COMPUTER NETWORKS

UNIT I:

Introduction: Network Types, LAN, MAN, WAN, Network Topologies

Reference models- The OSI Reference Model- the TCP/IP Reference Model - A Comparison of the OSI and TCP/IP Reference Models, OSI Vs TCP/IP, Lack of OSI models success, Internet History.
Physical Layer –Introduction to Guided Media- Twisted-pair cable, Coaxial cable and Fiber optic cable and unguided media: Wireless-Radio waves, microwaves, infrared.

NETWORK: Network is a set of devices (often referred to as *nodes)* connected by communication links. A node can be a computer, printer, or any other device capable of sending and/or receiving data generated by other nodes on the network.“Computer network'' to mean a collection of autonomous computers interconnected by a single technology. Two computers are said to be interconnected if they are able to exchange information.The connection need not be via a copper wire; fiber optics, microwaves, infrared, and communication satellites can also be used.

USES OF COMPUTER NETWORKS

1. Business Applications

- to distribute information throughout the company (**resource sharing).**
- sharing physical resources such as printers, and tape backup systems, is sharing information
- **client-server model**. It is widely used and forms the basis of much network usage.
- **communication medium** among employees.**email** (**electronic mail**), which employees generally use for a great deal of daily communication. Telephone calls between employees may be carried by the computer network instead of by the phone company. This technology is called **IP telephony** or
- **Voice over IP** (**VoIP**) when Internet technology is used.
- **Desktop sharing** lets remote workers see and interact with a graphical computer screen
- doing business electronically, especially with customers and suppliers. This new model is called **e-commerce** (**electronic commerce**) and it has grown rapidly in recent years.

2. Home Applications

- **peer-to-peer** communication
- person-to-person communication
- electronic commerce
- entertainment.(game playing,)

3. Mobile Users

- Text messaging or texting
- Smart phones,
- GPS (Global Positioning System)
- m-commerce
- NFC (Near Field Communication)

4. Social Issues

With the good comes the bad, as this new-found freedom brings with it many unsolved social, political, and ethical issues.

Network Definition – A group of computers which are connected to each other and follow similar usage protocols for the purpose of sharing information and having communications provided by the networking nodes is called a Computer Network.

A network may be small where it may include just one system or maybe as large as what one may want. The nodes may further be classified into various types. These include:

1. Personal Computers
2. Servers
3. Networking Hardware
4. General Hosts

- Networking can be classified into three types:

1. Types of Computer Networks
2. Topology
3. Interpreters

All are in detail further below

1.Types of Computer Networks

There are five main types of Computer Networks:

1. LAN (Local Area Network) –

- Systems connected in a small network like in a building or a small office
- It is inexpensive
- It uses Ethernet or Token-ring technology
- Two or more personal computers can be connected through wires or cables acting as nodes
- Transfer of data is fast and is highly score

2. PAN (Personal Area Network) –

- The smallest computer network
- Devices may be connected through Bluetooth or other infra-red enables devices
- It has a connectivity range of upto 10 metres
- It covers an area of upto 30 feet
- Personal devices belonging to a single person can be connected to each other using PAN

3. MAN (Metropolitan Area Network) –

- A network that can be connected within a city, for example, cable TV Connection
- It can be in the form of Ethernet, ATM, Token-ring and FDDI
- It has a higher range
- This type of network can be used to connect citizens with the various Organisations

4. WAN (Wide Area Network) –

- A network which covers over a country or a larger range of people
- Telephonic lines are also connected through WAN
- Internet is the biggest WAN in the world
- Mostly used by Government Organisations to manage data and information

5. VPN (Virtual Private Network): –

- A network which is constructed by using public wires to connect to a private network
- There are a number of systems which enable you to create networks using the Internet as a medium for transporting data
- These systems use encryptions and other security mechanisms to ensure only authorised users can access

Topology:

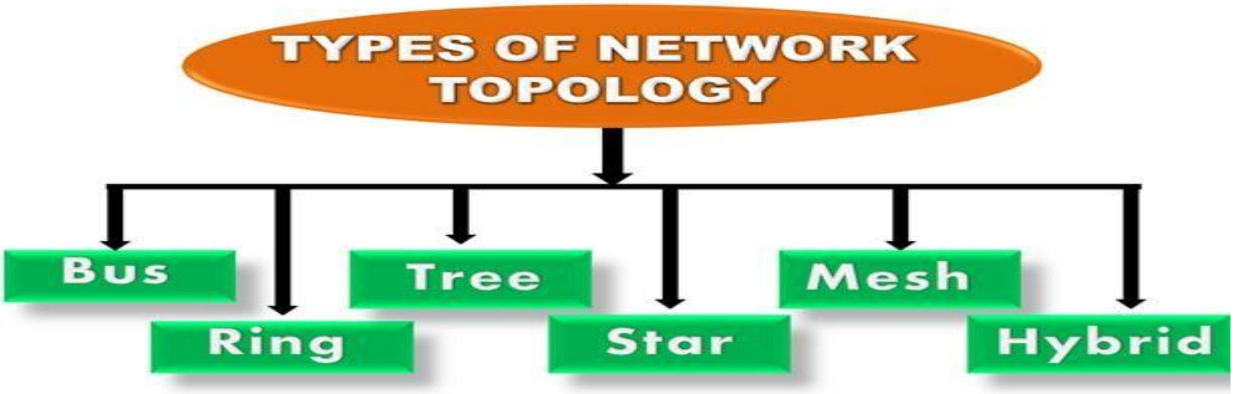
Topology defines the structure of the network of how all the components are interconnected to each other. There are two types of topology: physical and logical topology.
Physical topology is the geometric representation of all the nodes in a network.

Network Topologies

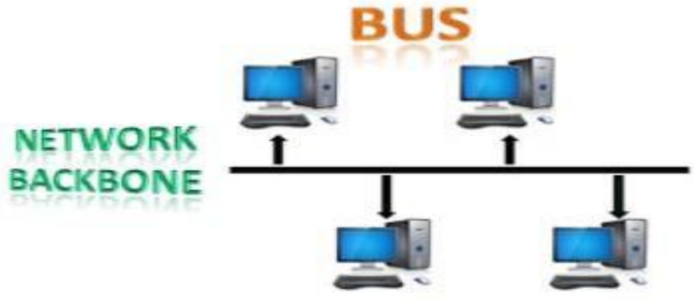
Given below are the eight types of Network Topologies:

1. **Point to Point Topology –** Point to Point topology is the simplest topology that connects two nodes directly together with a common link.
2. **Bus Topology –** A bus topology is such that there is a single line to which all nodes are connected and the nodes connect only to the bus
3. **Mesh Topology –** This type of topology contains at least two nodes with two or more paths between them
4. **Ring Topology –** In this topology every node has exactly two branches connected to it. The ring is broken and cannot work if one of the nodes on the ring fails
5. **Star Topology –** In this network topology, the peripheral nodes are connected to a central node, which rebroadcasts all the transmissions received from any peripheral node to all peripheral nodes on the network, including the originating node

6. **Tree Topology –** In this type of topology nodes are connected in the form of a tree. The function of the central node in this topology may be distributed
7. **Line Topology –** in this topology all the nodes are connected in a straight line
8. **Hybrid Topology –** When two more types of topologies combine together, they form a Hybrid topology



1. Bus Topology



1. The bus topology is designed in such a way that all the stations are connected through a single cable known as a backbone cable.
2. Each node is either connected to the backbone cable by drop cable or directly connected to the backbone cable.
3. 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.
4. The bus topology is mainly used in 802.3 (ethernet) and 802.4 standard networks.
5. The configuration of a bus topology is quite simpler as compared to other topologies.
6. The backbone cable is considered as a **"single lane"** through which the message is broadcast to all the stations.

- **Advantages of Bus topology:**

1. **Low-cost cable:** In bus topology, nodes are directly connected to the cable without

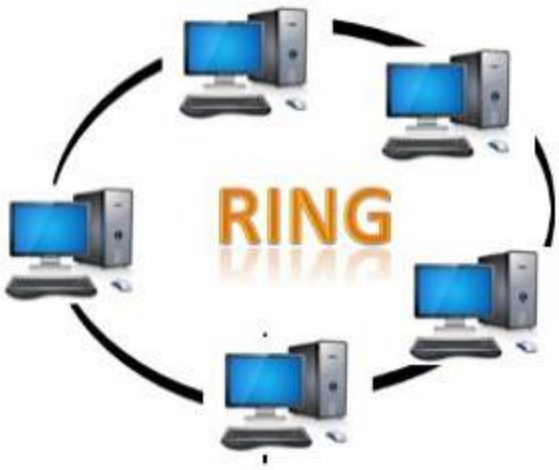
passing through a hub. Therefore, the initial cost of installation is low.

2. **Moderate data speeds:** Coaxial or twisted pair cables are mainly used in bus-based networks that support upto 10 Mbps.
3. **Familiar technology:** Bus topology is a familiar technology as the installation and troubleshooting techniques are well known, and hardware components are easily available.
4. **Limited failure:** A failure in one node will not have any effect on other nodes.

- **Disadvantages of Bus topology**:

1. **Extensive cabling:** A bus topology is quite simpler, but still it requires a lot of cabling.
2. **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.
3. **Signal interference:** If two nodes send the messages simultaneously, then the signals of both the nodes collide with each other.
4. **Reconfiguration difficult:** Adding new devices to the network would slow down the network.
5. **Attenuation:** Attenuation is a loss of signal leads to communication issues. Repeaters are used to regenerate the signal.

2. Ring Topology:



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

7. The most common access method of the ring topology is **token passing**.

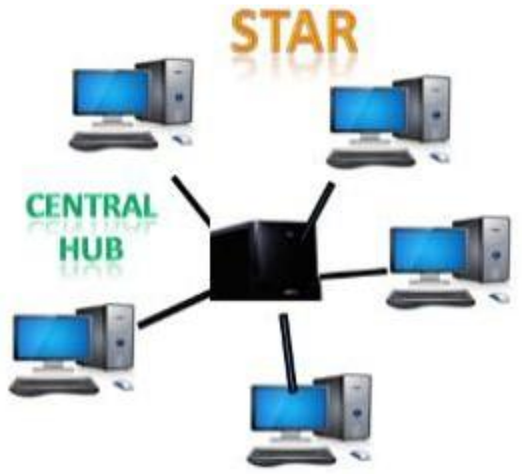
- **Token passing:** It is a network access method in which token is passed from one node to another node.
- **Token:** It is a frame that circulates around the network.
- **Advantages of Ring topology:**

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

- **Disadvantages of Ring topology:**

1. **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.
2. **Failure:** The breakdown in one station leads to the failure of the overall network.
3. **Reconfiguration difficult:** Adding new devices to the network would slow down the network.
4. **Delay:** Communication delay is directly proportional to the number of nodes. Adding new devices increases the communication delay.

3. Star Topology



1. Star topology is an arrangement of the network in which every node is connected to the central hub, switch or a central computer.
2. The central computer is known as a **server**, and the peripheral devices attached to the server are known as **clients**.

3. Coaxial cable or RJ-45 cables are used to connect the computers.
4. Hubs or Switches are mainly used as connection devices in a **physical star topology**.
5. Star topology is the most popular topology in network implementation.

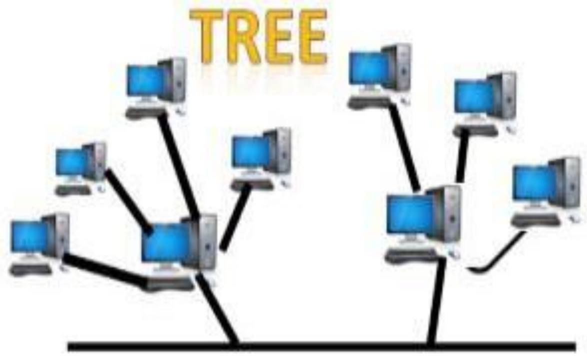
- **Advantages of Star topology:**

1. **Efficient troubleshooting:** Troubleshooting is quite efficient in a star topology as compared to bus topology. In a bus topology, the manager has to inspect the kilometers of cable. In a star topology, all the stations are connected to the centralized network. Therefore, the network administrator has to go to the single station to troubleshoot the problem.
2. **Network control:** Complex network control features can be easily implemented in the star topology. Any changes made in the star topology are automatically accommodated.
3. **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.
4. **Familiar technology:** Star topology is a familiar technology as its tools are cost- effective.
5. **Easily expandable:** It is easily expandable as new stations can be added to the open ports on the hub.
6. **Cost effective:** Star topology networks are cost-effective as it uses inexpensive coaxial cable.
7. **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**

1. **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.
2. **Cable:** Sometimes cable routing becomes difficult when a significant amount of routing is required.

4. Tree topology



1. Tree topology combines the characteristics of bus topology and star topology.
2. A tree topology is a type of structure in which all the computers are connected with each

other in hierarchical fashion.

3. The top-most node in tree topology is known as a root node, and all other nodes are the descendants of the root node.
4. There is only one path exists between two nodes for the data transmission. Thus, it forms a parent-child hierarchy.

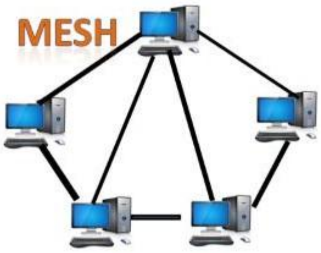
- **Advantages of Tree topology**

1. **Support for broadband transmission:** Tree topology is mainly used to provide broadband transmission, i.e., signals are sent over long distances without being attenuated.
2. **Easily expandable:** We can add the new device to the existing network. Therefore, we can say that tree topology is easily expandable.
3. **Easily manageable:** In tree topology, the whole network is divided into segments known as star networks which can be easily managed and maintained.
4. **Error detection:** Error detection and error correction are very easy in a tree topology.
5. **Limited failure:** The breakdown in one station does not affect the entire network.
6. **Point-to-point wiring:** It has point-to-point wiring for individual segments.

- **Disadvantages of Tree topology**

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

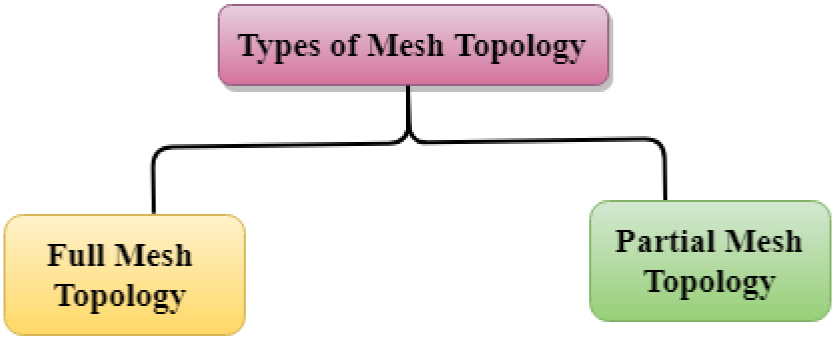
5. Mesh topology:



1. Mesh technology is an arrangement of the network in which computers are interconnected with each other through various redundant connections.
2. There are multiple paths from one computer to another computer.
3. It does not contain the switch, hub or any central computer which acts as a central point of communication.
4. The Internet is an example of the mesh topology.
5. Mesh topology is mainly used for WAN implementations where communication failures

are a critical concern.

6. Mesh topology is mainly used for wireless networks.
7. Mesh topology can be formed by using the formula: **Number of cables = (n*(n-1))/2;**
8. Where n is the number of nodes that represents the network.
9. **Mesh topology is divided into two categories:**
10. Fully connected mesh topology
11. Partially connected mesh topology



1.Full Mesh Topology: In a full mesh topology, each computer is connected to all the computers available in the network.

2.Partial Mesh Topology: In a partial mesh topology, not all but certain computers are connected to those computers with which they communicate frequently.

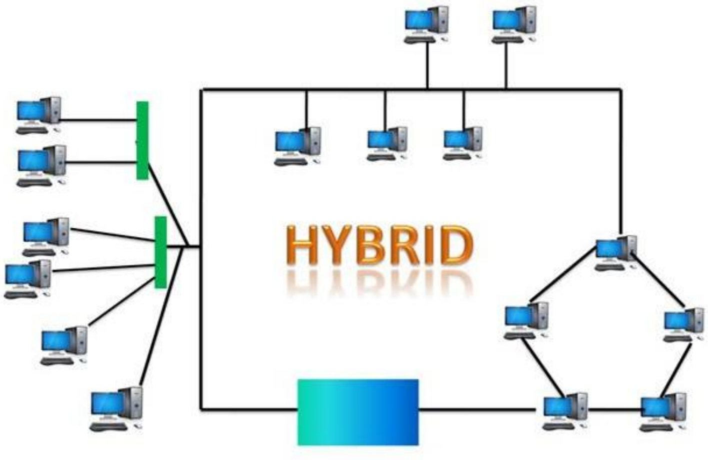
- **Advantages of Mesh topology:**

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

- **Disadvantages of Mesh topology**

1. **Cost:** A mesh topology contains a large number of connected devices such as a router and more transmission media than other topologies.
2. **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.
3. **Efficiency:** In this topology, redundant connections are high that reduces the efficiency of the network.

Hybrid Topology:



1. The combination of various different topologies is known as **Hybrid topology**.
2. A Hybrid topology is a connection between different links and nodes to transfer the data.
3. When two or more different topologies are combined together is termed as Hybrid topology and if similar topologies are connected with each other will not result in Hybrid topology. For example, if there exist a ring topology in one branch of ICICI bank and bus topology in another branch of ICICI bank, connecting these two topologies will result in Hybrid topology.

- **Advantages of Hybrid Topology:**

1. **Reliable:** If a fault occurs in any part of the network will not affect the functioning of the rest of the network.
2. **Scalable:** Size of the network can be easily expanded by adding new devices without affecting the functionality of the existing network.
3. **Flexible:** This topology is very flexible as it can be designed according to the requirements of the organization.
4. **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:**

1. **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.
2. **Costly Hub:** The Hubs used in the Hybrid topology are very expensive as these hubs are different from usual Hubs used in other topologies.
3. **Costly infrastructure:** The infrastructure cost is very high as a hybrid network requires a lot of cabling, network devices, etc.

3 REFERENCE MODELS:

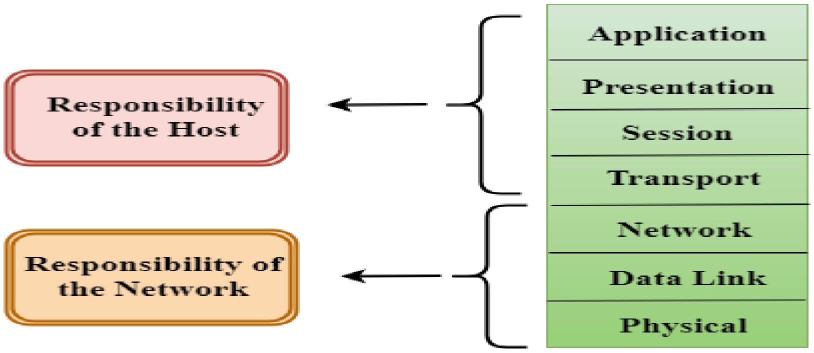
Computer Network Models

A communication subsystem is a complex piece of Hardware and software. Early attempts for implementing the software for such subsystems were based on a single, complex, unstructured program with many interacting components. The resultant software was very difficult to test and modify. To overcome such problem, the ISO has developed a layered approach. In a layered approach, networking concept is divided into several layers, and each layer is assigned a particular task. Therefore, we can say that networking tasks depend upon the layers.

1. OSI Model:

1. 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.
2. OSI consists of seven layers, and each layer performs a particular network function.
3. 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.
4. OSI model divides the whole task into seven smaller and manageable tasks. Each layer is assigned a particular task.
5. Each layer is self-contained, so that task assigned to each layer can be performed independently.

Characteristics of OSI Model:



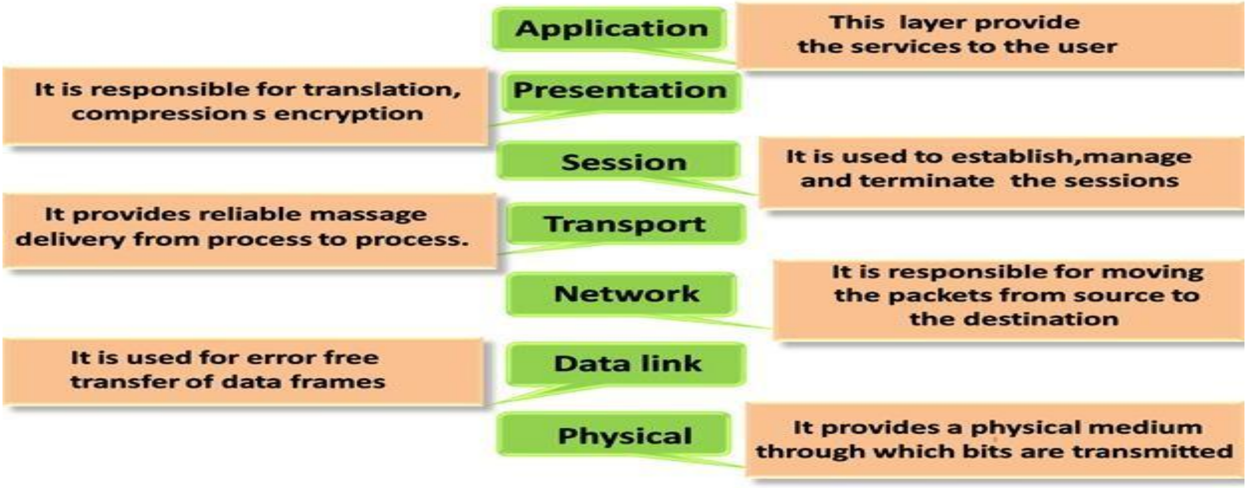
The OSI model is divided into **two** layers: **upper layers and lower layers**.

1. 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.
2. 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.

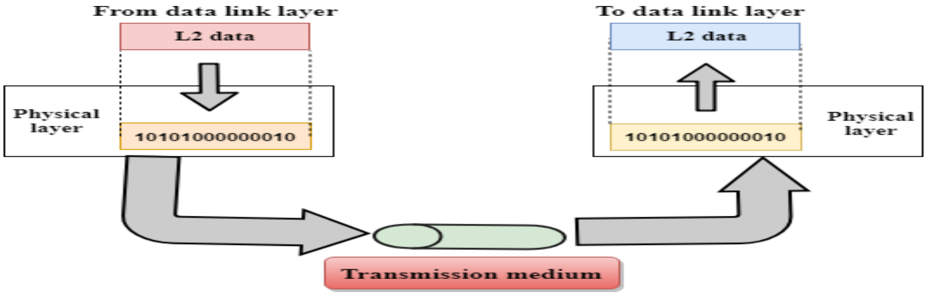
Functions of the OSI Layers:

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


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

1.Physical layer:



The main functionality of the physical layer is to transmit the individual bits from one node to another node.

- It is the lowest layer of the OSI model.
- It establishes, maintains and deactivates the physical connection.
- It specifies the mechanical, electrical and procedural network interface specifications.

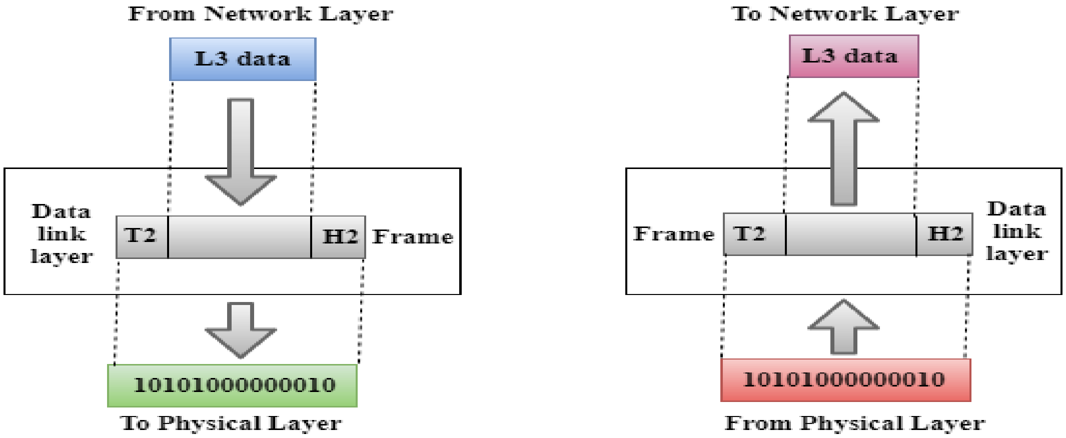
a.Functions of a Physical layer:

Line Configuration: It defines the way how two or more devices can be connected physically. **Data Transmission:** It defines the transmission mode whether it is simplex, half-duplex or full- duplex mode between the two devices on the network.

Topology: It defines the way how network devices are arranged.

Signals: It determines the type of the signal used for transmitting the information.

2. Data-Link Layer:



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

It contains two sub-layers: **1.** Logical Link Control Layer
2. Media Access Control Layer

1. 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.

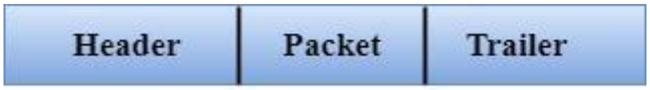
2. Media Access Control Layer

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 occurr, then the receiver sends the acknowledgment for the retransmission of the corrupted frames.

Access Control: When two or more devices are connected to the same communication channel, then the data link layer protocols are used to determine which device has control over the link at a given time.

3. Network Layer:

- It is a layer 3 that manages device addressing, tracks the location of devices on the network.
- It determines the best path to move data from source to the destination based on the network conditions, the priority of service, and other factors.
- The Data link layer is responsible for routing and forwarding the packets.
- Routers are the layer 3 devices, they are specified in this layer and used to provide the routing services within an internetwork.
- The protocols used to route the network traffic are known as Network layer protocols. Examples of protocols are IP and Ipv6.

Functions of Network Layer:

Internetworking: An internetworking is the main responsibility of the network layer. It provides a logical connection between different devices.

Addressing: A Network layer adds the source and destination address to the header of the frame. Addressing is used to identify the device on the internet.

Routing: Routing is the major component of the network layer, and it determines the best optimal path out of the multiple paths from source to the destination.

Packetizing: A Network Layer receives the packets from the upper layer and converts them into packets. This process is known as Packetizing. It is achieved by internet protocol (IP).

4. Transport Layer:

- The Transport layer is a Layer 4 ensures that messages are transmitted in the order in which they are sent and there is no duplication of data.
- The main responsibility of the transport layer is to transfer the data completely.
- It receives the data from the upper layer and converts them into smaller units known as segments.
- This layer can be termed as an end-to-end layer as it provides a point-to-point connection between source and destination to deliver the data reliably.

The two protocols used in this layer are:

Transmission Control Protocol

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

User Datagram Protocol:

- User Datagram Protocol is a transport layer protocol.
- It is an unreliable transport protocol as in this case receiver does not send any acknowledgment when the packet is received, the sender does not wait for any acknowledgment. Therefore, this makes a protocol unreliable.

Functions of Transport Layer:

1. 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.

2. **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.
3. **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.
4. **Flow control:** The transport layer also responsible for flow control but it is performed end-to- end rather than across a single link.
5. **Error control:** The transport layer is also responsible for Error control. Error control is performed end-to-end rather than across the single link. The sender transport layer ensures that message reach at the destination without any error.

5. Session Layer:

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

Functions of Session layer:

1. **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.
2. **Synchronization:** Session layer adds some checkpoints when transmitting the data in a sequence. If some error occurs in the middle of the transmission of data, then the transmission will take place again from the checkpoint. This process is known as Synchronization and recovery.

6. Presentation Layer:

1. A Presentation layer is mainly concerned with the syntax and semantics of the information exchanged between the two systems.

2. It acts as a data translator for a network.
3. This layer is a part of the operating system that converts the data from one presentation format to another format.
4. The Presentation layer is also known as the syntax layer.

Functions of Presentation layer:

1. 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.

2. 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.

3. Compression: Data compression is a process of compressing the data, i.e., it reduces the number of bits to be transmitted. Data compression is very important in multimedia such as text, audio, video.

7. Application Layer:

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

Functions of Application layer:

1. 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.

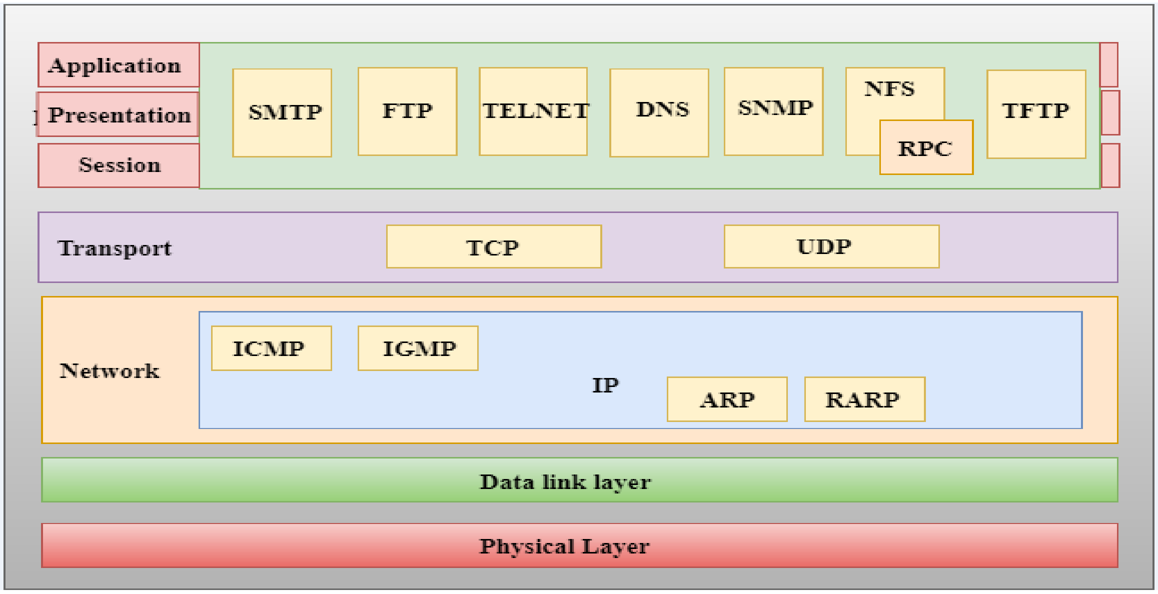
2. Mail services: An application layer provides the facility for email forwarding and storage. Directory services: An application provides the distributed database sources and is used to provide that global information about various objects.

TCP/IP model:

1. The TCP/IP model was developed prior to the OSI model.
2. The TCP/IP model is not exactly similar to the OSI model.

3. The TCP/IP model consists of five layers: the application layer, transport layer, network layer, data link layer and physical layer.
4. The first four layers provide physical standards, network interface, internetworking, and transport functions that correspond to the first four layers of the OSI model and these four layers are represented in TCP/IP model by a single layer called the application layer.
5. TCP/IP is a hierarchical protocol made up of interactive modules, and each of them provides specific functionality.
6. Here, hierarchical means that each upper-layer protocol is supported by two or more lower-level protocols.

Functions of TCP/IP layers:



Network Access Layer:

- A network layer is the lowest layer of the TCP/IP model.
- A network layer is the combination of the Physical layer and Data Link layer defined in the OSI reference model.
- It defines how the data should be sent physically through the network.
- This layer is mainly responsible for the transmission of the data between two devices on the same network.
- The functions carried out by this layer are encapsulating the IP datagram into frames transmitted by the network and mapping of IP addresses into physical addresses.
- The protocols used by this layer are ethernet, token ring, FDDI, X.25, frame relay.

Internet Layer:

1. An internet layer is the second layer of the TCP/IP model.
2. An internet layer is also known as the network layer.
3. 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:

1. **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:

2. **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.
3. **Host-to-host communication:** It determines the path through which the data is to be transmitted.
4. **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.
5. **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.
6. **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.
7. **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:

1. **ARP request:** When a sender wants to know the physical address of the device, it broadcasts the ARP request to the network.
2. **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

8. **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:

1. **ICMP Test:** ICMP Test is used to test whether the destination is reachable or not.
2. **ICMP Reply:** ICMP Reply is used to check whether the destination device is responding or not.

The core responsibility of the ICMP protocol is to report the problems, not correct them. The responsibility of the correction lies with the sender.

ICMP can send the messages only to the source, but not to the intermediate routers because the IP datagram carries the addresses of the source and destination but not of the router that it is passed to.

Transport Layer:

The transport layer is responsible for the reliability, flow control, and correction of data which is being sent over the network.

The two protocols used in the transport layer are **User Datagram protocol and Transmission control protocol**.

User Datagram Protocol (UDP)

It provides connectionless service and end-to-end delivery of transmission. It is an unreliable protocol as it discovers the errors but not specify the error.

User Datagram Protocol discovers the error, and ICMP protocol reports the error to the sender that user datagram has been damaged.

UDP consists of the following fields:

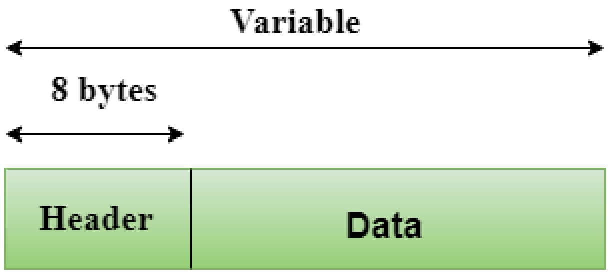
Source port address: The source port address is the address of the application program that has created the message.

Destination port address: The destination port address is the address of the application program that receives the message.

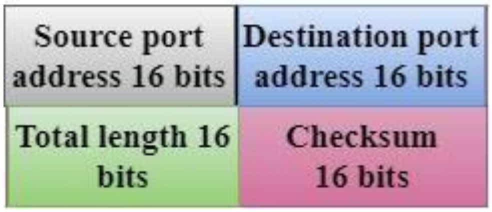
Total length: It defines the total number of bytes of the user datagram in bytes.

Checksum: The checksum is a 16-bit field used in error detection.

UDP does not specify which packet is lost. UDP contains only checksum; it does not contain any ID of a data segment.



Header Format



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

Transmission Control Protocol (TCP)

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:

1.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.

2.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.

3.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.

4.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.

5.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.

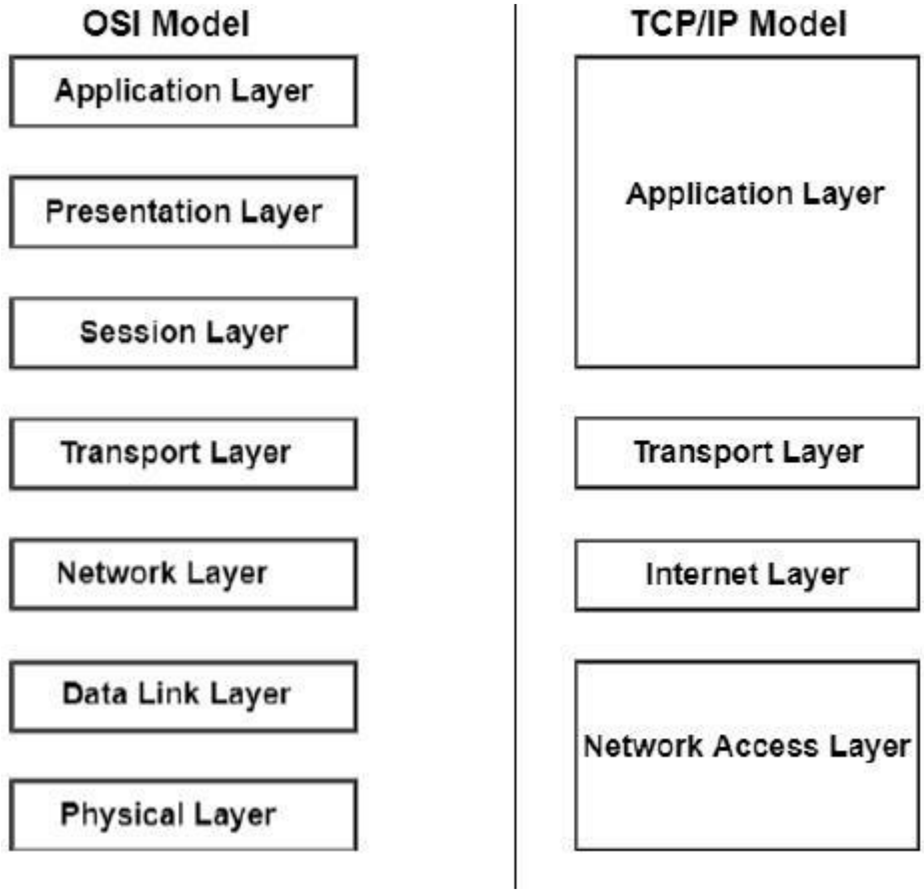
6.FTP: FTP stands for File Transfer Protocol. FTP is a standard internet protocol used for transmitting the files from one computer to another computer.

Difference between OSI and TCP/IP Reference Model

Following are the differences between OSI and TCP/IP Reference Model −

OSI	TCP/IP
OSI represents Open System Interconnection.	TCP/IP model represents the Transmission Control Protocol / Internet Protocol.
OSI is a generic, protocol independent standard. It is acting as an interaction gateway between the network and the final-user.	TCP/IP model depends on standard protocols about which the computer network has created. It is a connection protocol that assigns the network of hosts over the internet.
The OSI model was developed first, and then protocols were created to fit the network architecture's needs.	The protocols were created first and then built the TCP/IP model.
It provides quality services.	It does not provide quality services.

OSI	TCP/IP
The OSI model represents defines administration, interfaces and conventions. It describes clearly which layer provides services.	It does not mention the services, interfaces, and protocols.
The protocols of the OSI model are better unseen and can be returned with another appropriate protocol quickly.	The TCP/IP model protocols are not hidden, and we cannot fit a new protocol stack in it.
It is difficult as distinguished to TCP/IP.	It is simpler than OSI.
It provides both connection and connectionless oriented transmission in the network layer; however, only connection-oriented transmission in the transport layer.	It provides connectionless transmission in the network layer and supports connecting and connectionless- oriented transmission in the transport layer.
It uses a horizontal approach.	It uses a vertical approach.
The smallest size of the OSI header is 5 bytes.	The smallest size of the TCP/IP header is 20 bytes.
Protocols are unknown in the OSI model and are returned while the technology modifies.	In TCP/IP, returning protocol is not difficult.



Main difference between TCP/IP and OSI Model:

1. TCP/IP Model is a communication protocols suite using which network devices can be connected to the Internet. On the other hand, the OSI Model is a conceptual framework, using which the functioning of a network can be described.

2. TCP/IP vs OSI: TWO are the different layers

The TCP/IP Model comprises four layers: Network Interface, Internet, Transport and Application. The OSI Model comprises seven layers: Physical, Data Link, Network, Transport, Session, Presentation and Application.

3. TCP/IP a part of the OSI Model

There is a separate layer for Data Link and Physical in the OSI Model, whereas, the TCP/IP has a single Network Interface layer for the same. Similarly, there is Application, Presentation and Session layers in OSI, which are combined into one layer (Application) for TCP/IP.

4. TCP/IP vs OSI: Which came first

Among TCP/IP and OSI, the Open Systems Interconnection model was introduced by the

International Organisation of Standardization in 1984 and the TCP/IP model was introduced about 10 years before that.

Similarities between the OSI and TCP/IP model:

The following are the similarities between the OSI and TCP/IP model:

1. Share common architecture

Both the models are the logical models and having similar architectures as both the models are constructed with the layers.

2. Define standards

Both the layers have defined standards, and they also provide the framework used for implementing the standards and devices.

3. Simplified troubleshooting process

Both models have simplified the troubleshooting process by breaking the complex function into simpler components.

4. Pre-defined standards

The standards and protocols which are already pre-defined; these models do not redefine them; they just reference or use them. For example, the Ethernet standards were already defined by the IEEE before the development of these models; instead of recreating them, models have used these pre-defined standards.

5. Both have similar functionality of 'transport' and 'network' layers

The function which is performed between the **'presentation'** and the **'network'** layer is similar to the function performed at the **transport** layer.

8. Lack of osi model success: One is TCP/IP model (Transmission Control Protocol / Internet ~~Protocol) and other is OSI model (Open Systems Interconnection). The OSI model was developed~~ by the International Organization of Standardization (ISO) and the TCP/IP model was with the US Defense Advanced Research Projects Agency (DARPA).

Development of TCP/IP model and OSI model were started during early 1970s. TCP/IP model and OSI model were evolved during 1980s.

TCP/IP is the protocol suite on which almost all of the world's computer networks run. OSI model couldn't compete with TCP/IP model, and failed in getting wider acceptance. One of the main reasons behind the failure of OSI model and wider acceptance of TCP/IP model was because big global networks like internet started running on TCP/IP protocol suite.

All leading vendors discarded their proprietary networking protocols in favor of TCP/IP protocol suite.Even now we refer OSI model terminologies while discussing about networking related topics.

OSI model clearly explained, how different functions of computer networking should work together. The functions of different layers are clearly defined in OSI model. Universities, colleges and networking training institutes explained the concepts of computer networking based on the terminologies from OSI model for many decades.

For example, while discussing about IP addresses, we also call IP addresses as layer 3 addresses. IP addresses are also called as layer 3 addresses, because IP addresses are linked with the function of layer 3 of OSI model.

As a networking student, we need to understand that OSI model is not being implemented as a software product or as a service these days. But, OSI model explains about the functions of different components of computer networking in a simpler and easier way. The terminologies of OSI model are still used to teach and explain computer networking. you may never ever work on an implementation of OSI model in future, but the legacy of OSI model still continues.

9. Internet history:

1. The Internet started off with research into what was then known as packet switching as early as the 1960s. Packet switching was thought of as a better and faster method to transfer data than the hardware solution to the problem, i.e., the circuitry. The packet switching technology was essential to the development of ARPANET by the United States Military. ARPANET is considered the first known group of interconnected computers aka the internet. This system was used to transfer confidential data between the Military. This data-sharing technology was then opened to educational institutes in the United States to allow them to access to government's supercomputer, first at 56 kbit/s, then at 1.5 Mbit/s, and then at 45 Mbit/s. Com Internet service providers began to arise in the late 1980s and the internet was fully commercialized in the US by 1995.
2. Internet, also known as the World Wide Web (www), is a global system of interconnected computer networks that use a protocol called the Internet Protocol Suite (TCP/IP) to link to billions of devices all around the world. The impact of this has been so enormous that it has been referred to as the 8th continent of the world. This carries a vast range of information, from the top-secret military and research files to the most trending and viral video of the week. This

massive storage is shared by everyone, with everyone's computer contributing to the ever- expanding treasure trove of knowledge.

3. The advent of the internet is heavily influencing most traditional communication methods such as newspapers, telephones, television, etc. They are giving rise to new services such as internet phones and internet tv. The exchange of information has been accelerated exponentially and consequentially the exchange of information has led to an improvement in the standard of life for many people across the globe.

4. World Wide Web is a complex web of websites and web pages connected together through hypertexts. Hypertext is a word or group of words linking to another web page of the same or different website. When the hypertext is clicked, another web page opens.

The evolution from ARPANET to WWW was possible due to many new achievements by researchers and computer scientists all over the world. Here are some of those developments −

Year	Milestone
1957	Advanced Research Project Agency formed by US
1969	ARPANET became functional
1970	ARPANET connected to BBNs
1972	Roy Tomlinson develops network messaging or E-mail. Symbol @ comes to mean "at"
1973	APRANET connected to Royal Radar Network of Norway
1974	Term Internet coined First commercial use of ARPANET, Telenet, is approved
1982	TCP/IP introduced as standard protocol on ARPANET
1983	Domain Name System introduced
1986	National Science Foundation brings connectivity to more people with its NSFNET program
1990	ARPANET decommissioned First web browser Nexus developed HTML developed

2002-2004	Web 2.0 is born

10. Physical layer:

1. it is the lowest layer of the OSI Model.
2. It activates, maintains and deactivates the physical connection.
3. It is responsible for transmission and reception of the unstructured raw data over network.
4. Voltages and data rates needed for transmission is defined in the physical layer.
5. It converts the digital/analog bits into electrical signal or optical signals.
6. Data encoding is also done in this layer.

11. Guided Media

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

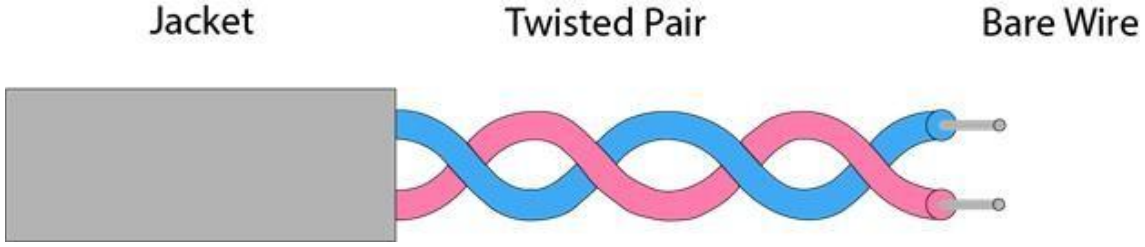
Types Of Guided media:

1. Twisted pair:

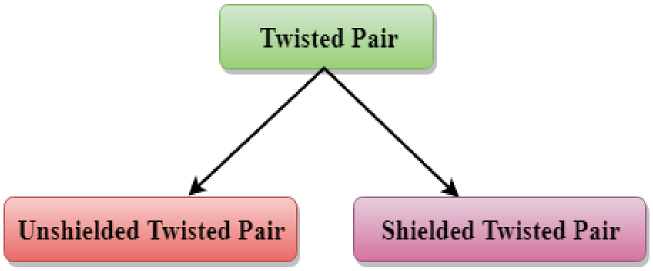
Twisted pair is a physical media made up of a pair of cables twisted with each other. A twisted pair cable is cheap as compared to other transmission media. Installation of the twisted pair cable is easy, and it is a lightweight cable. The frequency range for twisted pair cable is from 0 to 3.5KHz.

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

The degree of reduction in noise interference is determined by the number of turns per foot. Increasing the number of turns per foot decreases noise interference.



Types of Twisted pair:



1. 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.

2. 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:**

1. The cost of the shielded twisted pair cable is not very high and not very low.
2. An installation of STP is easy.
3. It has higher capacity as compared to unshielded twisted pair cable.
4. It has a higher attenuation.
5. It is shielded that provides the higher data transmission rate.

- **Disadvantages**

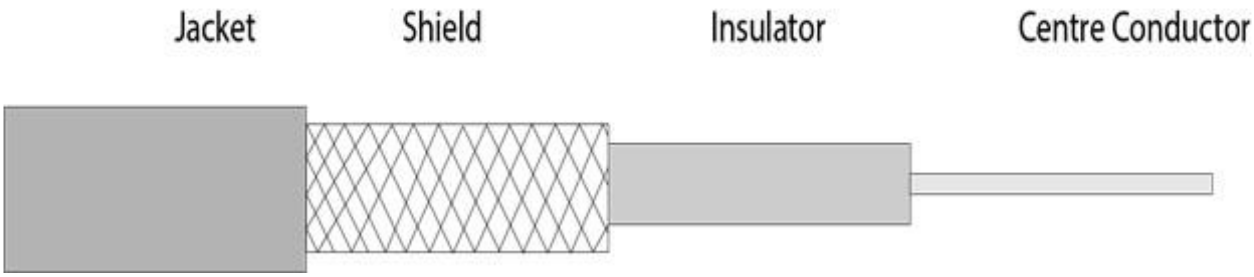
1. It is more expensive as compared to UTP and coaxial cable.
2. It has a higher attenuation rate.

---

2 Coaxial Cable:

1. Coaxial cable is very commonly used transmission media, for example, TV wire is usually a coaxial cable.
2. The name of the cable is coaxial as it contains two conductors parallel to each other.
3. It has a higher frequency as compared to Twisted pair cable.
4. 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.

5. 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:**

1. The data can be transmitted at high speed.
2. It has better shielding as compared to twisted pair cable.
3. It provides higher bandwidth.

- **Disadvantages Of Coaxial cable:**

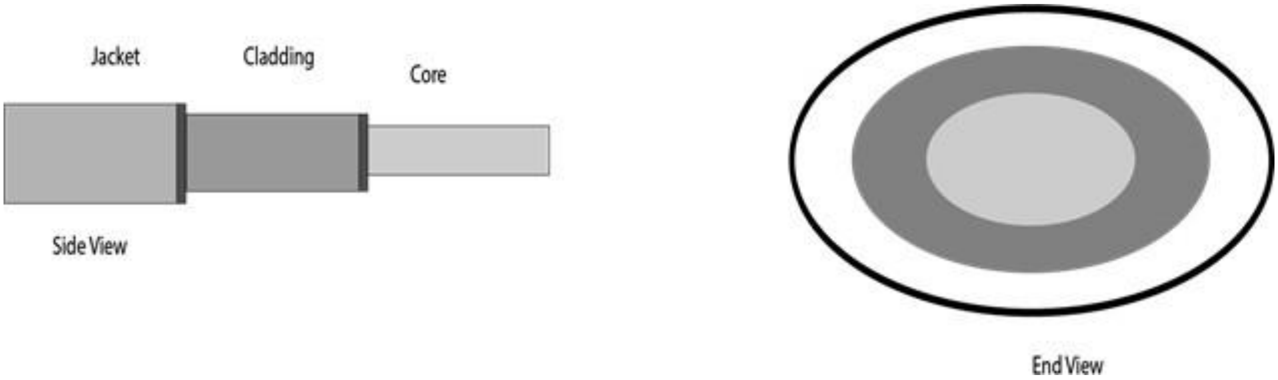
1. It is more expensive as compared to twisted pair cable.
2. If any fault occurs in the cable causes the failure in the entire network.

---

3 Fibre Optic:

1. Fibre optic cable is a cable that uses electrical signals for communication.
2. Fibre optic is a cable that holds the optical fibres coated in plastic that are used to send the data by pulses of light.
3. The plastic coating protects the optical fibres from heat, cold, electromagnetic interference from other types of wiring.
4. Fibre optics provide faster data transmission than copper wires.

- **Diagrammatic representation of fibre optic cable:**



Basic Elements of Fibre optic cable:

1. **Core:** The optical fibre consists of a narrow strand of glass or plastic known as a core. A core is a light transmission area of the fibre. The more the area of the core, the more light will be transmitted into the fibre.
2. **Cladding:** The concentric layer of glass is known as cladding. The main functionality of the cladding is to provide the lower refractive index at the core interface as to cause the reflection within the core so that the light waves are transmitted through the fibre.
3. **Jacket:** The protective coating consisting of plastic is known as a jacket. The main purpose of a jacket is to preserve the fibre strength, absorb shock and extra fibre protection.

- **Following are the advantages of fibre optic cable over copper:**

1. **Greater Bandwidth:** The fibre optic cable provides more bandwidth as compared copper. Therefore, the fibre optic carries more data as compared to copper cable.
2. **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.
3. **Longer distances:** The fibre optic cable carries the data at a longer distance as compared to copper cable.
4. **Better reliability:** The fibre optic cable is more reliable than the copper cable as it is immune to any temperature changes while it can cause obstruct in the connectivity of copper cable.
5. **Thinner and Sturdier:** Fibre optic cable is thinner and lighter in weight so it can withstand more pull pressure than copper cable.

12. UnGuided Transmission:

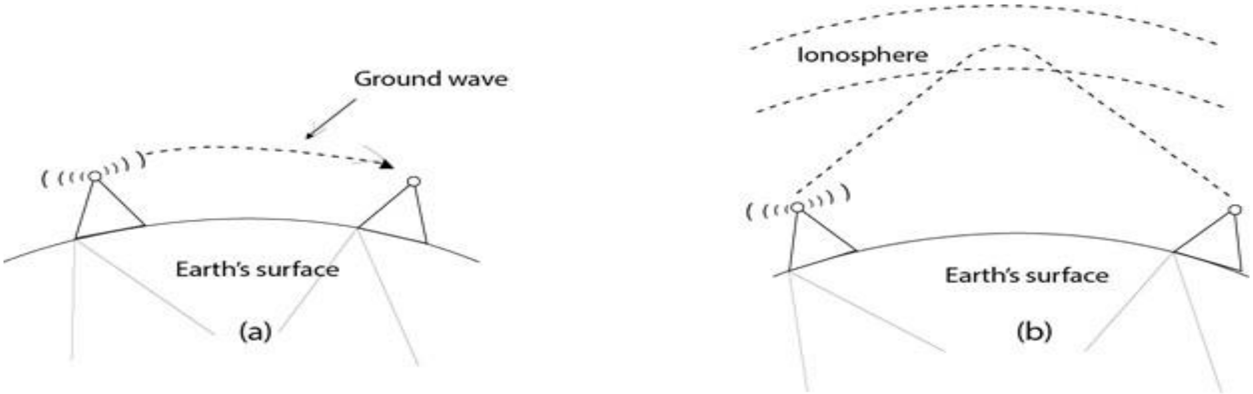
An unguided transmission transmits the electromagnetic waves without using any physical medium. Therefore it is also known as **wireless transmission**.

In unguided media, air is the media through which the electromagnetic energy can flow easily. Unguided transmission is broadly classified into three categories:

1. Radio waves:

1. Radio waves are the electromagnetic waves that are transmitted in all the directions of free space.
2. Radio waves are omnidirectional, i.e., the signals are propagated in all the directions.
3. The range in frequencies of radio waves is from 3Khz to 1 khz.
4. In the case of radio waves, the sending and receiving antenna are not aligned, i.e., the wave sent by the sending antenna can be received by any receiving antenna.

An example of the radio wave is **FM radio**.



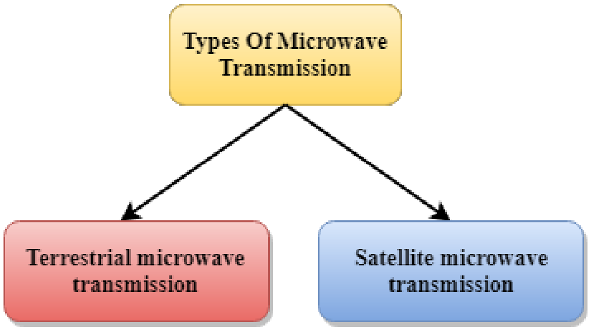
- **Applications Of Radio waves:**

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

Advantages Of Radio transmission:

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

2. Microwaves:


Types Of Microwave Transmission
Terrestrial microwave transmission
Satellite microwave transmission

Microwaves are of two types:

1. Terrestrial microwave
2. Satellite microwave communication.

1. Terrestrial Microwave Transmission:

1. Terrestrial Microwave transmission is a technology that transmits the focused beam of a radio signal from one ground-based microwave transmission antenna to another.
2. Microwaves are the electromagnetic waves having the frequency in the range from 1GHz to 1000 GHz.
3. 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.
4. In this case, antennas are mounted on the towers to send a beam to another antenna which is km away.
5. 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:

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

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

1. **Eavesdropping:** An eavesdropping creates insecure communication. Any malicious user can catch the signal in the air by using its own antenna.
2. **Out of phase signal:** A signal can be moved out of phase by using microwave transmission.
3. **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.
4. **Bandwidth limited:** Allocation of bandwidth is limited in the case of microwave transmission.

2. Satellite Microwave Communication

1. A satellite is a physical object that revolves around the earth at a known height.
2. Satellite communication is more reliable nowadays as it offers more flexibility than cable and fibre optic systems.
3. We can communicate with any point on the globe by using satellite communication.

Satellite working:

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:**

1. The coverage area of a satellite microwave is more than the terrestrial microwave.
2. The transmission cost of the satellite is independent of the distance from the centre of the coverage area.
3. Satellite communication is used in mobile and wireless communication applications.

4. It is easy to install.
5. 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:**

1. Satellite designing and development requires more time and higher cost.
2. The Satellite needs to be monitored and controlled on regular periods so that it remains in orbit.
3. 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.

3. Infrared:

1. An infrared transmission is a wireless technology used for communication over short ranges.
2. The frequency of the infrared in the range from 300 GHz to 400 THz.
3. It is used for short-range communication such as data transfer between two cell phones, TV remote operation, data transfer between a computer and cell phone resides in the same closed area.

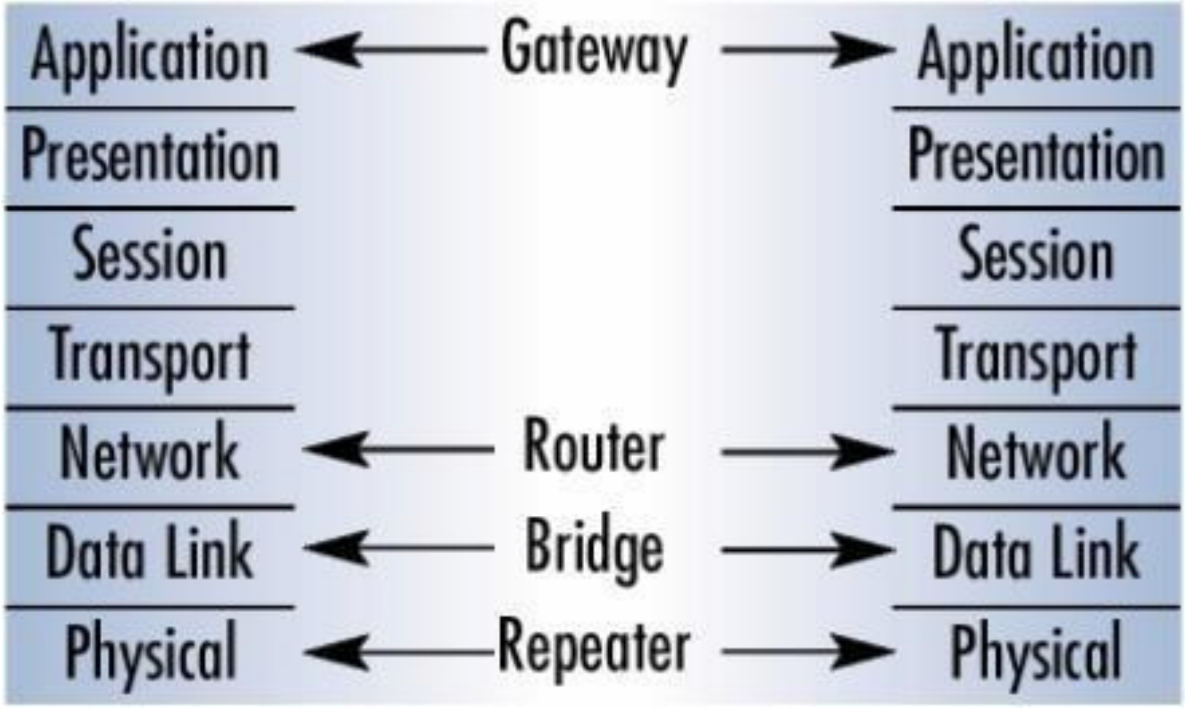
- **Characteristics Of Infrared:**

1. It supports high bandwidth, and hence the data rate will be very high.
2. Infrared waves cannot penetrate the walls. Therefore, the infrared communication in one room cannot be interrupted by the nearby rooms.
3. An infrared communication provides better security with minimum interference.
4. Infrared communication is unreliable outside the building because the sun rays will interfere with the infrared waves.

Differences among network controllers and network devices (Hub,Switch and Router)

S. No	**Hub**	**Switch**	**Router**
1.	Hub belongs to layer 1 of an OSI model that means it is a physical layer device.	Switch belongs to layer 2 of an OSI model that means it is a data link layer device.	Router belongs to layer 3 of an OSI model that means it is a network layer device.
2.	Hub prefers half-duplex transmission method.	Switch prefers full-duplex transmission method.	It is full duplex in nature.
3.	It functions based on broadcasting.	It functions based on MAC addresses.	It functions based on IP addresses.

4	Hub is commonly used to link components of a LAN	A switch is used by LAN.	A router is utilised by LAN as well as MAN.
5.	Hubs are not smart gadgets because they pass on everything obtained on one connection to all other connections.	A Switch is a smart and wise device as it gives a message to a specific device by scanning the address.	Routers are basically tiny computers that accomplish a variety of intelligent jobs. They can also help in building address tables that support routing decisions.
6.	In a hub, we need a single network to connect.	Here also, we require a single network to connect.	It demands a minimum of two networks to connect.
7.	It is inexpensive as compared to switch and ro router.	It is an expensive device than a hub.	It is a more expensive device than a hub and switch.



3.Gateway: A network gateway is a device or node that connects disparate networks by translating communications from one protocol to another.

How is a gateway different from a router:

A gateway connects networks, while a router typically delivers data within a network.

Historically, gateways and routers have been separate devices. However, it's becoming more common for their functions to be combined and simply called a router. For example, the Wi-Fi routers commonly provided for home and small business internet service are both a router (delivering data) and a gateway (translating it so destination devices can use it).

4. Bridge:A **network bridge** is a computer networking device that creates a single, aggregate network from multiple communication networks or network segments. This function is called **network bridging**.
1.) Bridging is distinct from routing. Routing allows multiple networks to communicate independently and yet remain separate, whereas bridging connects two separate networks as if they were a single network.In the OSI model, bridging is performed in the data link layer (layer 2) If one or more segments of the bridged network are wireless, the device is known as a **wireless bridge**.

5. Router:A router is a device that connects two or more packet-switched networks or subnetworks. It serves two primary functions: managing traffic between these networks by forwarding data packets to their intended IP addresses, and allowing multiple devices to use the same Internet connection.