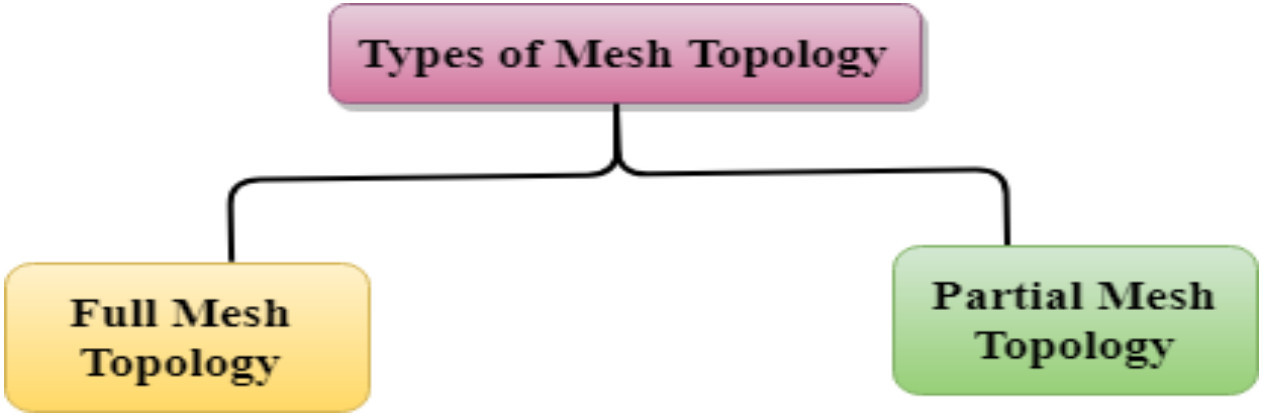
- **Easily expandable:** It is easily expandable as new stations can be added to the open ports on the hub.
- **Cost effective:** Star topology networks are cost-effective as it uses inexpensive coaxial cable.
- **High data speeds:** It supports a bandwidth of approx 100Mbps. Ethernet 100BaseT is one of the most popular Star topology networks.

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


MESH

- **Mesh technology** is an arrangement of the network in which computers are interconnected with each other through various redundant connections.
- There are multiple paths from one computer to another computer.
- It does not contain the switch, hub or any central computer which acts as a central point of communication.
- The Internet is an example of the mesh topology.

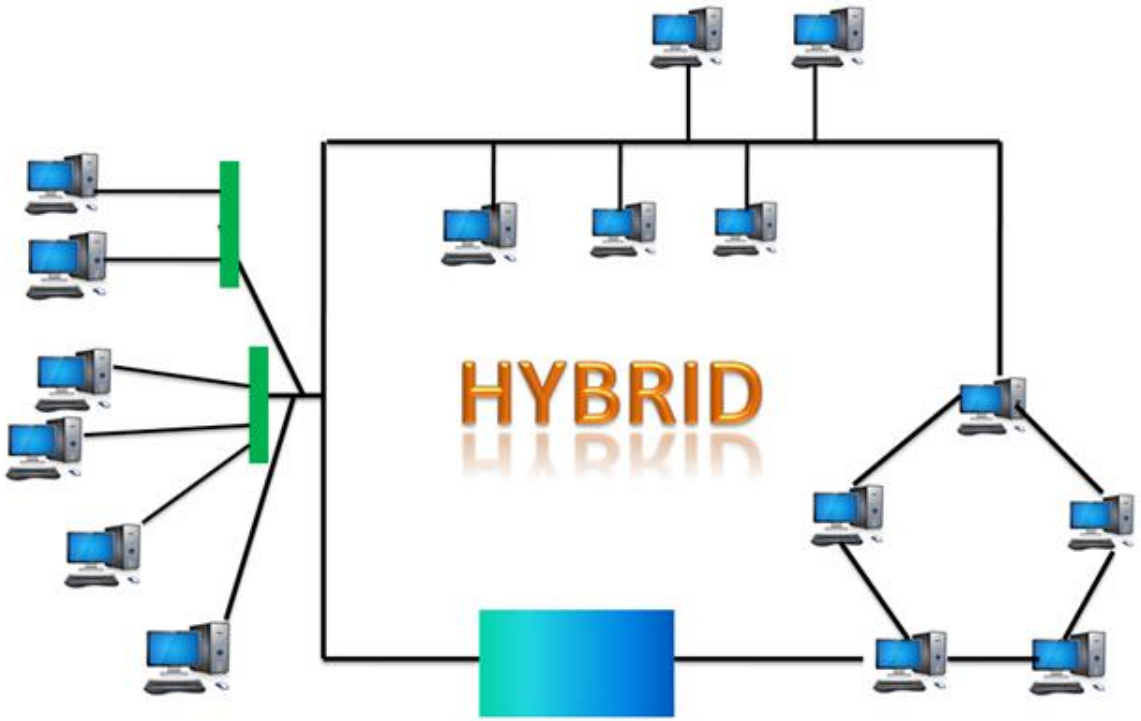
- **Mesh topology is divided into two categories:**
- Fully connected mesh topology
- Partially connected mesh topology



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

- **Advantages of Mesh topology:**
- **Reliable:** The mesh topology networks are very reliable as if any link breakdown will not affect the communication between connected computers.
- **Fast Communication:** Communication is very fast between the nodes.
- **Easier Reconfiguration:** Adding new devices would not disrupt the communication between other devices.

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


HYBRID

- The combination of various topologies is known as **Hybrid topology**.
- A Hybrid topology is a connection between different links and nodes to transfer the data.
- When two or more different topologies are combined is termed as Hybrid topology and if similar topologies relate to each other will not result in Hybrid topology.

- **For example :** If there exist a ring topology in one branch of ICICI bank and bus topology in another branch of ICICI bank, connecting these two topologies will result in Hybrid topology.
- **Advantages of Hybrid Topology**
- **Reliable:** If a fault occurs in any part of the network will not affect the functioning of the rest of the network.
- **Scalable:** Size of the network can be easily expanded by adding new devices without affecting the functionality of the existing network.

- **Flexible:** This topology is very flexible as it can be designed according to the requirements of the organization.
- **Effective:** Hybrid topology is very effective as it can be designed in such a way that the strength of the network is maximized, and weakness of the network is minimized.

- **Disadvantages of Hybrid topology**
- **Complex design:** The major drawback of the Hybrid topology is the design of the Hybrid network. It is very difficult to design the architecture of the Hybrid network.
- **Costly Hub:** The Hubs used in the Hybrid topology are very expensive as these hubs are different from usual Hubs used in other topologies.
- **Costly infrastructure:** The infrastructure cost is very high as a hybrid network requires a lot of cabling, network devices, etc.

Design Issues for the Layers of Computer Networks

- **Reliability :** Network channels and components may be unreliable, resulting in loss of bits while data transfer. So, an important design issue is to make sure that the information transferred is not distorted.
- **Scalability :** Networks are continuously evolving. The sizes are continually increasing leading to congestion.
- Also, when new technologies are applied to the added components, it may lead to incompatibility issues. Hence, the design should be done so that the networks are scalable and can accommodate such additions and alterations.

- **Addressing :** At a particular time, innumerable messages are being transferred between large numbers of computers. So, a naming or addressing system should exist so that each layer can identify the sender and receivers of each message.
- **Error Control :** Unreliable channels introduce several errors in the data streams that are communicated. So, the layers need to agree upon common error detection and error correction methods so as to protect data packets while they are transferred.

- **Flow Control :** If the rate at which data is produced by the sender is higher than the rate at which data is received by the receiver, there are chances of overflowing the receiver. So, a proper flow control mechanism needs to be implemented.
- **Resource Allocation :** Computer networks provide services in the form of network resources to the end users.
- The main design issue is to allocate and deallocate resources to processes.
- The allocation/deallocation should occur so that minimal interference among the hosts occurs and there is optimal usage of the resources.

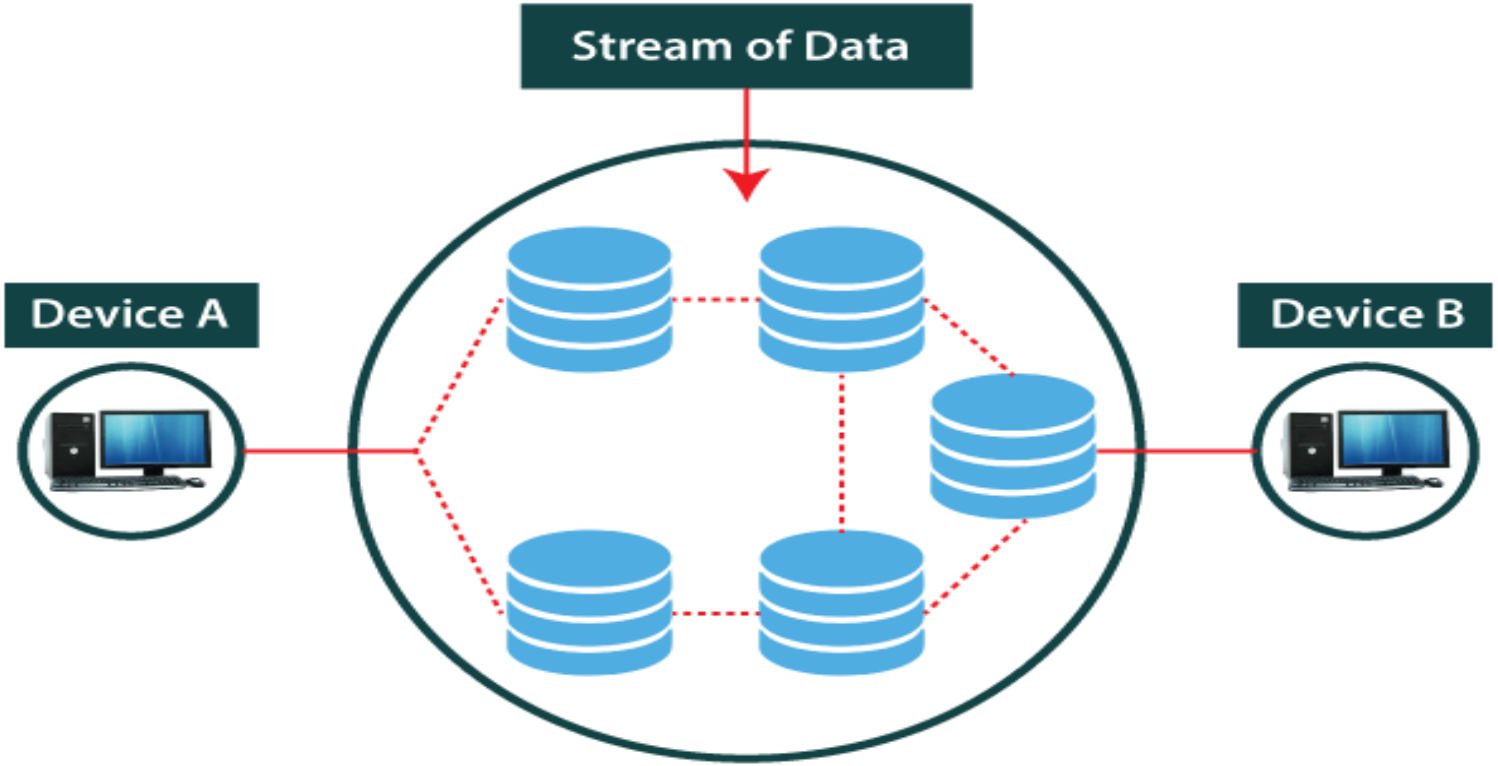
- **Statistical Multiplexing :** It is not feasible to allocate a dedicated path for each message while it is being transferred from the source to the destination.
- So, the data channel needs to be multiplexed, so as to allocate a fraction of the bandwidth or time to each host.
- **Routing :** There may be multiple paths from the source to the destination. Routing involves choosing an optimal path among all possible paths, in terms of cost and time. There are several routing algorithms that are used in network systems.

- **Security :** A major factor of data communication is to defend it against threats like eavesdropping and surreptitious alteration of messages.
- So, there should be adequate mechanisms to prevent unauthorized access to data through authentication and cryptography.

- **Connection oriented and connectionless services :**
- Data communication is a telecommunication network to send and receive data between two or more computers over the same or different network.
- There are two ways to establish a connection before sending data from one device to another, that are **Connection-Oriented** and **Connectionless Service**.
- Connection-oriented service involves the creation and termination of the connection for sending the data between two or more devices. In contrast, connectionless service does not require establishing any connection and termination process for transferring the data over a network.

- **Connection Oriented Service :**
- A connection-oriented service is one that establishes a dedicated connection between the communicating entities before data communication commences.
- It is modelled after the telephone system.
- To use a connection-oriented service, the user first establishes a connection, uses it and then releases it.
- In connection-oriented services, the data streams/packets are delivered to the receiver in the same order in which they have been sent by the sender.

Connection-oriented Communication

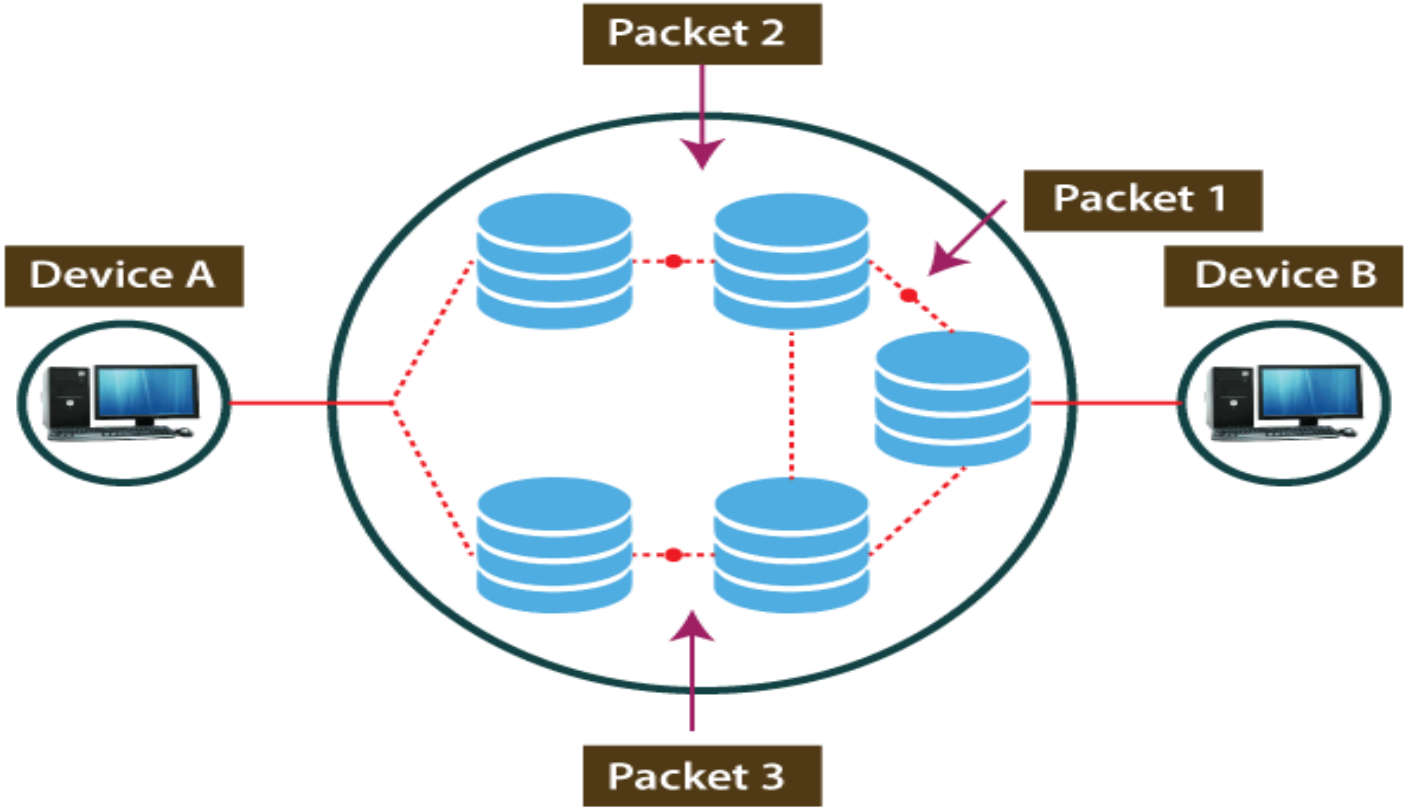


- **Advantages of Connection-Oriented Services**
- This is mostly a reliable connection.
- Congestions are less frequent.
- Sequencing of data packets is guaranteed.
- Suitable for long connection.

- **Disadvantages of Connection-Oriented Services**
- Resource allocation is needed before communication. This often leads to under-utilized network resources.
- The lesser speed of connection due to the time is taken for establishing and relinquishing the connection.
- In the case of router failures or network congestions, there are no alternative ways to continue communication.

- **Connectionless Services :**
- A Connectionless service is a data communication between two nodes where the sender sends data without ensuring whether the receiver is available to receive the data.
- Here, each data packet has the destination address and is routed independently irrespective of the other packets.
- Thus, the data packets may follow different paths to reach the destination.
- There's no need to setup connection before sending a message and relinquish it after the message has been sent. The data packets in a connectionless service are usually called datagrams.

Connectionless Communication



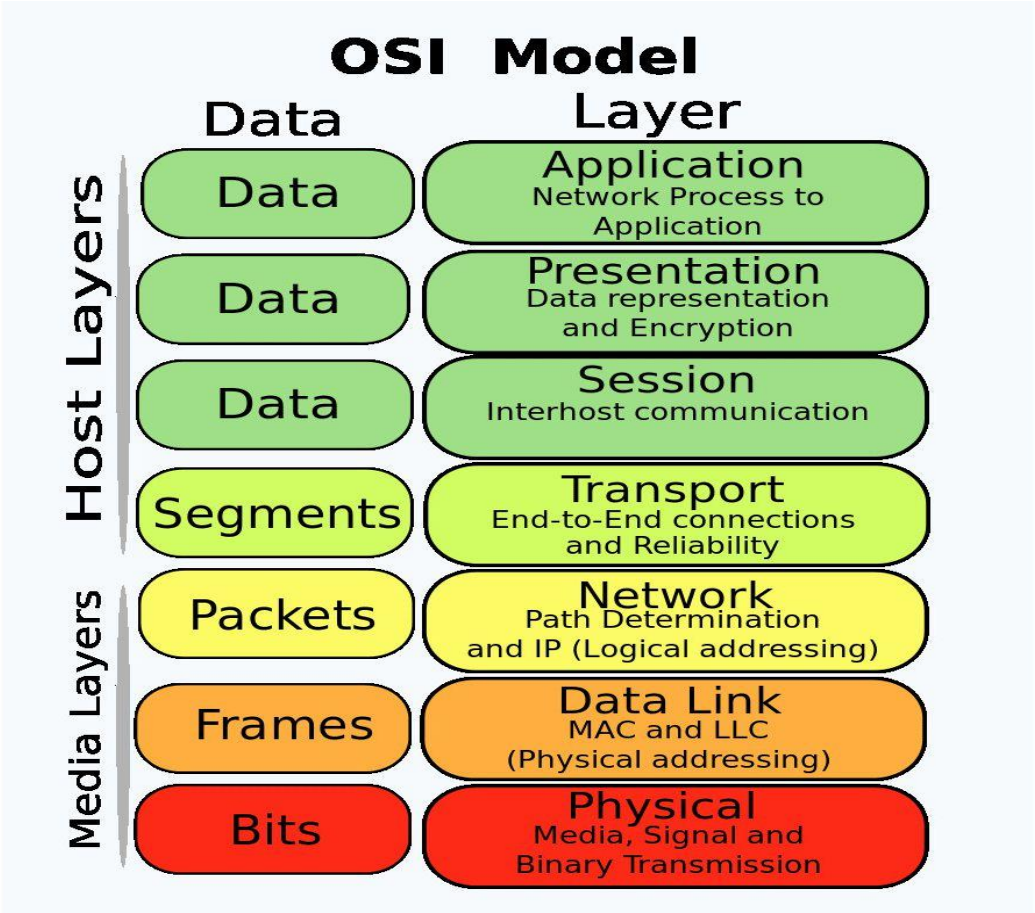
- Protocols for connectionless services are –
- Internet Protocol (IP)
- User Datagram Protocol (UDP)
- Internet Control Message Protocol (ICMP)

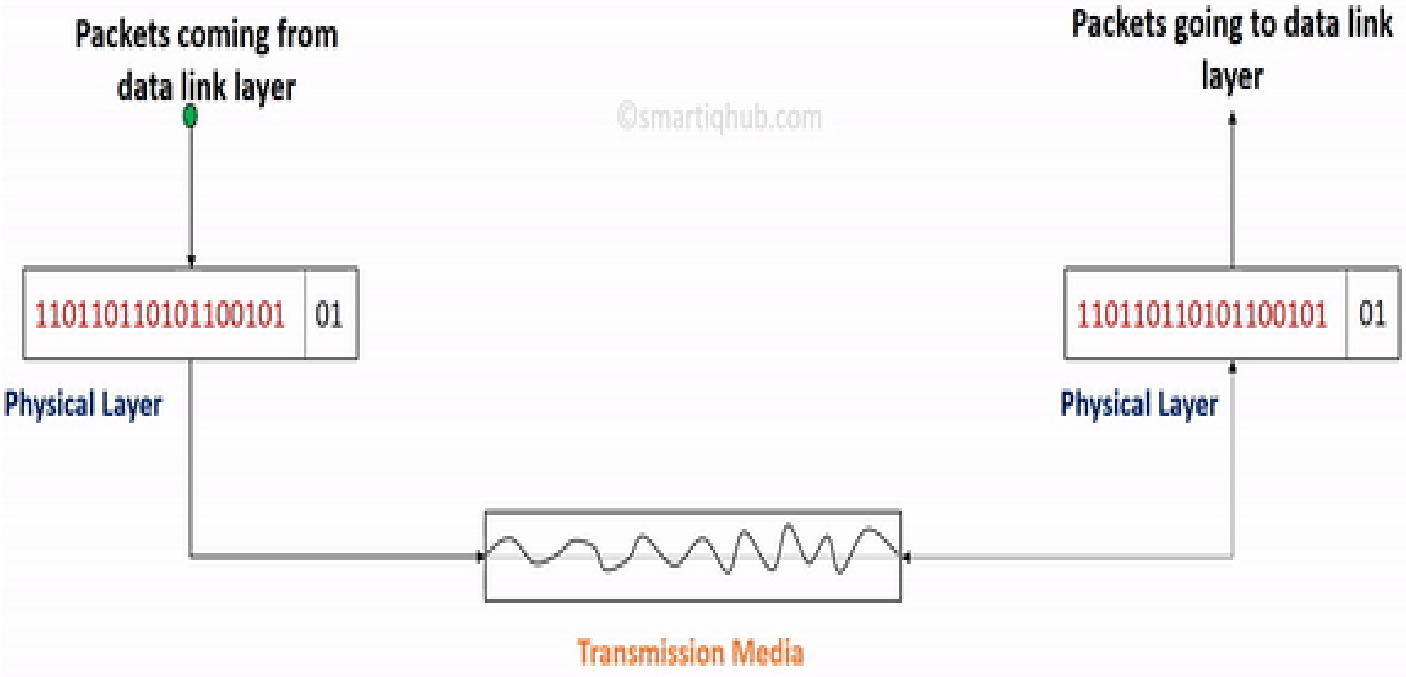
- **Advantages of Connectionless Services**
- It has low overhead.
- It enables to broadcast and multicast messages, where the sender sends messages to multiple recipients.
- It does not require any time for circuit setup.
- In case of router failures or network congestions, the data packets are routed through alternate paths. Hence, communication is not disrupted.

- **Disadvantages of Connectionless Services**
- It is not a reliable connection.
- It does not guarantee that there will not be a loss of packets, wrong delivery, out – of – sequence delivery or duplication of packets.
- Each data packet requires longer data fields since it should hold all the destination address and the routing information.
- They are prone to network congestions.

Reference models: Layer details of OSI

- 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**.
- 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

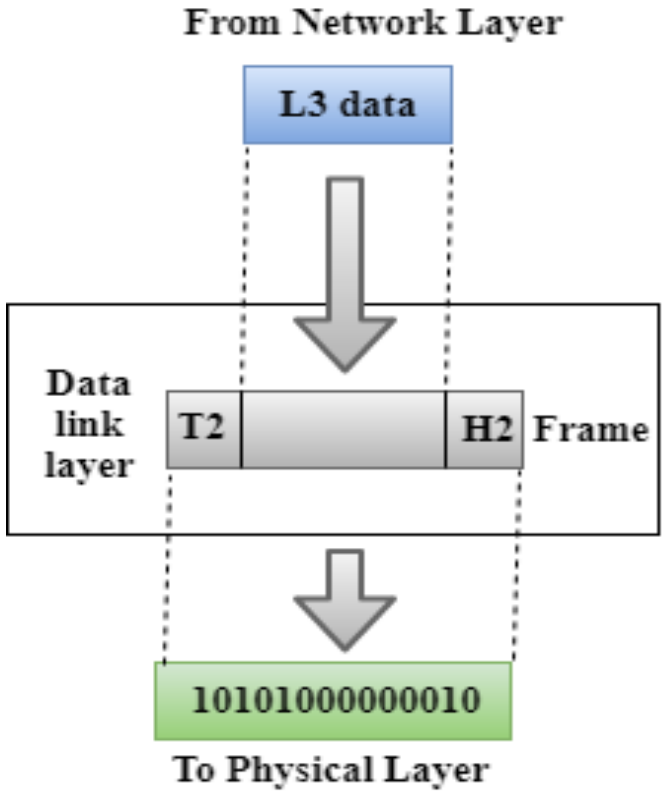

OSI Model
Data
Layer
Host Layers
Media Layers
Data
Application
Network Process to Application
Data
Presentation
Data representation and Encryption
Data
Session
Interhost communication
Segments
Transport
End-to-End connections and Reliability
Packets
Network
Path Determination and IP (Logical addressing)
Frames
Data Link
MAC and LLC (Physical addressing)
Bits
Physical
Media, Signal and Binary Transmission

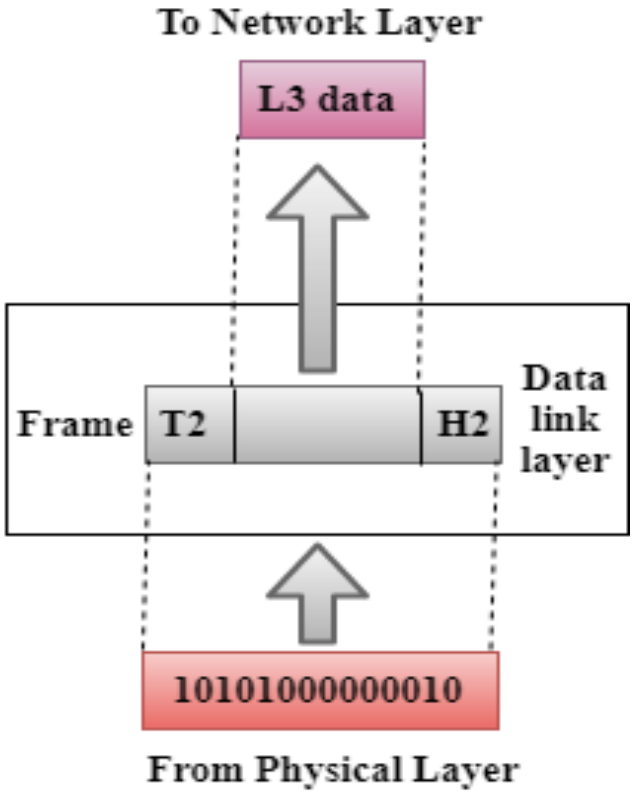

Packets coming from data link layer
©smartiqhub.com
Packets going to data link layer
1101101101011001010 1
1101101101011001010 1
Physical Layer
Physical Layer
Transmission Media

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.


From Network Layer
L3 data
Data link layer
T2
H2
Frame
10101000000010
To Physical Layer

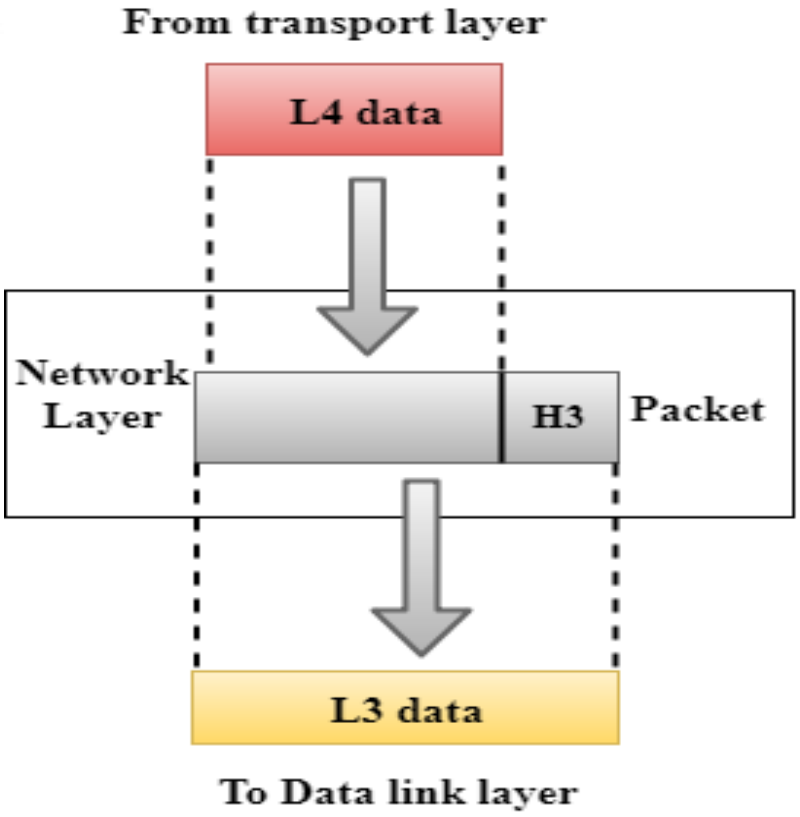

To Network Layer
L3 data
Frame
T2
H2
Data link layer
10101000000010
From Physical Layer

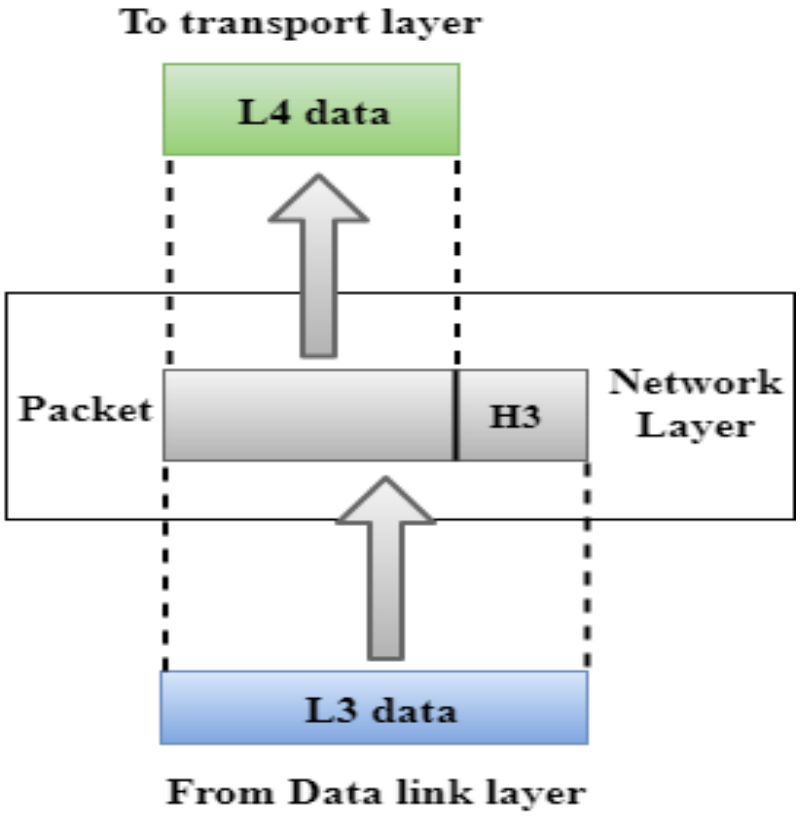
- **Data-Link Layer :**
- This layer is responsible for the error-free transfer of data frames.
- It defines the format of the data on the network.
- It provides a reliable and efficient communication between two or more devices.
- It is mainly responsible for the unique identification of each device that resides on a local network.

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.
- **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.

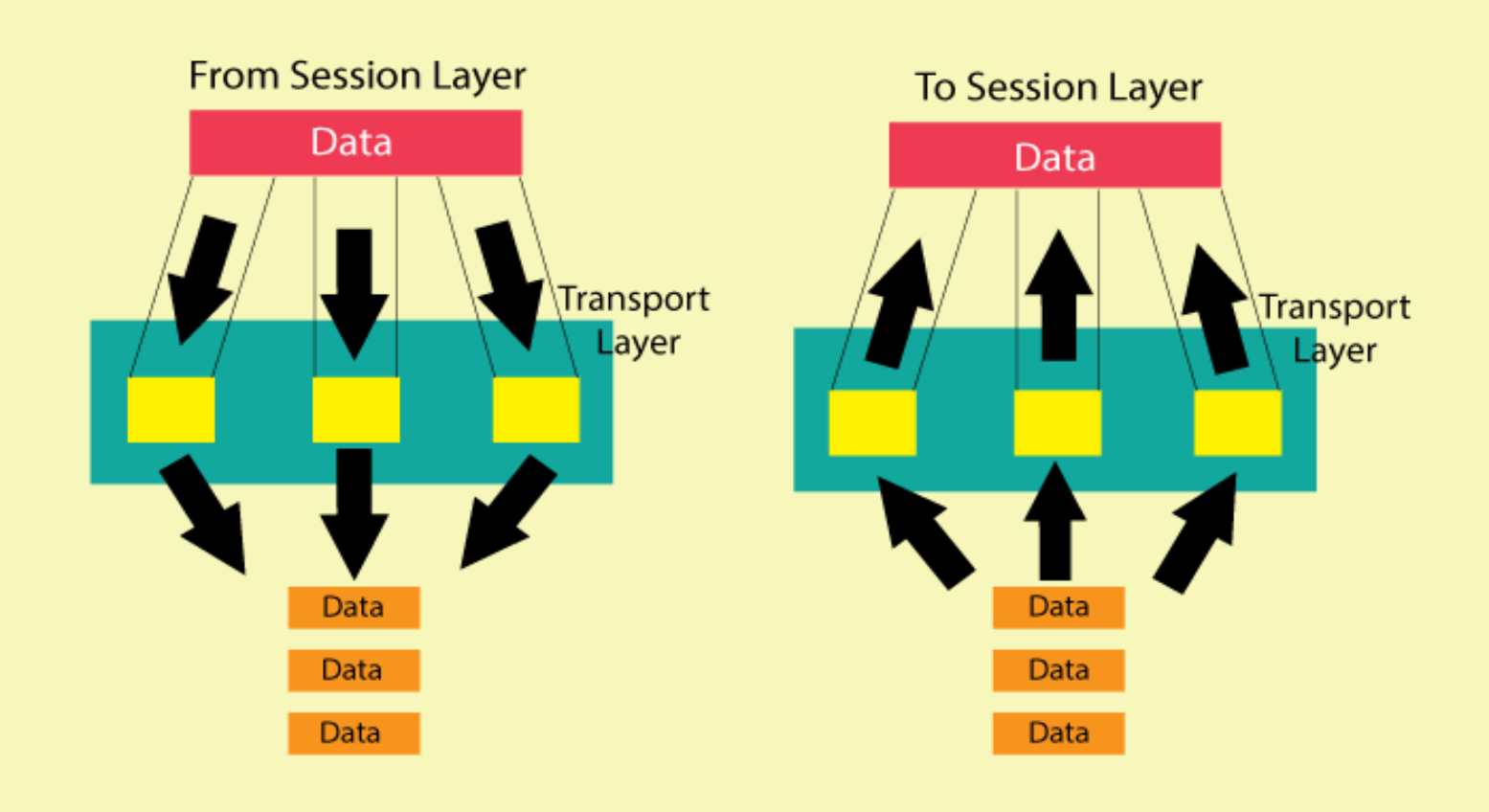
- **Error Control:** Error control is achieved by adding a calculated value CRC (Cyclic Redundancy Check) that is placed to the Data link layer's trailer which is added to the message frame before it is sent to the physical layer.
- If any error seems to occur, then the receiver sends the acknowledgment 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.


From transport layer
L4 data
Network Layer
H3
Packet
L3 data
To Data link layer


To transport layer
L4 data
Packet
H3
Network Layer
L3 data
From Data link layer

- **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.
- 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.

- **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).


From Session Layer
Data
Transport Layer
Data
Data
Data
To Session Layer
Data
Transport Layer
Data
Data
Data

- **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.

Functions of Transport Layer:

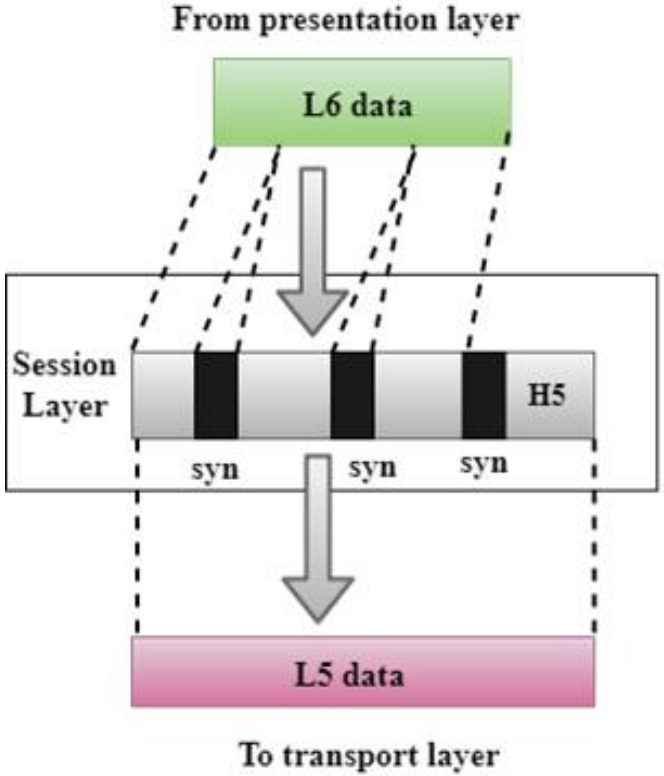
- **Service-point addressing:**
- Computers run several programs simultaneously due to this reason, the transmission of data from source to the destination not only from one computer to another computer but also from one process to another process.
- The transport layer adds the header that contains 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.

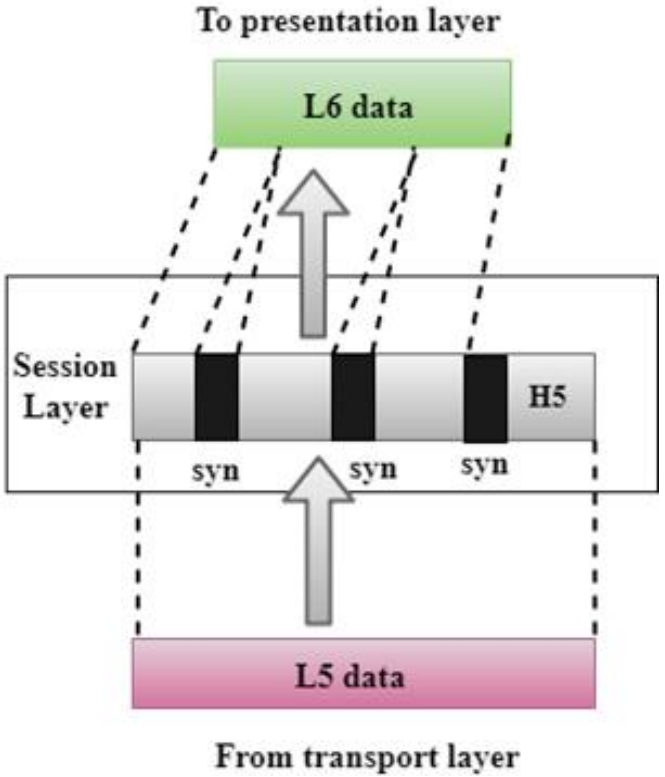
- **Segmentation and reassembly:**
- When the transport layer receives the message from the upper layer, it divides the message into multiple segments, and each segment is assigned with a sequence number that uniquely identifies each segment.
- When the message has arrived at the destination, then the 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.

- **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 edestination without any errornsures that message reach at the.
- **Flow control:** The transport layer also responsible for flow control but it is performed end-to-end rather than across a single link.

Session Layer

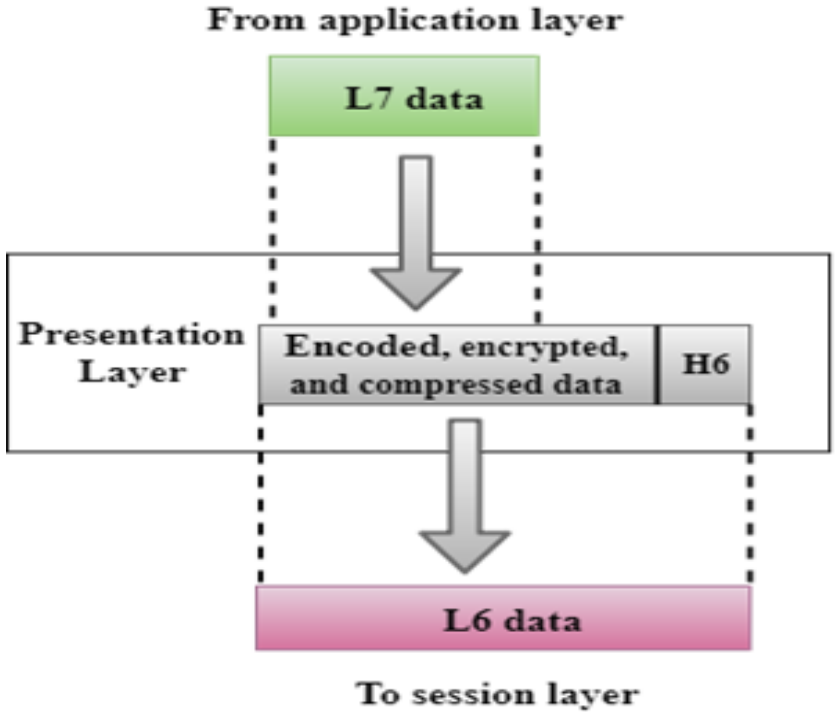


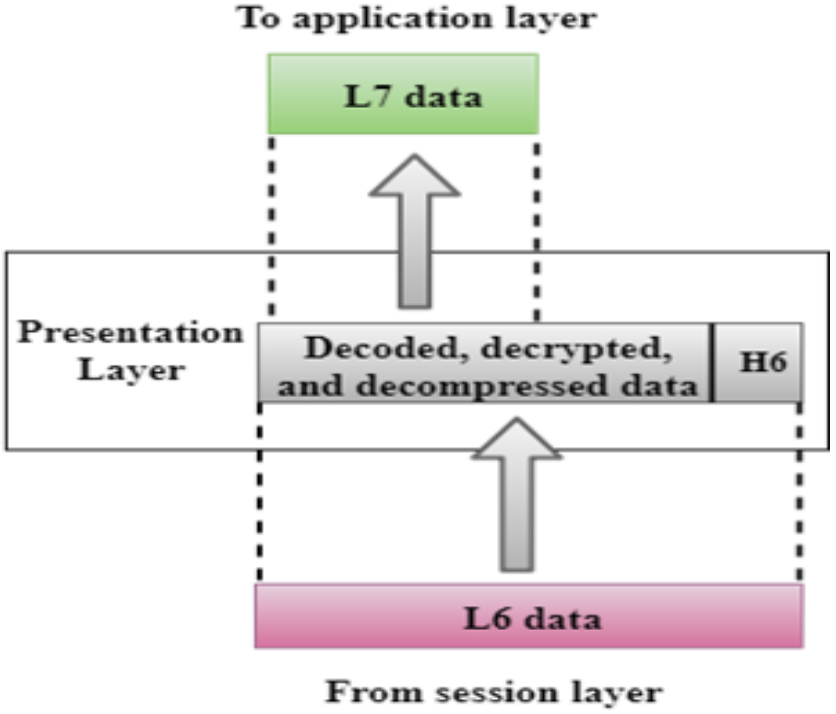


- **Session Layer**
- The Session layer is used to establish, maintain and synchronizes the interaction between communicating devices.
- Functions of Session layer:
- **Dialog control:** Session layer acts as a dialog controller that creates a dialog between two processes, or we can say that it allows 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 :



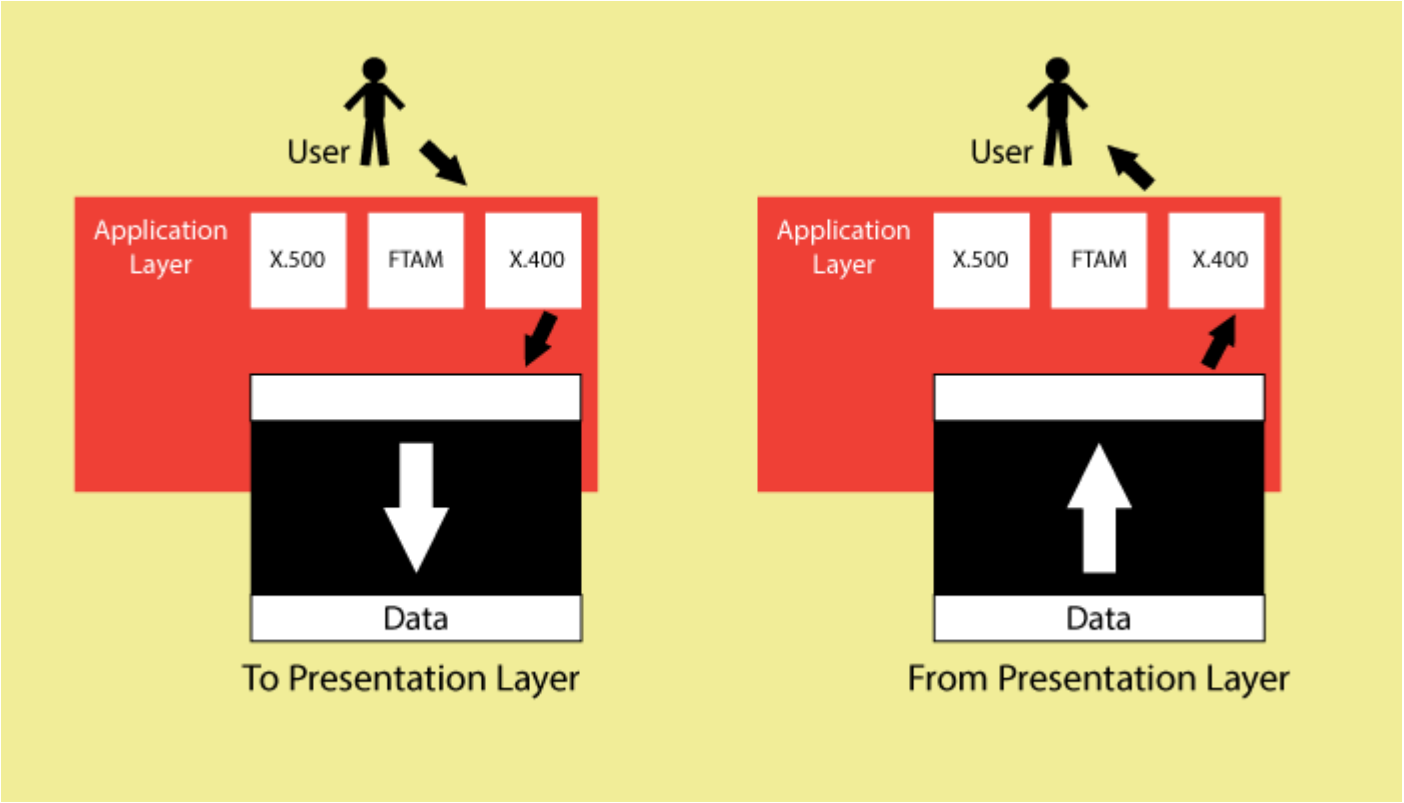


- **Presentation Layer :**
- A Presentation layer is mainly concerned with the syntax and semantics of the information exchanged between the two systems.
- It acts as a data translator for a network.
- This layer is a part of the operating system that converts the data from one presentation format to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

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

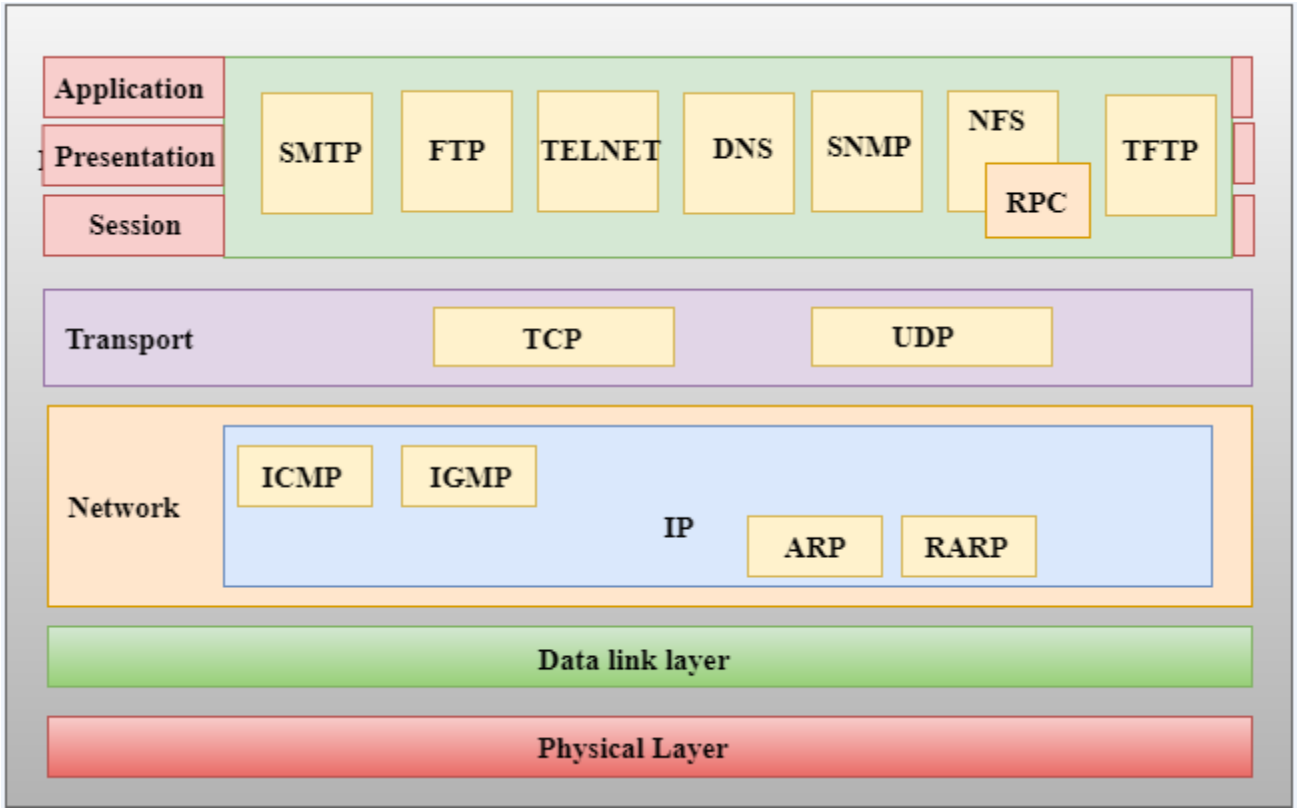
- **Encryption:** Encryption is needed to maintain privacy.
- Encryption is a process of converting the sender-transmitted information into another form and sends the resulting message over the network.
- **Compression:** Data compression is a process of compressing the data, i.e., it reduces the number of bits to be transmitted.
- Data compression is very important in multimedia such as text, audio, video.

• Application layer :



- **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.


Application
Presentation
Session
SMTP
FTP
TELNET
DNS
SNMP
NFS
RPC
TFTP
Transport
TCP
UDP
Network
ICMP
IGMP
IP
ARP
RARP
Data link layer
Physical Layer

Network Access Layer :

- 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 packet into frames transmitted by the network and mapping of IP addresses into physical addresses.

- **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:** The IP addresses are used by the internet and higher layers to identify the device and to provide internetwork routing.
- It determines the path through which the data packet 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.

- **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.
- **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.

- 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**.

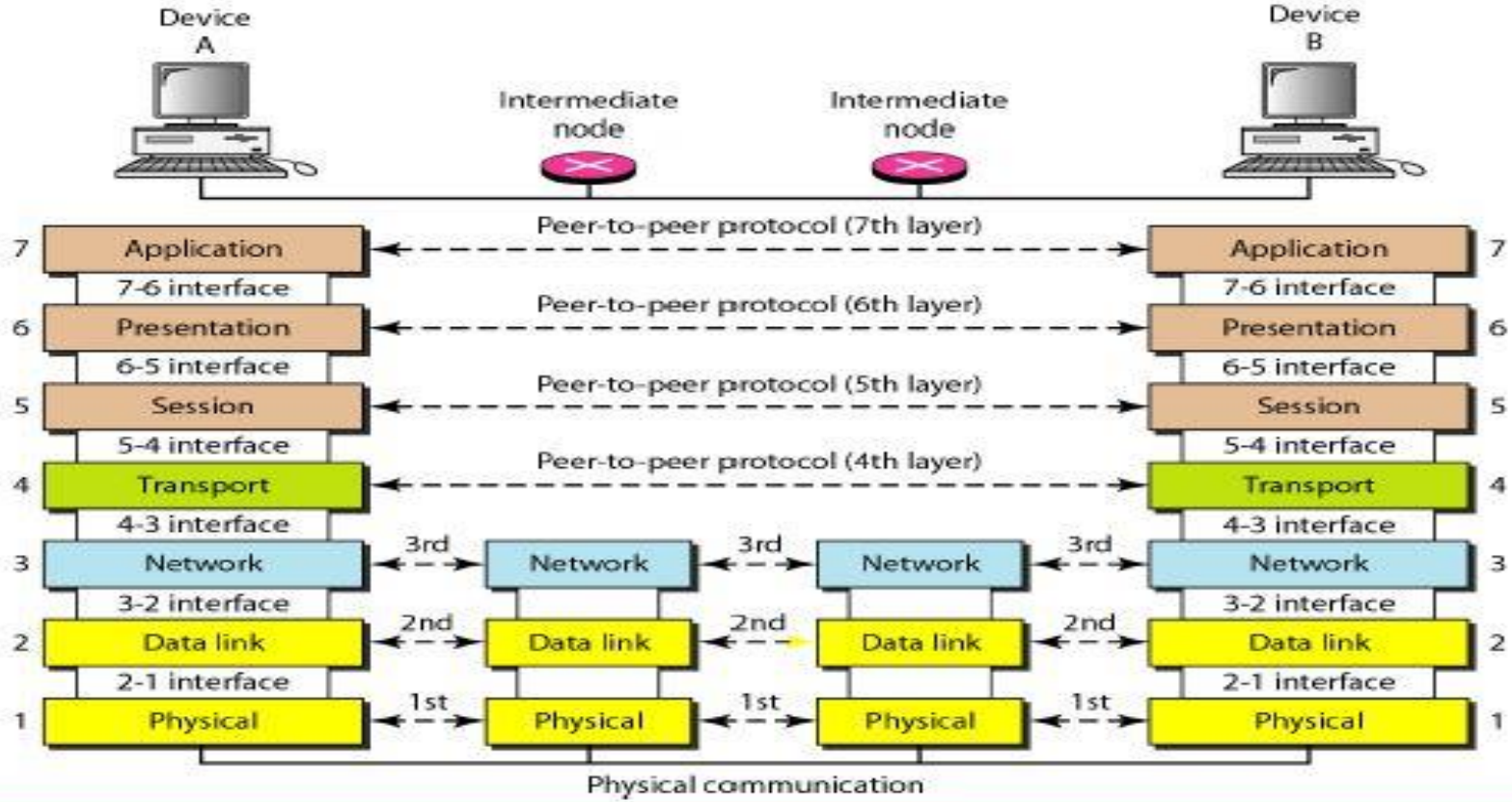
- **Transmission Control Protocol (TCP)**
- It provides a full transport layer services to applications.
- It creates a virtual circuit between the sender and receiver, and it is active for the duration of the transmission.
- TCP is a reliable protocol as it detects the error and retransmits the damaged frames. Therefore, it ensures all the segments must be received and acknowledged before the transmission is completed and a virtual circuit is discarded.

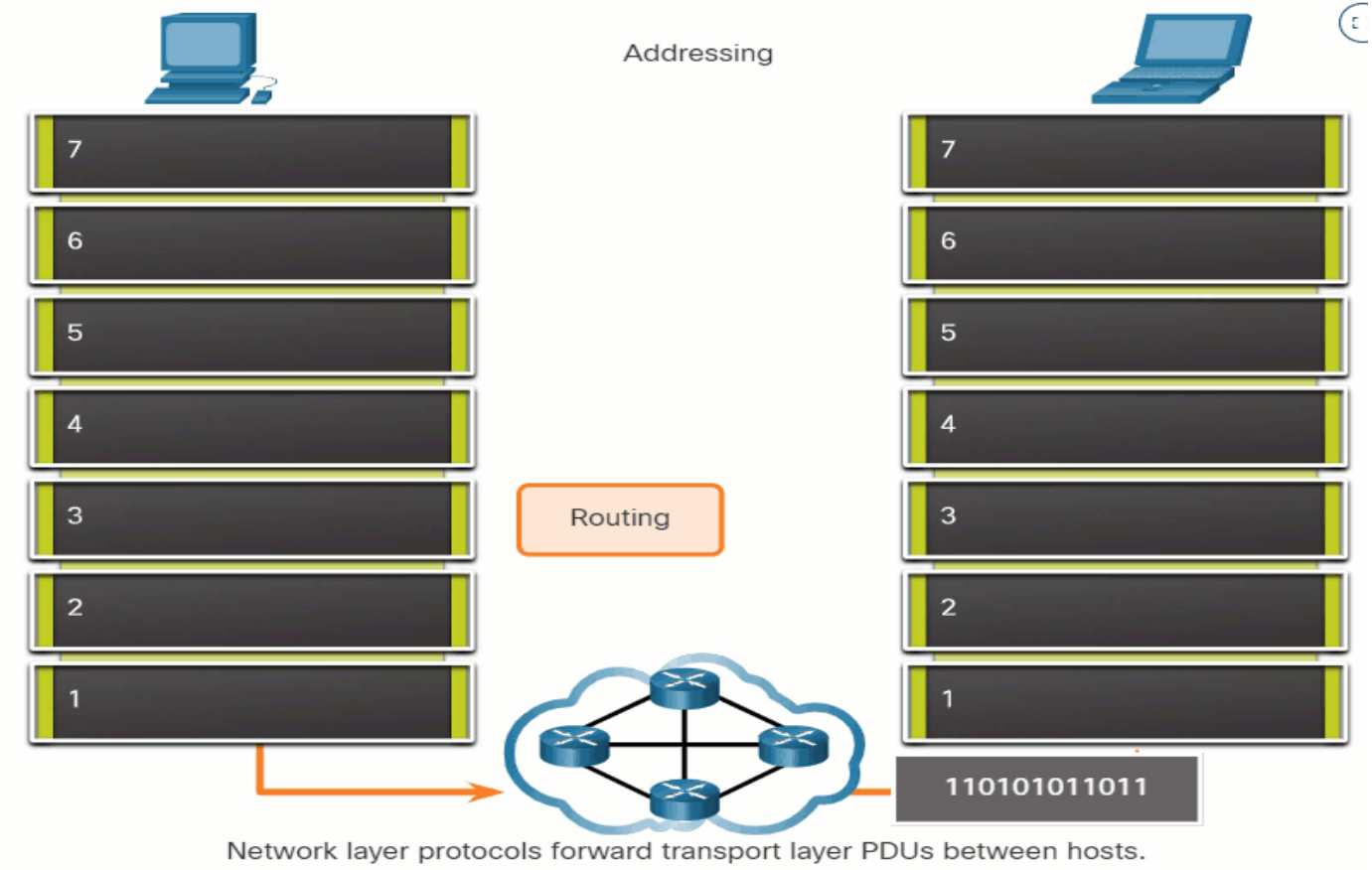
- Application Layer :
- An application layer is the topmost layer in the TCP/IP model.
- It is responsible for handling high-level protocols, issues of representation.
- This layer allows the user to interact with the application.

- **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.
- **SNMP:** SNMP stands for Simple Network Management Protocol. It is a framework used for managing the devices on the internet.

- **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.

Communication Between Layers :




Addressing
7
6
5
4
3
2
1
Routing
7
6
5
4
3
2
1
110101011011
Network layer protocols forward transport layer PDUs between hosts.

- End of Module 1