UNIT1

Topic name: Computer networks definition,Characteristics, Network Types

1) *what do you mean by computer networks? Classify computer networks and explain them In brief.* *[7M] [R20,February2022]*

(or)

Explain different Network types *[7M] [R20, Set-I, July2023]*

(or)

Classify the networks by scale. *[8M] [R19,Set-1,July 2023]*

(or)

Classify networks by scale and explain each with figures. *[R19, Set-1,February 2022]*

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.

A computer network is a collection of two or more computer systems that are linked together. A network connection can be established using either cable or wireless media. Hardware and software are used to connect computers and tools in any network.

Local Area Network (LAN) –

LAN or Local Area Network connects network devices in such a way that personal computers and workstations can share data, tools, and programs. The group of computers and devices are connected together by a switch, or stack of switches, using a private addressing scheme as defined by the TCP/IP protocol. Private addresses are unique in relation to other computers on the local network. Routers are found at the boundary of a LAN, connecting them to the larger WAN.

Data transmits at a very fast rate as the number of computers linked is limited. By definition, the connections must be high-speed and relatively inexpensive hardware (Such as hubs, network adapters, and Ethernet cables). LANs cover a smaller geographical area (Size is limited to a few kilometres) and are privately owned. One can use it for an office building, home, hospital, school, etc. LAN is easy to design and maintain. A Communication medium used for LAN has twisted-pair cables and coaxial cables. It covers a short distance, and so the error and noise are minimized.

Early LANs had data rates in the 4 to 16 Mbps range. Today, speeds are normally 100 or 1000 Mbps. Propagation delay is very short in a LAN. The smallest LAN may only use two

computers, while larger LANs can accommodate thousands of computers. LAN has a range up to 2km. A LAN typically relies mostly on wired connections for increased speed and security, but wireless connections can also be part of a LAN. The fault tolerance of a LAN is more and there is less congestion in this network. For example A bunch of students playing Counter-Strike in the same room (without internet).

Advantages:

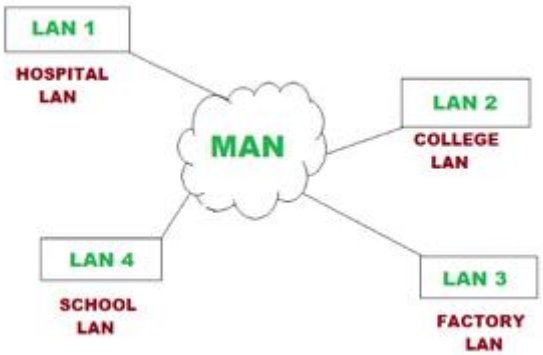
- Provides fast data transfer rates and high-speed communication.
- Easy to set up and manage.
- Can be used to share peripheral devices such as printers and scanners.
- Provides increased security and fault tolerance compared to WANs.

Disadvantages:

- Limited geographical coverage.
- Limited scalability and may require significant infrastructure upgrades to accommodate growth.
- May experience congestion and network performance issues with increased usage

Metropolitan Area Network (MAN) –

MAN or Metropolitan area Network covers a larger area than that covered by a LAN and a smaller area as compared to WAN. MAN has a range of 5-50km. It connects two or more computers that are apart but reside in the same or different cities. It covers a large geographical area and may serve as an ISP (Internet Service Provider). MAN is designed for customers who need high-speed connectivity. Speeds of MAN range in terms of Mbps. It's hard to design and maintain a Metropolitan Area Network.



The fault tolerance of a MAN is less and also there is more congestion in the network. It is costly and may or may not be owned by a single organization. The data transfer rate and the propagation delay of MAN are moderate. Devices used for transmission of data through MAN are Modem and Wire/Cable. Examples of a MAN are part of the telephone company network that can provide a high-speed DSL line to the customer or the cable TV network in a city.

Advantages:

- Provides high-speed connectivity over a larger geographical area than LAN.
- Can be used as an ISP for multiple customers.
- Offers higher data transfer rates than WAN in some cases.

Disadvantages:

- Can be expensive to set up and maintain.
- May experience congestion and network performance issues with increased usage.
- May have limited fault tolerance and security compared to LANs.

Wide Area Network (WAN) –

WAN or Wide Area Network is a computer network that extends over a large geographical area, although it might be confined within the bounds of a state or country. WAN has a range of above 50 km. A WAN could be a connection of LAN connecting to other LANs via telephone lines and radio waves and may be limited to an enterprise (a corporation or an organization) or accessible to the public. The technology is high-speed and relatively expensive.

There are two types of WAN: Switched WAN and Point-to-Point WAN. WAN is difficult to design and maintain. Similar to a MAN, the fault tolerance of a WAN is less and there is more congestion in the network. A Communication medium used for WAN is PSTN or Satellite Link. Due to long-distance transmission, the noise and error tend to be more in WAN.

WAN's data rate is slow about a 10th LAN's speed since it involves increased distance and increased number of servers and terminals etc. The speed of WAN ranges from a few kilobits per second (Kbps) to megabits per second (Mbps). Propagation delay is one of the biggest problems faced here. Devices used for the transmission of data through WAN are Optic wires, Microwaves, and Satellites. An example of a Switched WAN is the asynchronous transfer mode (ATM) network and Point-to-Point WAN is a dial-up line that connects a home computer to the Internet.

Advantages:

- Covers large geographical areas and can connect remote locations.
- Provides connectivity to the internet.
- Offers remote access to resources and applications.
- Can be used to support multiple users and applications simultaneously.

Disadvantages:

- Can be expensive to set up and maintain.
- Offers slower data transfer rates than LAN or MAN.
- May experience higher latency and longer propagation delays due to longer distances and multiple network hops.
- May have lower fault tolerance and security compared to LANs.

2) Explain in detail about LAN & WAN. What are the advantages and disadvantages?

[7M] [R16,Set-1,February 2022]

(or)

Summarize network topologies. [8M][R19, Set-1June/July-2022]

(or)

What is Network topology? List any 3 network topologies. [7M] R20,Set-1,Dec/Jan -2022-23]

In Computer Network, there are various ways through which different components are connected to one another. **Network Topology** is the way that defines the structure, and how these components are connected to each other.

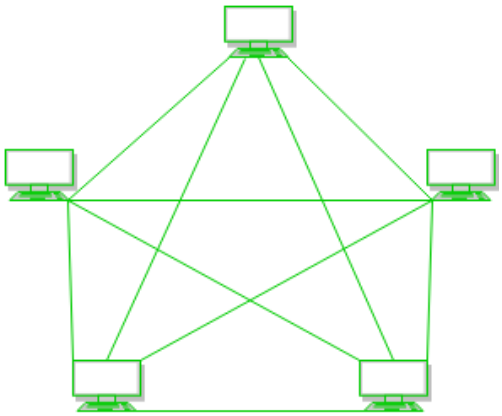
Types of Network Topology

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

- Star Topology
- Mesh Topology
- Bus Topology
- Ring Topology
- Tree Topology
- Hybrid Topology

Mesh Topology

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



Mesh Topology

Figure 1: Every device is connected to another via dedicated channels. These channels are known as links.

- Suppose, the N number of devices are connected with each other in a mesh topology, the total number of ports that are required by each device is N-1. In Figure 1, there are 5 devices connected to each other, hence the total number of ports required by each device is 4. The total number of ports required = N * (N-1).
- Suppose, N number of devices are connected with each other in a mesh topology, then the total number of dedicated links required to connect them is ${}^{N}C_{2}$ i.e. N(N-1)/2. In Figure 1, there are 5 devices connected to each other, hence the total number of links required is 5*4/2 = 10.

Advantages of Mesh Topology

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

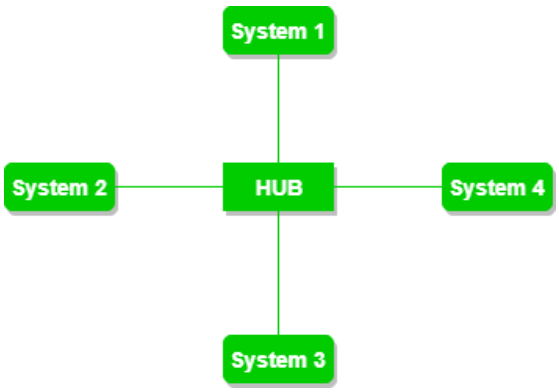
Drawbacks of Mesh Topology

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

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

Star Topology

In Star Topology, all the devices are connected to a single hub through a cable. This hub is the central node and all other nodes are connected to the central node. The hub can be passive in nature i.e., not an intelligent hub such as broadcasting devices, at the same time the hub can be intelligent known as an active hub. Active hubs have repeaters in them. Coaxial cables or RJ-45 cables are used to connect the computers. In Star Topology, many popular Ethernet LAN protocols are used as CD(Collision Detection), CSMA (Carrier Sense Multiple Access), etc.



Star Topology

Figure 2: A star topology having four systems connected to a single point of connection i.e. hub.

Advantages of Star Topology

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

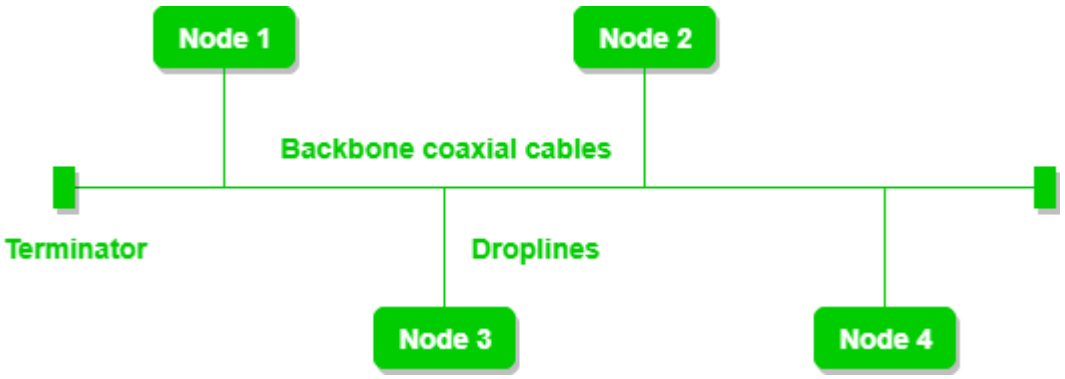
Drawbacks of Star Topology

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

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

Bus Topology

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



Bus Topology

Figure 3: A bus topology with shared backbone cable. The nodes are connected to the channel via drop lines.

Advantages of Bus Topology

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

Drawbacks of Bus Topology

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

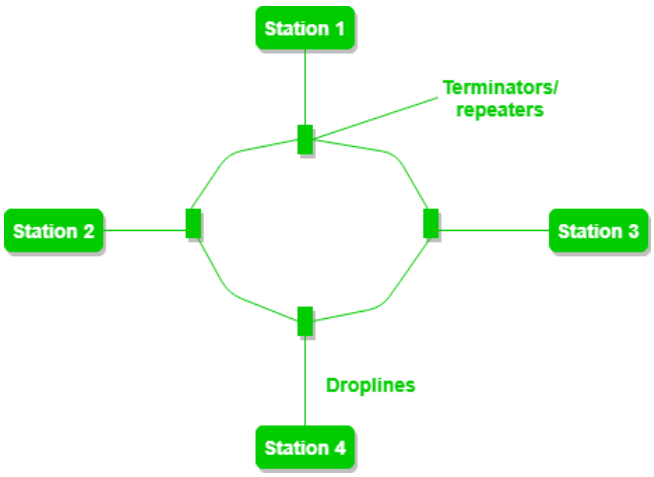
A common example of bus topology is the Ethernet LAN, where all devices are connected to a single coaxial cable or twisted pair cable. This topology is also used in cable television networks. For more,.

Ring Topology

In a Ring Topology, it forms a ring connecting devices with exactly two neighboring devices. A number of repeaters are used for Ring topology with a large number of nodes, because if someone wants to send some data to the last node in the ring topology with 100 nodes, then the data will

have to pass through 99 nodes to reach the 100th node. Hence to prevent data loss repeaters are used in the network.

The data flows in one direction, i.e. it is unidirectional, but it can be made bidirectional by having 2 connections between each Network Node, it is called Dual Ring Topology. In-Ring Topology, the Token Ring Passing protocol is used by the workstations to transmit the data.



Ring Topology

Figure 4: A ring topology comprises 4 stations connected with each forming a ring.

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

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

Operations of Ring Topology

1. One station is known as a **monitor** station which takes all the responsibility for performing the operations.
2. To transmit the data, the station has to hold the token. After the transmission is done, the token is to be released for other stations to use.
3. When no station is transmitting the data, then the token will circulate in the ring.
4. There are two types of token release techniques: **Early token release** releases the token just after transmitting the data and **Delayed token release** releases the token after the acknowledgment is received from the receiver.

Advantages of Ring Topology

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

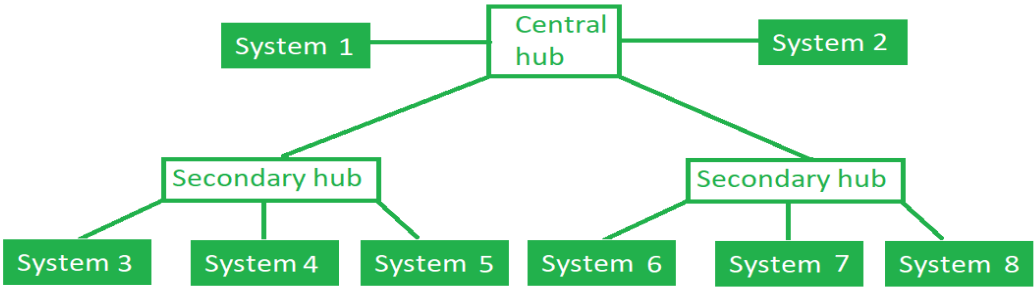
Drawbacks of Ring Topology

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

For more, refer to the Advantages and Disadvantages of Ring Topology.

Tree Topology

This topology is the variation of the Star topology. This topology has a hierarchical flow of data. In Tree Topology, protocols like DHCP and SAC (Standard Automatic Configuration) are used.



Tree Topology

Figure 5: In this, the various secondary hubs are connected to the central hub which contains the repeater. This data flow from top to bottom i.e. from the central hub to the secondary and then to the devices or from bottom to top i.e. devices to the secondary hub and then to the central hub. It is a multi-point connection and a non-robust topology because if the backbone fails the topology crashes.

Advantages of Tree Topology

- It allows more devices to be attached to a single central hub thus it decreases the distance that is traveled by the signal to come to the devices.
- It allows the network to get isolated and also prioritize from different computers.
- We can add **new devices to the existing network.**
- **Error detection** and **error correction** are very easy in a tree topology.

Drawbacks of Tree Topology

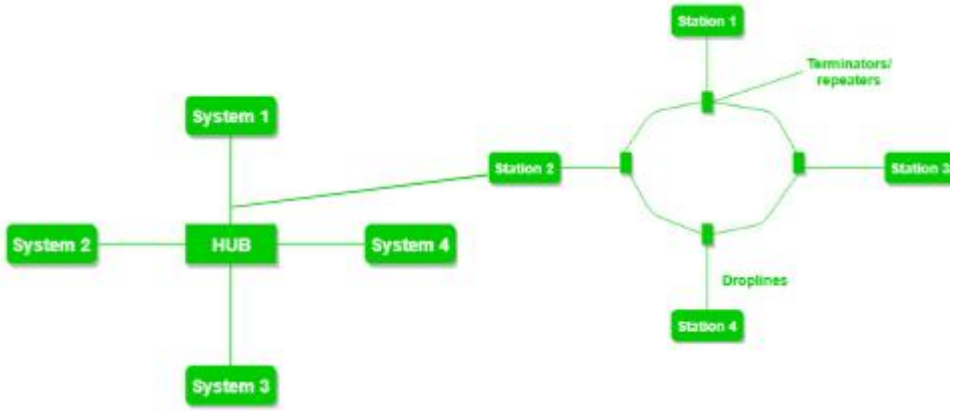
- If the central hub gets fails the entire system fails.
- The cost is high because of the cabling.
- If new devices are added, it becomes difficult to reconfigure.

A common example of a tree topology is the hierarchy in a large organization. At the top of the tree is the CEO, who is connected to the different departments or divisions (child nodes) of the

company. Each department has its own hierarchy, with managers overseeing different teams (grandchild nodes). The team members (leaf nodes) are at the bottom of the hierarchy, connected to their respective managers and departments.

Hybrid Topology

This topological technology is the combination of all the various types of topologies we have studied above. Hybrid Topology is used when the nodes are free to take any form. It means these can be individuals such as Ring or Star topology or can be a combination of various types of topologies seen above. Each individual topology uses the protocol that has been discussed earlier.



Hybrid Topology

Figure 6: The above figure shows the structure of the Hybrid topology. As seen it contains a combination of all different types of networks.

Advantages of Hybrid Topology

- This topology is **very flexible**.
- The size of the network can be easily expanded by **adding new devices.**

Drawbacks of Hybrid Topology

- It is challenging **to design the architecture** of the Hybrid Network.
- **Hubs** used in this topology are **very expensive.**
- The infrastructure cost is very high as a hybrid network **requires a lot of cabling and network devices**.

A common example of a hybrid topology is a university campus network. The network may have a backbone of a star topology, with each building connected to the backbone through a switch or router. Within each building, there may be a bus or ring topology connecting the different rooms and offices. The wireless access points also create a mesh topology for wireless devices. This hybrid topology allows for efficient communication between different buildings while providing flexibility and redundancy within each building.

Topic name: The OSI Reference Mode the TCP/IP Reference Model

3) *Explain why layered architecture is used for networks.* *[7] [R19, Set-1,February 2022]*

Or

Explain design issues for the layers in computer network. *[7M] [R19, Set-1June/July-2022]*

[8M][R19, Set-1June/July-2022]

Layering means decomposing the problem into more manageable components or layers. It means decomposing. Decomposing means breaking a big problem into smaller problems. For example, if we are supposed to solve a big problem, instead of solving a big problem at once, we can break the big problem into smaller problems. If we solve all smaller problems, obviously the big problem solved. So, layering means decomposing the problem into more manageable components or layers which has two advantages. It provides more modular design. In computer science we know very well that modularity has its own advantages, where big problem is broken into smaller problems and we are able to solve smaller problems effectively, so that we can get the solution for the big problem. And also it is easy to troubleshoot. Suppose, if we have five layers and there is a problem in one layer, we need not go and check other layers. We can just focus on the layer which has encountered an error. So that's the power of layering.

Why do we require Layered architecture?

- **Divide-and-conquer approach:** Divide-and-conquer approach makes a design process in such a way that the unmanageable tasks are divided into small and manageable tasks. In short, we can say that this approach reduces the complexity of the design.
- **Modularity:** Layered architecture is more modular. Modularity provides the independence of layers, which is easier to understand and implement.
- **Easy to modify:** It ensures the independence of layers so that implementation in one layer can be changed without affecting other layers.
- **Easy to test:** Each layer of the layered architecture can be analyzed and tested individuall

4) Discuss functionalities of different layers of OSI reference model.

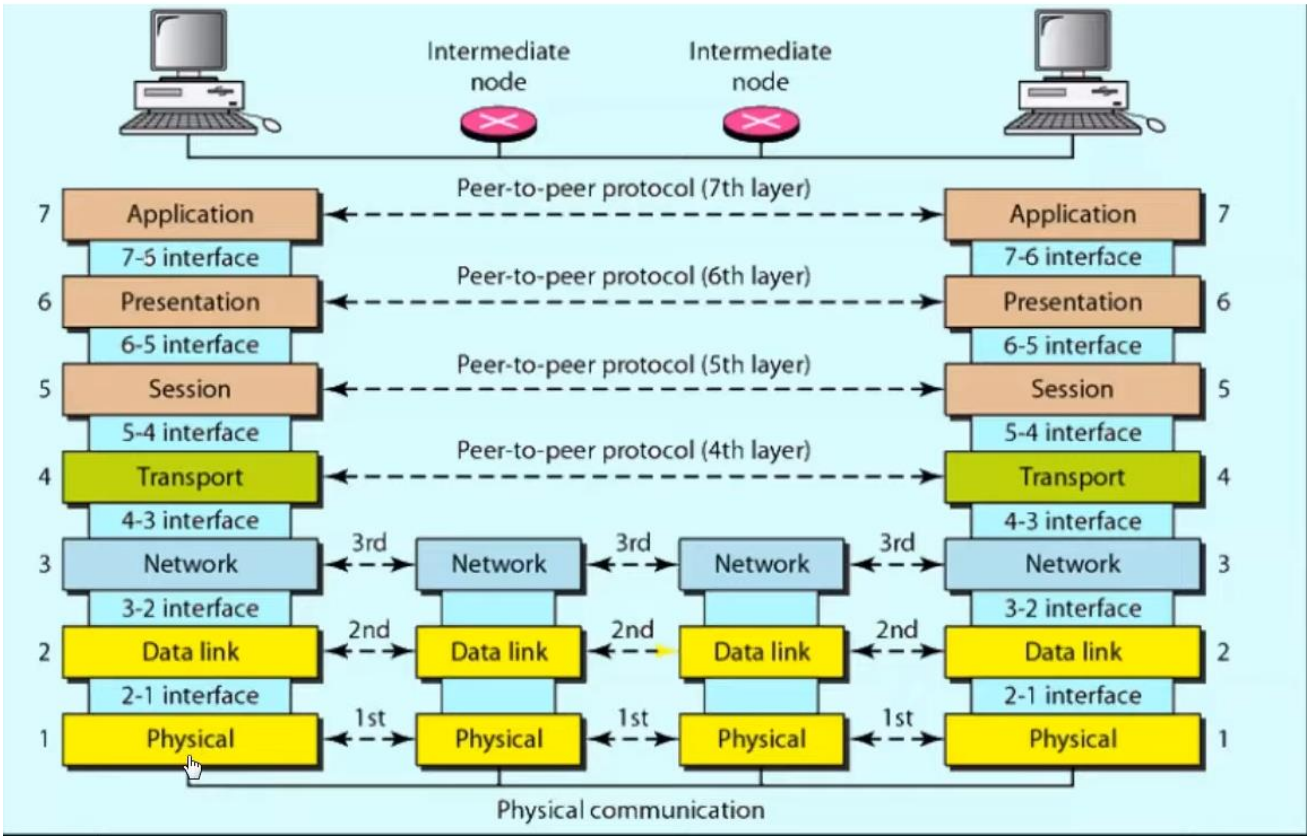
[7] [R19, Set-1,February 2022] [7] R20,Set-1,Dec/Jan -2022-23]

(Or)

Discuss functionalities of different layers of OSI reference model.

[7] [R19, Set-1,February 2022] [7] R20,Set-1,Dec/Jan -2022-23]

OSI stands for **Open Systems Interconnection**. It has been developed by ISO – '**International Organization for Standardization**', in the year 1984. It is a 7-layer architecture with each layer having specific functionality to perform. All these 7 layers work collaboratively to transmit the data from one person to another across the globe.

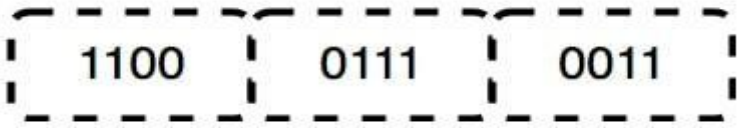


Layers of OSI Model

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

Layer 1- Physical Layer

The lowest layer of the OSI reference model is the physical layer. It is responsible for the actual physical connection between the devices. The physical layer contains information in the form of **bits.** It is responsible for transmitting individual bits from one node to the next. When receiving data, this layer will get the signal received and convert it into 0s and 1s and send them to the Data Link layer, which will put the frame back together.



Data Bits in the Physical Layer

The Functions of the Physical Layer

- **Bit synchronization:** The physical layer provides the synchronization of the bits by providing a clock. This clock controls both sender and receiver thus providing synchronization at the bit level.
- **Bit rate control:** The Physical layer also defines the transmission rate i.e. the number of bits sent per second.
- **Physical topologies:** Physical layer specifies how the different, devices/nodes are arranged in a network i.e. bus, star, or mesh topology.
- **Transmission mode:** Physical layer also defines how the data flows between the two connected devices. The various transmission modes possible are Simplex, half-duplex and full-duplex.

Note: 1. Hub, Repeater, Modem, and Cables are Physical Layer devices.

2. Network Layer, Data Link Layer, and Physical Layer are also known as **Lower Layers** or **Hardware Layers**.

Layer 2- Data Link Layer (DLL)

The data link layer is responsible for the node-to-node delivery of the message. The main function of this layer is to make sure data transfer is error-free from one node to another, over the physical layer. When a packet arrives in a network, it is the responsibility of the DLL to transmit it to the Host using its MAC address.

The Data Link Layer is divided into two sublayers:

1. Logical Link Control (LLC)
2. Media Access Control (MAC)

The packet received from the Network layer is further divided into frames depending on the frame size of the NIC(Network Interface Card). DLL also encapsulates Sender and Receiver's MAC address in the header.

The Receiver's MAC address is obtained by placing an ARP(Address Resolution Protocol) request onto the wire asking "Who has that IP address?" and the destination host will reply with its MAC address.

The Functions of the Data Link Layer

- **Framing:** Framing is a function of the data link layer. It provides a way for a sender to transmit a set of bits that are meaningful to the receiver. This can be accomplished by attaching special bit patterns to the beginning and end of the frame.
- **Physical addressing:** After creating frames, the Data link layer adds physical addresses (MAC addresses) of the sender and/or receiver in the header of each frame.
- **Error control:** The data link layer provides the mechanism of error control in which it detects and retransmits damaged or lost frames.
- **Flow Control:** The data rate must be constant on both sides else the data may get corrupted thus, flow control coordinates the amount of data that can be sent before receiving an acknowledgment.
- **Access control:** When a single communication channel is shared by multiple devices, the MAC sub-layer of the data link layer helps to determine which device has control over the channel at a given time.

Function of DLL

Note: 1. Packet in the Data Link layer is referred to as **Frame.**

2. Data Link layer is handled by the NIC (Network Interface Card) and device drivers of host machines.

3. Switch & Bridge are Data Link Layer devices.

Layer 3- Network Layer

The network layer works for the transmission of data from one host to the other located in different networks. It also takes care of packet routing i.e. selection of the shortest path to transmit the packet, from the number of routes available. The sender & receiver's IP addresses are placed in the header by the network layer.

The Functions of the Network Layer

- **Routing:** The network layer protocols determine which route is suitable from source to destination. This function of the network layer is known as routing.

- **Logical Addressing:** To identify each device on Internetwork uniquely, the network layer defines an addressing scheme. The sender & receiver's IP addresses are placed in the header by the network layer. Such an address distinguishes each device uniquely and universally.

Note: 1. Segment in the Network layer is referred to as **Packet**.

2. Network layer is implemented by networking devices such as routers and switches.

Layer 4- Transport Layer

The transport layer provides services to the application layer and takes services from the network layer. The data in the transport layer is referred to as *Segments*. It is responsible for the End to End Delivery of the complete message. The transport layer also provides the acknowledgment of the successful data transmission and re-transmits the data if an error is found.

At the sender's side: The transport layer receives the formatted data from the upper layers, performs **Segmentation**, and also implements **Flow & Error control** to ensure proper data transmission. It also adds Source and Destination port numbers in its header and forwards the segmented data to the Network Layer.

Note: The sender needs to know the port number associated with the receiver's application.

Generally, this destination port number is configured, either by default or manually. For example, when a web application requests a web server, it typically uses port number 80, because this is the default port assigned to web applications. Many applications have default ports assigned.

At the receiver's side: Transport Layer reads the port number from its header and forwards the Data which it has received to the respective application. It also performs sequencing and reassembling of the segmented data.

The Functions of the Transport Layer

- **Segmentation and Reassembly:** This layer accepts the message from the (session) layer, and breaks the message into smaller units. Each of the segments produced has a header associated with it. The transport layer at the destination station reassembles the message.
- **Service Point Addressing:** To deliver the message to the correct process, the transport layer header includes a type of address called service point address or port address. Thus by specifying this address, the transport layer makes sure that the message is delivered to the correct process.

Services Provided by Transport Layer

1. Connection-Oriented Service
2. Connectionless Service

1. Connection-Oriented Service: It is a three-phase process that includes

- Connection Establishment
- Data Transfer
- Termination/disconnection

In this type of transmission, the receiving device sends an acknowledgment, back to the source after a packet or group of packets is received. This type of transmission is reliable and secure.

2. Connectionless service: It is a one-phase process and includes Data Transfer. In this type of transmission, the receiver does not acknowledge receipt of a packet. This approach allows for much faster communication between devices. Connection-oriented service is more reliable than connectionless Service.

Note: 1. Data in the Transport Layer is called **Segments**.

2. Transport layer is operated by the Operating System. It is a part of the OS and communicates with the Application Layer by making system calls.

3. The transport layer is called as **Heart of the OSI** model.

3. **Device or Protocol Use :** TCP, UDP NetBIOS, PPTP

Layer 5- Session Layer

This layer is responsible for the establishment of connection, maintenance of sessions, and authentication, and also ensures security.

The Functions of the Session Layer

- **Session establishment, maintenance, and termination:** The layer allows the two processes to establish, use and terminate a connection.
- **Synchronization:** This layer allows a process to add checkpoints that are considered synchronization points in the data. These synchronization points help to identify the error so that the data is re-synchronized properly, and ends of the messages are not cut prematurely and data loss is avoided.
- **Dialog Controller:** The session layer allows two systems to start communication with each other in half-duplex or full-duplex.

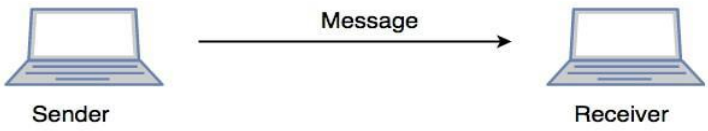
Note: 1. All the below 3 layers(including Session Layer) are integrated as a single layer in the TCP/IP model as the “Application Layer”.

2. Implementation of these 3 layers is done by the network application itself. These are also known as **Upper Layers or Software Layers.**

3. **Device or Protocol Use :** NetBIOS, PPTP

Scenario

Let us consider a scenario where a user wants to send a message through some Messenger application running in his browser. The “Messenger” here acts as the application layer which provides the user with an interface to create the data. This message or so-called Data is compressed, encrypted (if any secure data), and converted into bits (0’s and 1’s) so that it can be transmitted.



Communication in Session Layer

Layer 6- Presentation Layer

The presentation layer is also called the **Translation layer**. The data from the application layer is extracted here and manipulated as per the required format to transmit over the network.

The Functions of the Presentation Layer are

- **Translation:** For example, ASCII to EBCDIC.
- **Encryption/ Decryption:** Data encryption translates the data into another form or code. The encrypted data is known as the ciphertext and the decrypted data is known as plain text. A key value is used for encrypting as well as decrypting data.
- **Compression:** Reduces the number of bits that need to be transmitted on the network.

Note: **Device or Protocol Use :** JPEG, MPEG, GIF

Layer 7- Application Layer

At the very top of the OSI Reference Model stack of layers, we find the Application layer which is implemented by the network applications. These applications produce the data, which has to be transferred over the network. This layer also serves as a window for the application services to access the network and for displaying the received information to the user.

Example: Application – Browsers, Skype Messenger, etc.

Note: 1. The application Layer is also called Desktop Layer.

3. **Device or Protocol Use :** SMTP

The Functions of the Application Layer are

- Network Virtual Terminal: It allows a user to log on to a remote host.
- FTAM- File transfer access and management : This application allows a user to access file in a remote host, retrieve files in remote host and manage or control files from a remote computer.

- Mail Services : Provide email service.
- Directory Services : This application provides distributed database sources and access for global information about various objects and services.

OSI model acts as a reference model and is not implemented on the Internet because of its late invention. The current model being used is the TCP/IP model.

5) *Compare OSI and TCP/IP reference models.* *[8M] [R19,Set-1,July 2023]*
[7] R20,Set-1,Dec/Jan -2022-23]
[7M] [R16,Set-1,February 2022]

OSI Model	TCP/IP Model
It stands for **Open System Interconnection.**	It stands for **Transmission Control Protocol.**
OSI model has been developed by ISO (International Standard Organization).	It was developed by ARPANET (Advanced Research Project Agency Network).
It is an independent standard and generic protocol used as a communication gateway between the network and the end user.	It consists of standard protocols that lead to the development of an internet. It is a communication protocol that provides the connection among the hosts.
In the OSI model, the transport layer provides a guarantee for the delivery of the packets.	The transport layer does not provide the surety for the delivery of packets. But still, we can say that it is a reliable model.
This model is based on a vertical approach.	This model is based on a horizontal approach.
In this model, the session and presentation layers are separated, i.e., both the layers are different.	In this model, the session and presentation layer are not different layers. Both layers are included in the application layer.
It is also known as a reference model through which various networks are built. For example, the TCP/IP model is built from the OSI model. It is also referred to as a guidance tool.	It is an implemented model of an OSI model.
In this model, the network layer provides both	The network layer provides only

connection-oriented and connectionless service.	connectionless service.
Protocols in the OSI model are hidden and can be easily replaced when the technology changes.	In this model, the protocol cannot be easily replaced.
It consists of 7 layers.	It consists of 4 layers.
OSI model defines the services, protocols, and interfaces as well as provides a proper distinction between them. It is protocol independent.	In the TCP/IP model, services, protocols, and interfaces are not properly separated. It is protocol dependent.
The usage of this model is very low.	This model is highly used.
It provides standardization to the devices like router, motherboard, switches, and other hardware devices.	It does not provide the standardization to the devices. It provides a connection between various computers.

Topic name: Internet History

6) What is Internet? Discuss its history *[8][R20, Set-I, July2023]*

Internet: internet is a global network that connects billions of computers across the world with each other and to the World Wide Web. It uses standard internet protocol suite (TCP/IP) to connect billions of computer users worldwide. It is set up by using cables such as optical fibers and other wireless and networking technologies. At present, internet is the fastest mean of sending or exchanging information and data between computers across the world. It is believed that the internet was developed by "Defense Advanced Projects Agency" (DARPA) department of the United States. And, it was first connected in 1969.

Internet History: The first question that pops into your mind is probably, “Who started the internet?”. The Internet was developed by Bob Kahn and Vint Cerf in the 1970s. They began the design of what we today know as the ‘internet.’ It was the result of another research experiment which was called ARPANET, which stands for Advanced Research Projects Agency Network. This was initially supposed to be a communications system for the Defense Team of the United States of America - a network that would also survive a nuclear attack. It eventually became a successful nationwide experimental packet network. But when was the

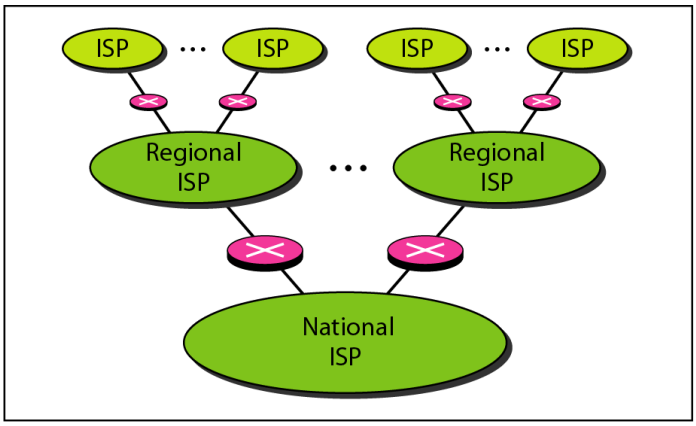
7) *explain the architecture of internet with a neat sketch [7][model paper]*

International Internet Service Providers:

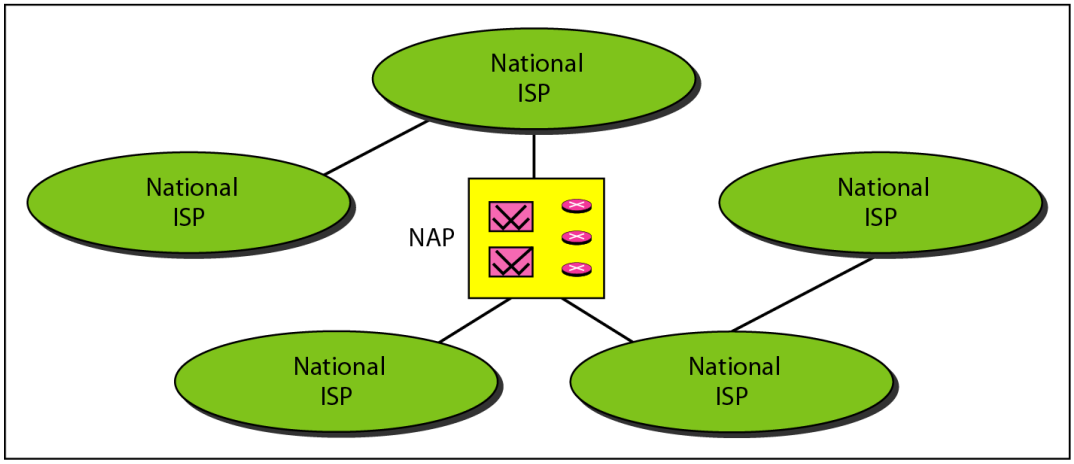
At the top of the hierarchy are the international service providers that connect nations together.

National Internet Service Providers:

The national Internet service providers are backbone networks created and maintained by specialized companies. There are many national ISPs operating in North America; some of the most well known are SprintLink, PSINet, UUNet Technology, AGIS, and internet Mel. To provide connectivity between the end users, these backbone networks are connected by complex switching stations (normally run by a third party) called network access points (NAPs). Some national ISP networks are also connected to one another by private switching stations called *peering points.* These normally operate at a high data rate (up to 600 Mbps).



a. Structure of a national ISP



b. Interconnection of national ISPs

Regional Internet Service Providers:

Regional internet service providers or regional ISPs are smaller ISPs that are connected to one or more national ISPs. They are at the third level of the hierarchy with a smaller data rate.

Local Internet Service Providers:

Local Internet service providers provide direct service to the end users. The local ISPs can be connected to regional ISPs or directly to national ISPs. Most end users are connected to the local ISPs. Note that in this sense, a local ISP can be a company that just provides Internet services, a corporation with a network that supplies services to its own employees, or a nonprofit organization, such as a college or a university, that runs its own network. Each of these local ISPs can be connected to a regional or national service provider.

8) Classify internet, intranet and extranet with applications [7M] [R19, Set-1June/July-2022]

1. Internet :

The network formed by the co-operative interconnection of millions of computers, linked together is called Internet. Internet comprises of :

- **People :** People use and develop the network.
- **Resources :** A collection of resources that can be reached from those networks.
- **A setup for collaboration :** It includes the member of the research and educational committees worldwide.

2. Intranet :

It is an internal private network built within an organization using Internet and World Wide Web standards and products that allows employees of an organization to gain access to corporate information.

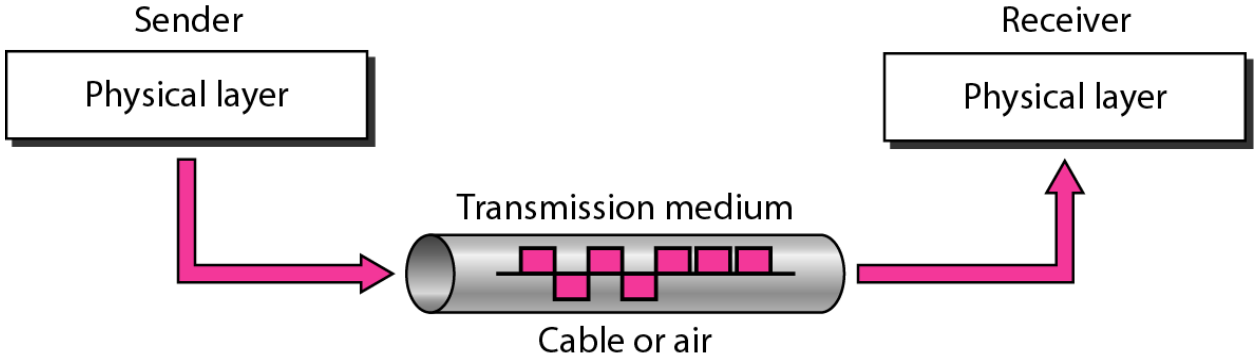
3. Extranet :

It is the type of network that allows users from outside to access the Intranet of an organization.

Internet	**Intranet**	**Extranet**
Internet is open to the public, but the other two are heavily censored.	An intranet may be accessed via the Internet, although its authentication requires logging in.	Extranets are mostly used by businesses and organizations to limit access to secret information.
It is owned by no one.	It is owned by a particular company/ organization.	It is owned by single/ multiple organizations.
Everyone who is linked has access to it.	Only members of the organization have access to it.	Only members of the organization and external members with logins have access.
Its goal is to provide information all across the world.	Its goal is to communicate information within the company.	Its goal is to allow members and external members to share information.
It is used by the public.	It is used by employees of the organization.	It is used by the members having login information.
It is more cost-effective to utilize.	It is less cost-effective.	It is also less cost-effective.

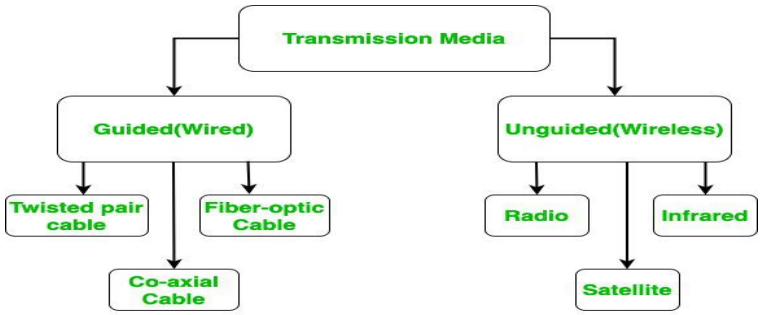
Topic name: Guided Media,unguided media- **Twisted-pair cable, Coaxial cable and Fiber optic cable and unguided media: Wireless-Radio waves, microwaves, infrared.**

9) Describe the Transmission media. Explain the ***Twisted Pair Cable****? [7][model paper]*



Transmission medium and physical layer

In data communication terminology, a transmission medium is a physical path between the transmitter and the receiver i.e. it is the channel through which data is sent from one place to another. Transmission Media is broadly classified into the following types:



1. Guided Media: It is also referred to as Wired or Bounded transmission media. Signals being transmitted are directed and confined in a narrow pathway by using physical links.

Features:

- High Speed
- Secure
- Used for comparatively shorter distances

There are 3 major types of Guided Media:

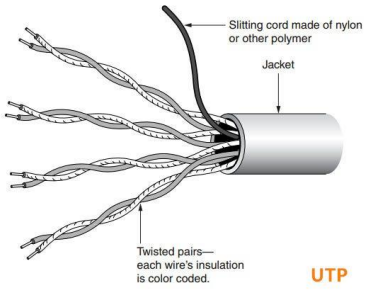
(i) Twisted Pair Cable –

It consists of 2 separately insulated conductor wires wound about each other. Generally, several such pairs are bundled together in a protective sheath. They are the most widely used Transmission Media. Twisted Pair is of two types:

- **Unshielded Twisted Pair (UTP):**

  UTP consists of two insulated copper wires twisted around one another. This type of cable has the

ability to block interference and does not depend on a physical shield for this purpose. It is used for telephonic applications.



Advantages:

⇢ Least expensive

⇢ Easy to install

⇢ High-speed capacity

Disadvantages:

⇢ Susceptible to external interference

⇢ Lower capacity and performance in comparison to STP

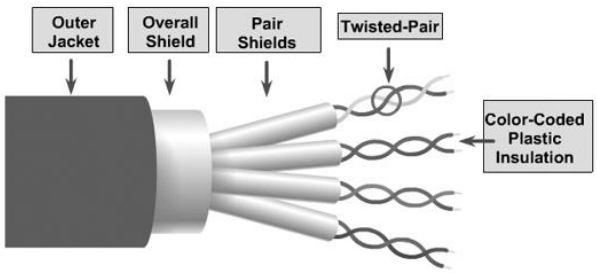
⇢ Short distance transmission due to attenuation

Applications:

Used in telephone connections and LAN networks

- **Shielded Twisted Pair (STP):**

  This type of cable consists of a special jacket (a copper braid covering or a foil shield) to block external interference. It is used in fast-data-rate Ethernet and in voice and data channels of telephone lines.



Advantages:

⇢ Better performance at a higher data rate in comparison to UTP

⇢ Eliminates crosstalk

⇢ Comparatively faster

Disadvantages:

⇢ Comparatively difficult to install and manufacture

⇢ More expensive

⇢ Bulky

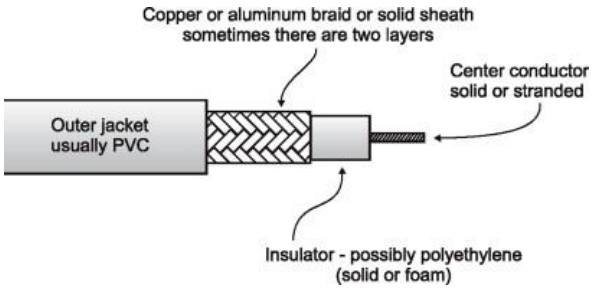
Applications:

The shielded twisted pair type of cable is most frequently used in extremely cold climates, where the additional layer of outer covering makes it perfect for withstanding such temperatures or for shielding the interior components.

10) Discuss Coaxial cable and Fiber optical cable of guided media [R20, Set-I, July2023]

Coaxial Cable –

It has an outer plastic covering containing an insulation layer made of PVC or Teflon and 2 parallel conductors each having a separate insulated protection cover. The coaxial cable transmits information in two modes: Baseband mode(dedicated cable bandwidth) and Broadband mode(cable bandwidth is split into separate ranges). Cable TVs and analog television networks widely use Coaxial cables.



Advantages:

- High Bandwidth
- Better noise Immunity
- Easy to install and expand
- Inexpensive

Disadvantages:

- Single cable failure can disrupt the entire network

Applications:

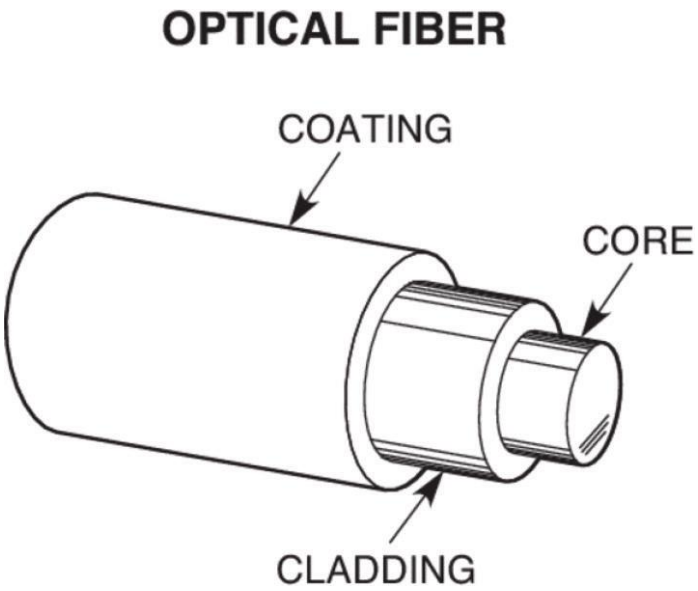
Radio frequency signals are sent over coaxial wire. It can be used for cable television signal distribution, digital audio (S/PDIF), computer network connections (like Ethernet), and feedlines that connect radio transmitters and receivers to their antennas.

(iii) Optical Fiber Cable –

It uses the concept of refraction of light through a core made up of glass or plastic. The core is

surrounded by a less dense glass or plastic covering called the cladding. It is used for the transmission of large volumes of data.

The cable can be unidirectional or bidirectional. The WDM (Wavelength Division Multiplexer) supports two modes, namely unidirectional and bidirectional mode.



Advantages:

- Increased capacity and bandwidth
- Lightweight
- Less signal attenuation
- Immunity to electromagnetic interference
- Resistance to corrosive materials

Disadvantages:

- Difficult to install and maintain
- High cost
- Fragile

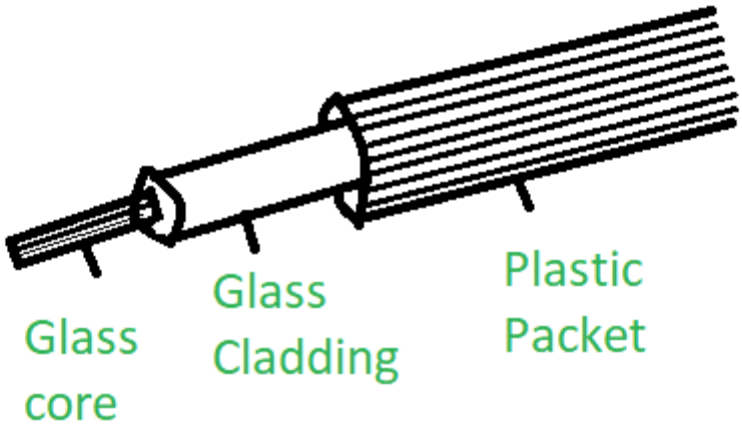
Applications:

- Medical Purpose: Used in several types of medical instruments.
- Defence Purpose: Used in transmission of data in aerospace.
- For Communication: This is largely used in formation of internet cables.
- Industrial Purpose: Used for lighting purposes and safety measures in designing the interior and exterior of automobiles.

11) Explain about Fiber optic cable? What are the types of Fiber optic cable?

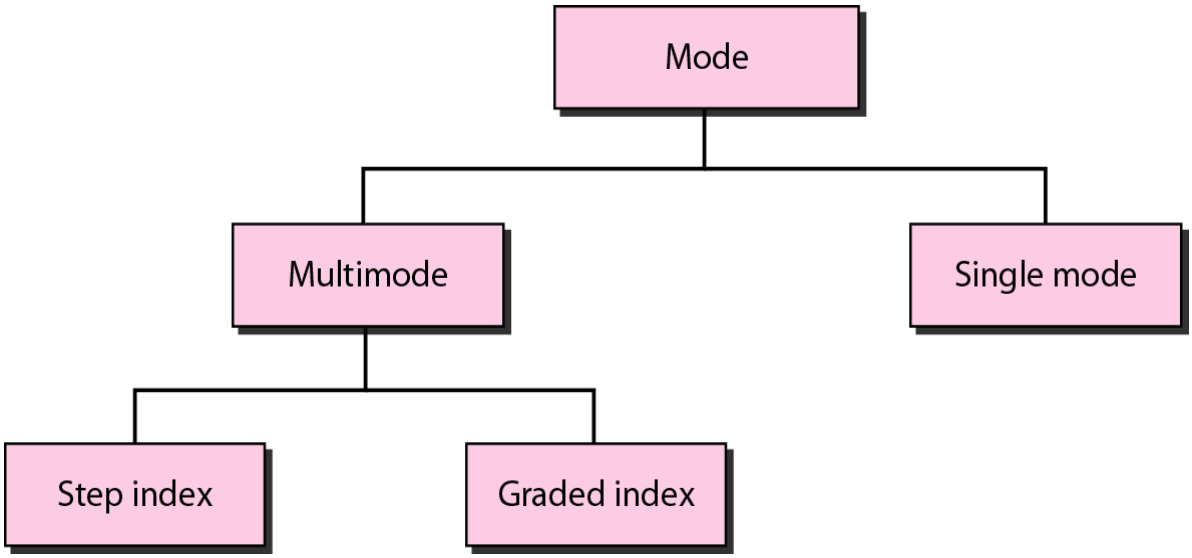
[7] R20,Set-1,Dec/Jan -2022-23]

An **Optical Fiber** is a cylindrical fiber of glass which is hair thin size or any transparent dielectric medium. The fiber which is used for optical communication is waveguides made of transparent dielectrics.



Main element of Fiber Optics:

1. **Core:**
   It is the central tube of very thin size made of optically transparent dielectric medium and carries the light transmitter to receiver and the core diameter may vary from about 5um to 100 um.
2. **Cladding:**
   It is outer optical material surrounding the core having reflecting index lower than core and cladding helps to keep the light within the core throughout the phenomena of total internal reflection.
3. **Buffer Coating:**
   It is a plastic coating that protects the fiber made of silicon rubber. The typical diameter of the fiber after the coating is 250-3



Types of Fiber optics:

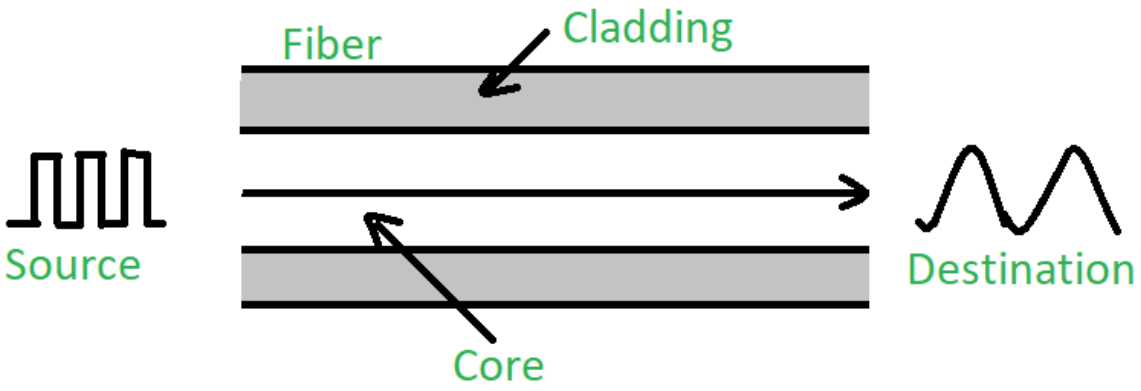
Generally optical fiber is classified into two categories based on: *the number of modes, and the refractive index*. These are explained as following below.

1. On the basis of the Number of Modes:

It is classified into 2 types:

- **(a). Single-mode fiber:**

  In single-mode fiber, only one type of ray of light can propagate through the fiber. This type of fiber has a small core diameter (5um) and high cladding diameter (70um) and the difference between the refractive index of core and cladding is very small. There is no dispersion i.e. no degradation of the signal during traveling through the fiber. The light is passed through it through a laser diode.



- **(b). Multi-mode fiber:**

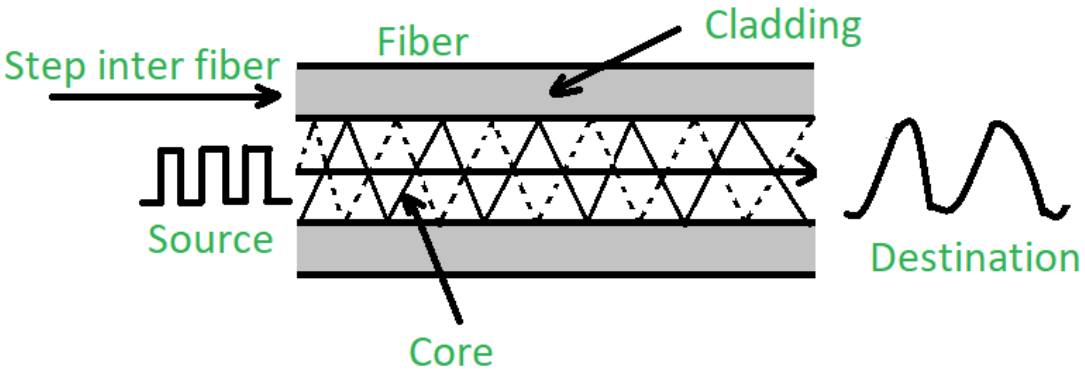
  Multimode fiber allows a large number of modes for the light ray traveling through it. The core diameter is generally (40um) and that of cladding is (70um). The relative refractive index difference is also greater than single mode fiber. There is signal degradation due to multimode dispersion. It is not suitable for long-distance communication due to large dispersion and attenuation of the signal.There are two categories on the basis of Multi-mode fiber i.e.**Step Index Fiber** and **Graded Index Fiber**.Basically these are categories under the types of optical fiber on the basis of Refractive Index

2. On the basis of Refractive Index:

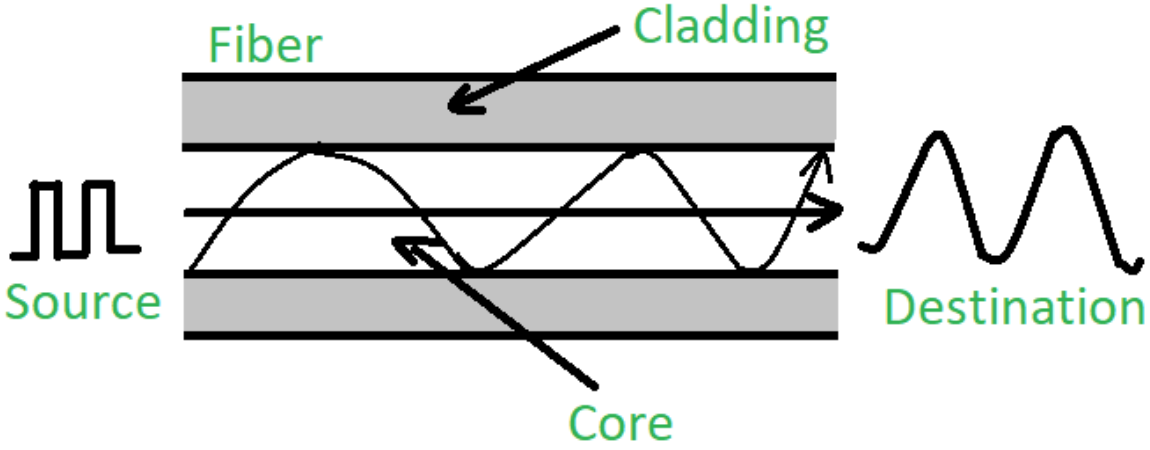
It is also classified into 2 types:

- **(a). Step-index optical fiber:**

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



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



12) Explain Wireless Radio waves and microwaves of unguided media

[R20, Set-I, July2023]

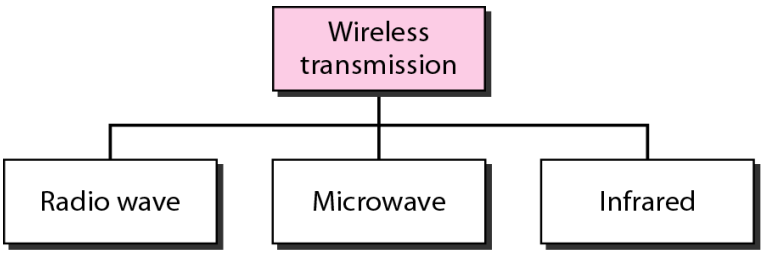
Unguided Media:

It is also referred to as Wireless or Unbounded transmission media. No physical medium is required for the transmission of electromagnetic signals.

Features:

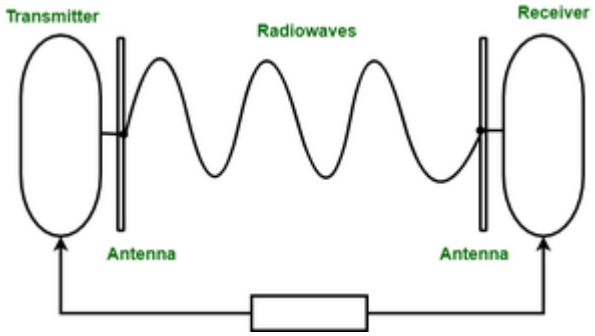
- The signal is broadcasted through air
- Less Secure
- Used for larger distances

There are 3 types of Signals transmitted through unguided media:



(i) Radio waves –

These are easy to generate and can penetrate through buildings. The sending and receiving antennas need not be aligned. Frequency Range:3KHz – 1GHz. AM and FM radios and cordless phones use Radio waves for transmission. **Radio waves are used for multicast communications, such as radio and television, and paging systems.**



Further Categorized as (i) Terrestrial and (ii) Satellite.

(ii) Microwaves –

It is a line of sight transmission i.e. the sending and receiving antennas need to be properly aligned with each other. The distance covered by the signal is directly proportional to the height of the antenna. Frequency Range:1GHz – 300GHz. These are majorly used for mobile phone communication and television distribution.**Microwaves are used for unicast communication such as cellular telephones, satellite networks, and wireless LANs.**

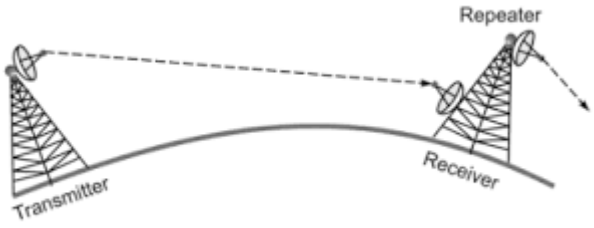


Fig: Microwave Transmission

Microwave Transmission

(iii) Infrared –

Infrared waves are used for very short distance communication. They cannot penetrate through obstacles. This prevents interference between systems. Frequency Range:300GHz – 400THz. It is

used in TV remotes, wireless mouse, keyboard, printer, etc. **Infrared signals can be used for short-range communication in a closed area using line-of-sight propagation.**

13) Distinguish between wired and wireless LANs. [7M] [R19,Set-1,July 2023]

LAN	WLAN
LAN stands for Local Area Network.	WLAN stands for Wireless Local Area Network.
LAN connections include both wired and wireless connections.	WLAN connections are completely wireless.
LAN network is a collection of computers or other such network devices in a particular location that are connected together by communication elements or network elements.	WLAN network is a collection of computers or other such network devices in a particular location that are connected together wirelessly by communication elements or network elements.
LAN is free from external attacks like interruption of signals, cyber criminal attacks and so on.	Whereas, WLAN is vulnerable to external attacks.
LAN is secure.	WLAN is not secure.
LAN network has lost its popularity due to the arrival of latest wireless networks.	WLAN is popular.
Wired LAN needs physical access like connecting the wires to the switches or routers.	Work on connecting wires to the switches and routers are neglected.
In LAN, devices are connected locally with Ethernet cable.	For WLAN Ethernet cable is not necessary.
Mobility limited.	Outstanding mobility.
It may or may not vary with external factors like environment and quality of cables.	It varies due to external factors like environment and quality of cables. Most of the external factors affect the signal transmission.
LAN is less expensive.	WLAN is more expensive.
Example: Computers connected in a college.	Example: Laptops, cellphones, tablets connected to a wireless router or hotspot.