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.

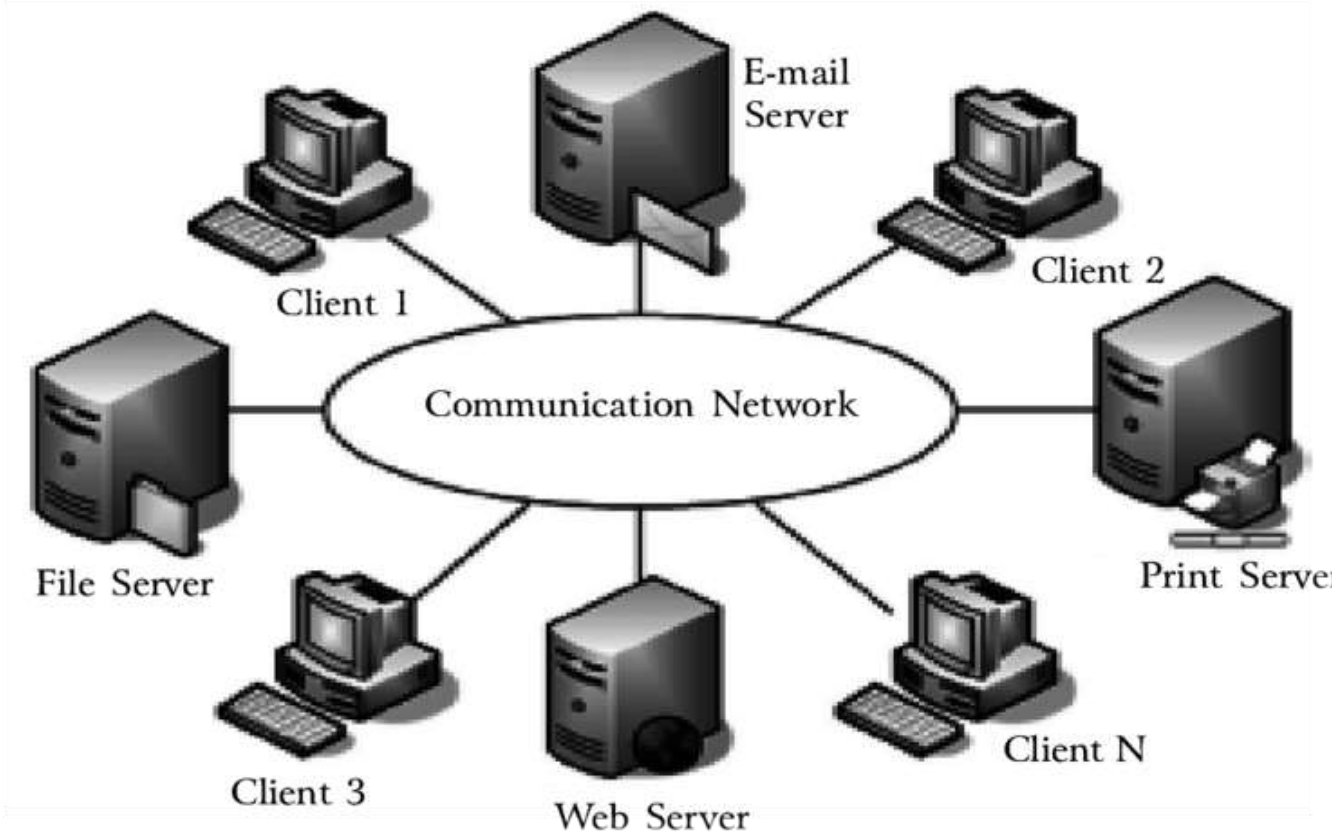
Physical Layer –Introduction to Guided Media- Twisted-pair cable, Coaxial cable and Fiber optic cable and introduction about unguided media.

What is Computer Network?

- A computer network is a set of nodes connected by communication links

OR

- A computer network is a set of computers connected together and able to exchange information with one another.
- Nodes – computer, printer, server, laptop, mobile, cell tower, router, bridge or switch, etc
- Communication links– wired or wireless



Source: Saxena and Arora (2009)

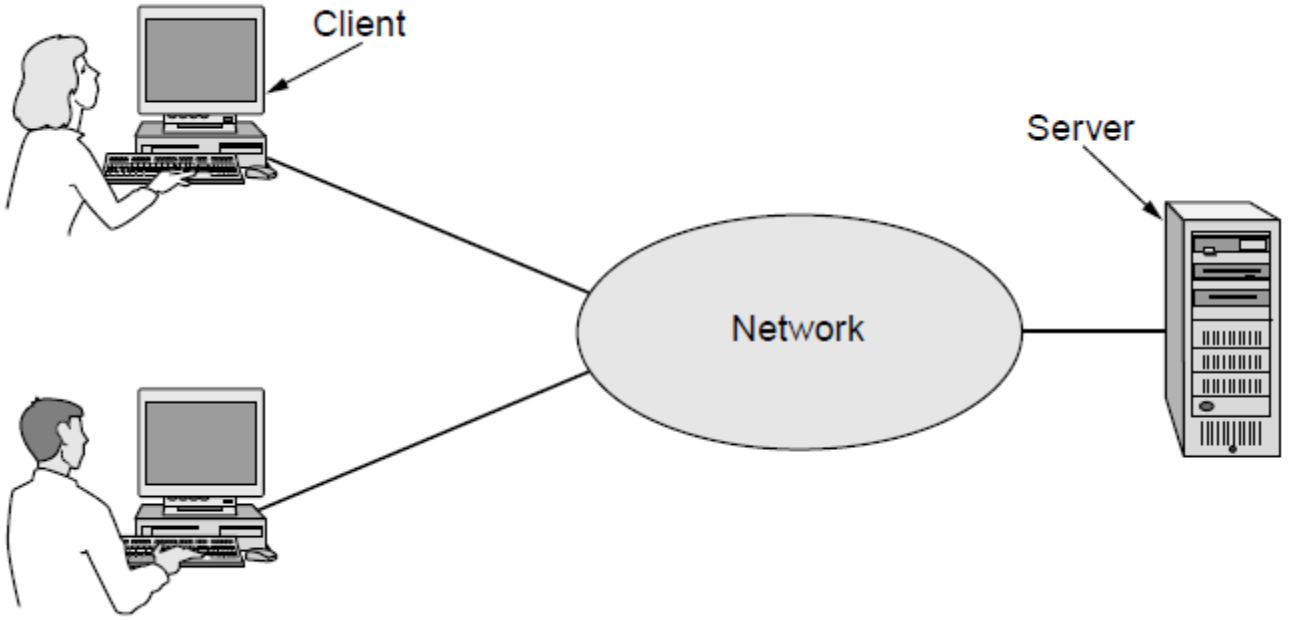
Applications

- Business Applications
- Home Applications
- Mobile Users Applications

Business Applications

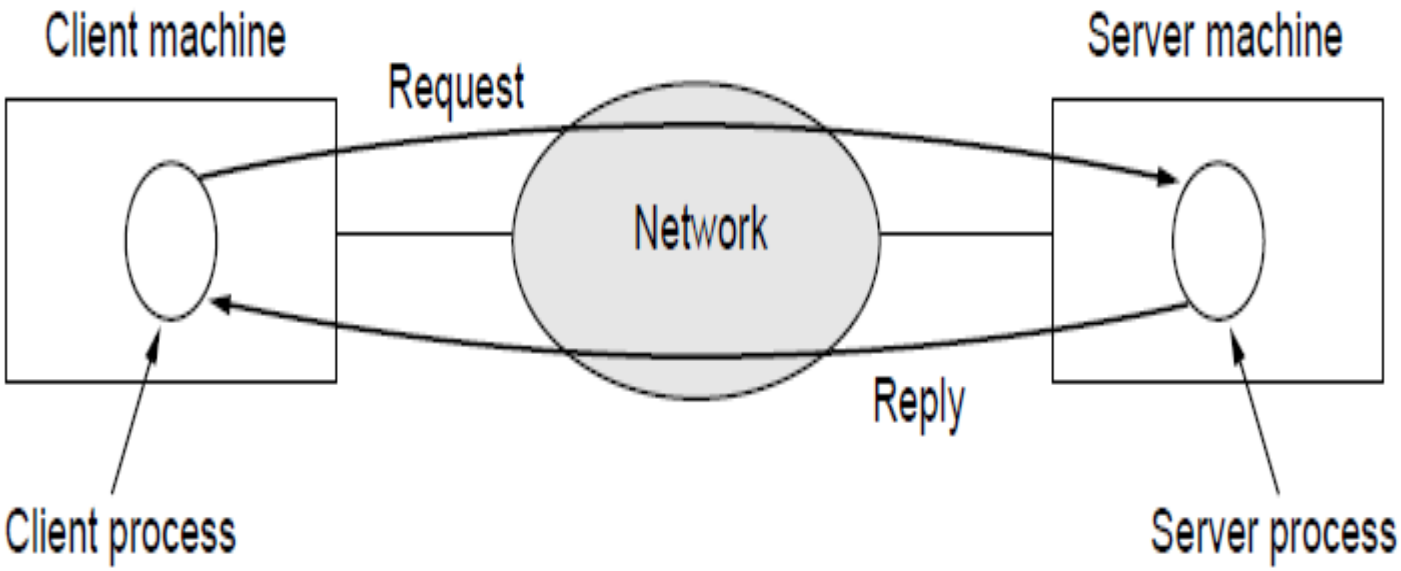
- Resource sharing
  - Hardware and Data
  - VPN, Client-Server
- Communication Medium
  - E-mail, VoIP, Desktop Sharing
- E-commerce
  - Airlines, Book Stores, Other Online Retail stores

Business Applications



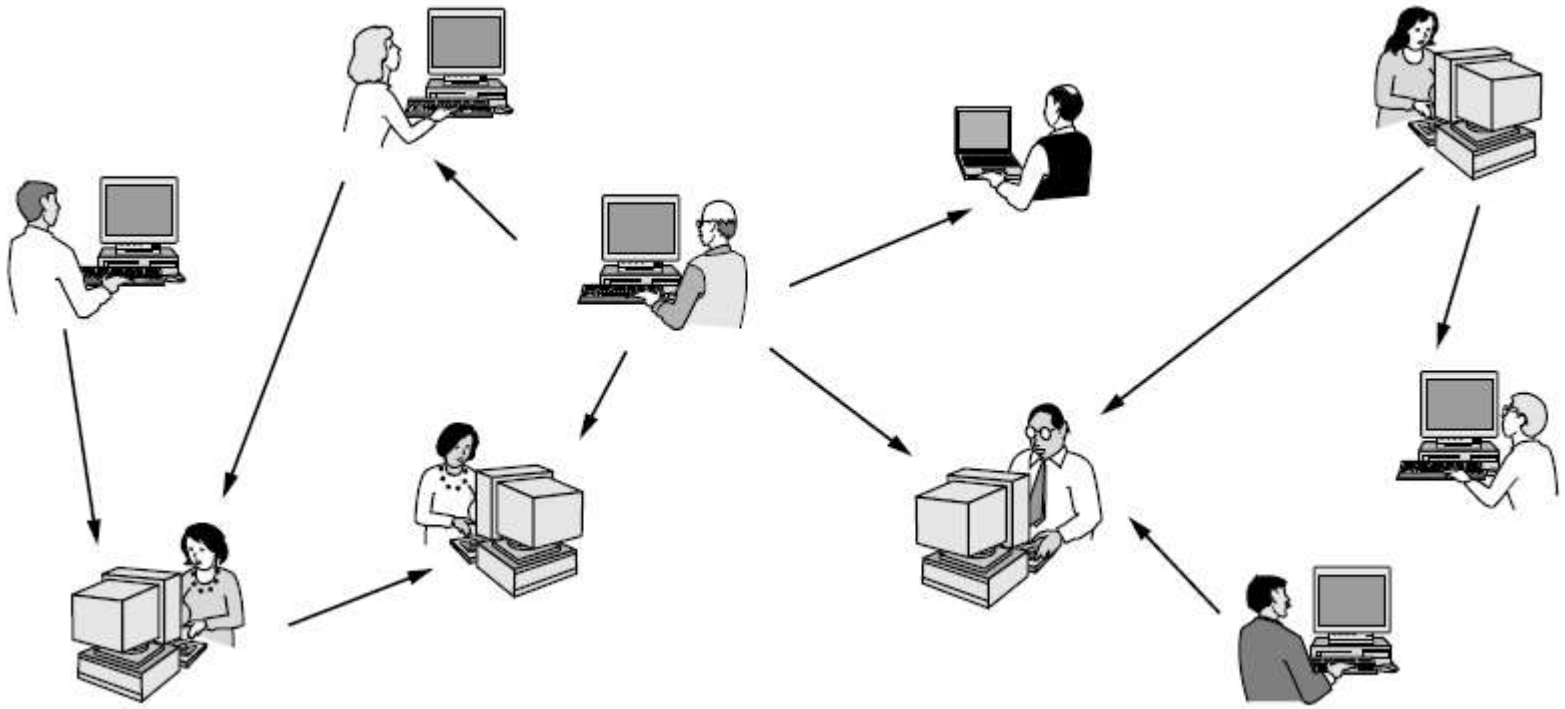
A network with two clients and one server

Business Applications



The client-server model involves requests and replies

Home Applications



In a peer-to-peer system there are no fixed clients and servers

Types of Network

- Personal Area Networks
- Local Area Networks
- Metropolitan Area Networks
- Wide Area Networks
- Campus Area Networks
- Virtual Private Networks

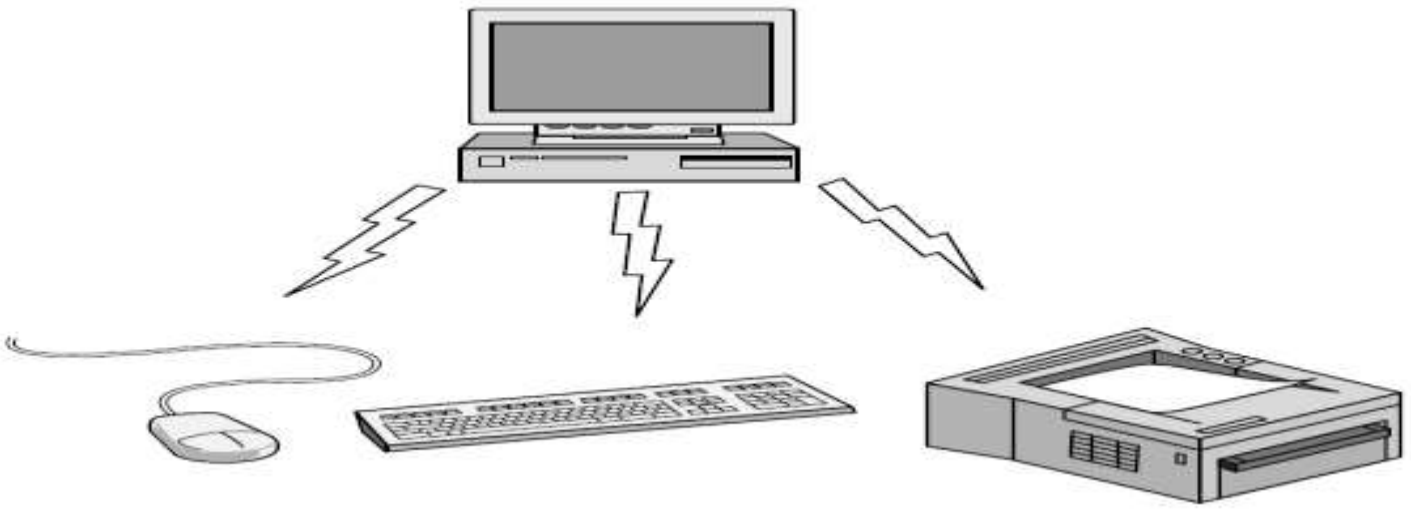
Types of Networks (2)

Interprocessor distance	Processors located in same	Example
1 m	Square meter	Personal area network
10 m	Room	Local area network
100 m	Building	
1 km	Campus	
10 km	City	Metropolitan area network
100 km	Country	Wide area network
1000 km	Continent	
10,000 km	Planet	The Internet

Classification of interconnected processors by scale.

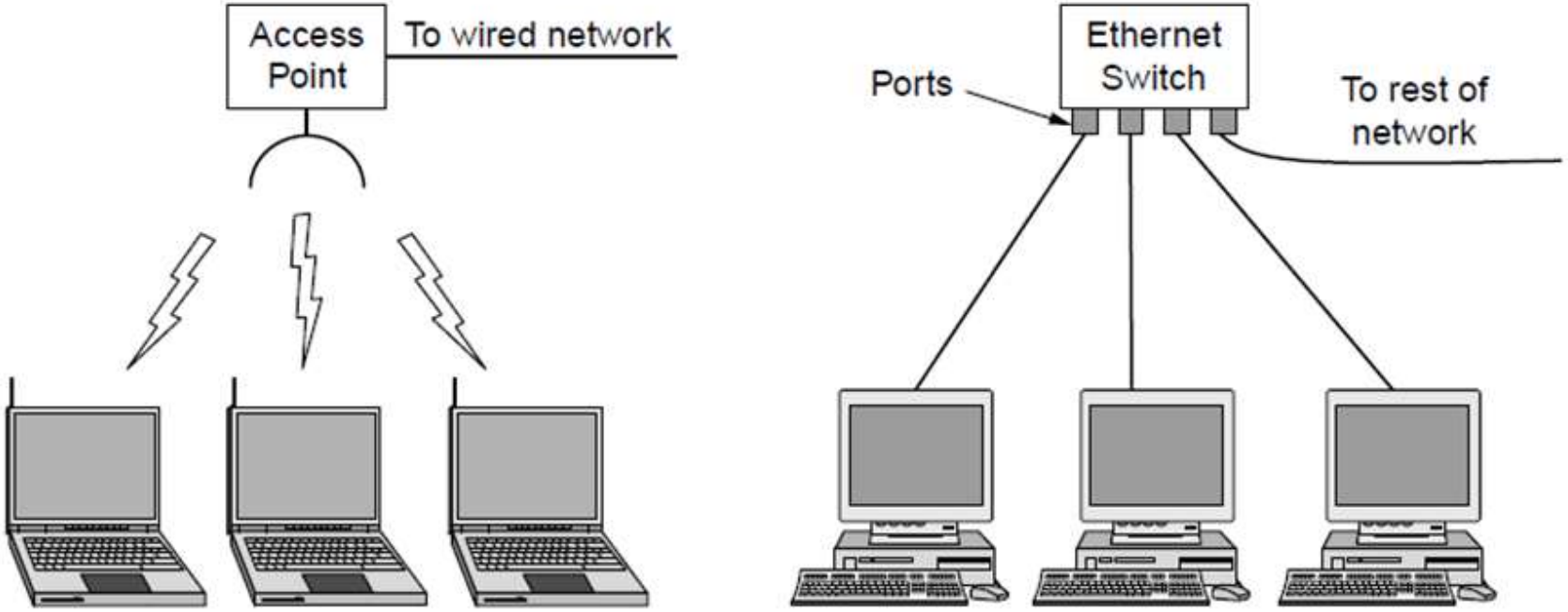
Personal Area Network

- PANs (Personal Area Networks) let devices communicate over the range of a person.
  - Wired
  - Wireless
    - Bluetooth
    - RFID(Radio-frequency Identification)



Bluetooth PAN configuration

Local Area Networks



Wireless and wired LANs. (a) 802.11. (b) Switched Ethernet.

Local Area Networks

- Local Area Network is a group of computers connected to each other in a small area such as building, office.
- LAN is used for connecting two or more personal computers through a communication medium such as twisted pair, coaxial cable, etc.
- It is less costly as it is built with inexpensive hardware such as hubs, network adapters, and Ethernet cables.
- The data is transferred at an extremely faster rate in Local Area Network.
- Local Area Network provides higher security.

Local Area Networks

- A LAN (Local Area Network) is a privately owned network that operates within and nearby a single building like a home, office or factory.
- When LANs are used by companies, they are called **enterprise networks**.
- Wired LANs: Generally uses copper wires, older ones operate at **100 Mbps to 1 Gbps**, newer can operate **upto 10Gbps**.
- Wireless LANs are very popular these days that uses: AP (Access Point), wireless router

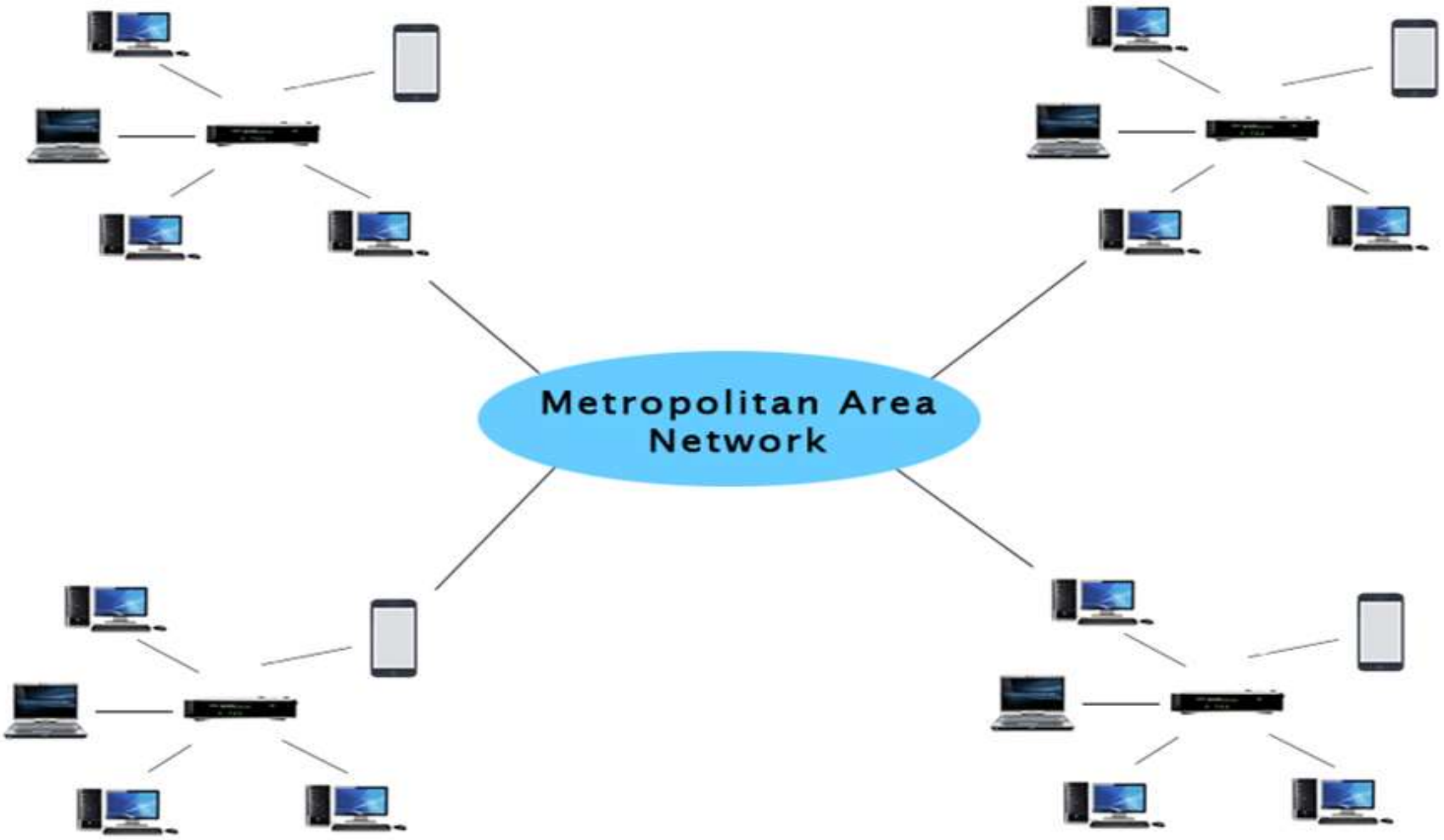
MAN(Metropolitan Area Network)

- A metropolitan area network is a network that covers a larger geographic area by interconnecting a different LAN to form a larger network.
- Government agencies use MAN to connect to the citizens and private industries.
- In MAN, various LANs are connected to each other through a telephone exchange line.
- The most widely used protocols in MAN are RS-232, Frame Relay, ATM, ISDN, OC-3, ADSL, etc.
- It has a higher range than Local Area Network(LAN).

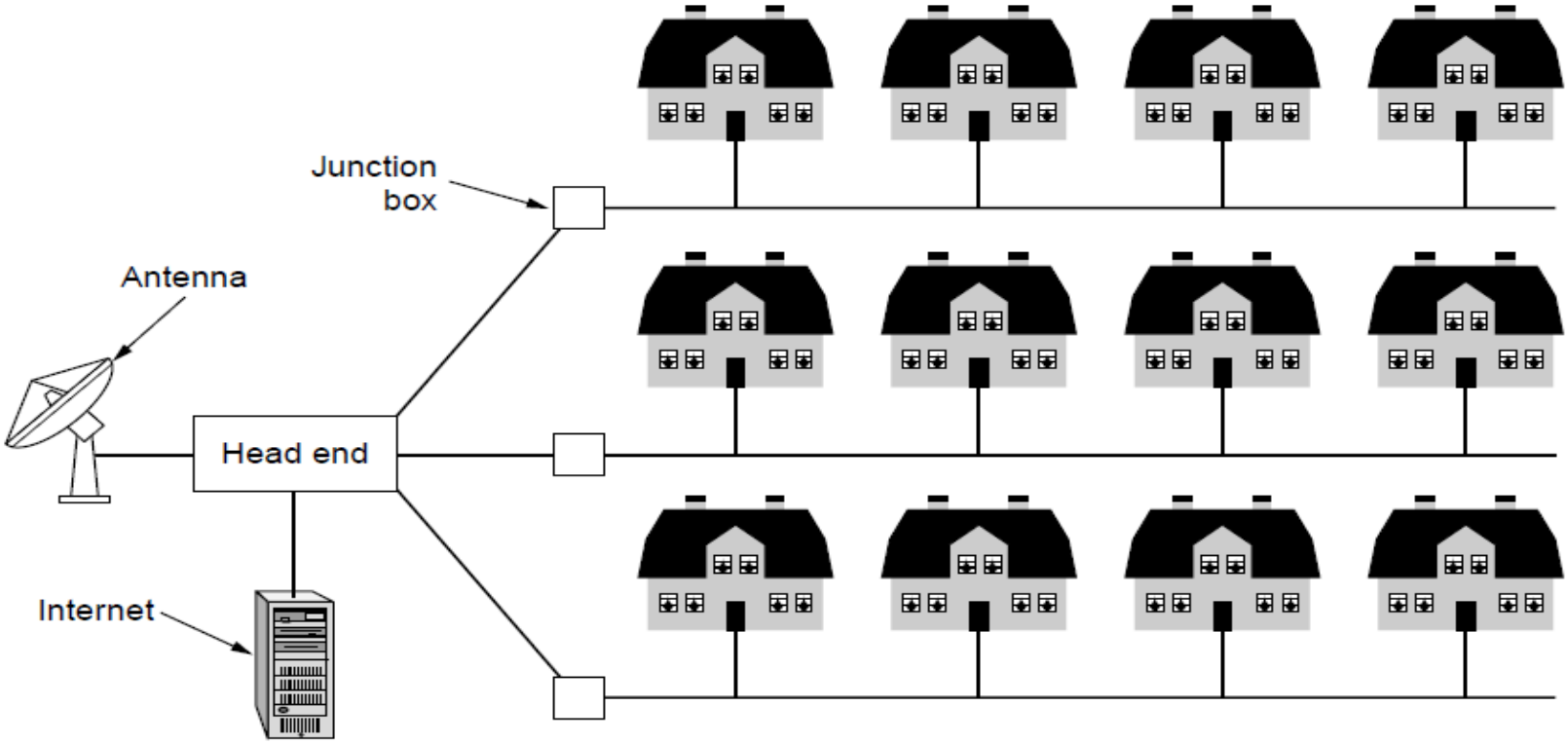
Metropolitan Area Networks

- A MAN (Metropolitan Area Network) covers a city. Ex: Cable Network.
- In this figure we see both television signals and Internet being fed into the centralized cable headend for subsequent distribution to people's homes.
- Recent developments in high-speed wireless Internet access have resulted in another MAN, called WiMAX(Worldwide Interoperability for Microwave Access).

Metropolitan Area Network



Metropolitan Area Networks



A metropolitan area network based on cable TV.

Uses Of Metropolitan Area Network

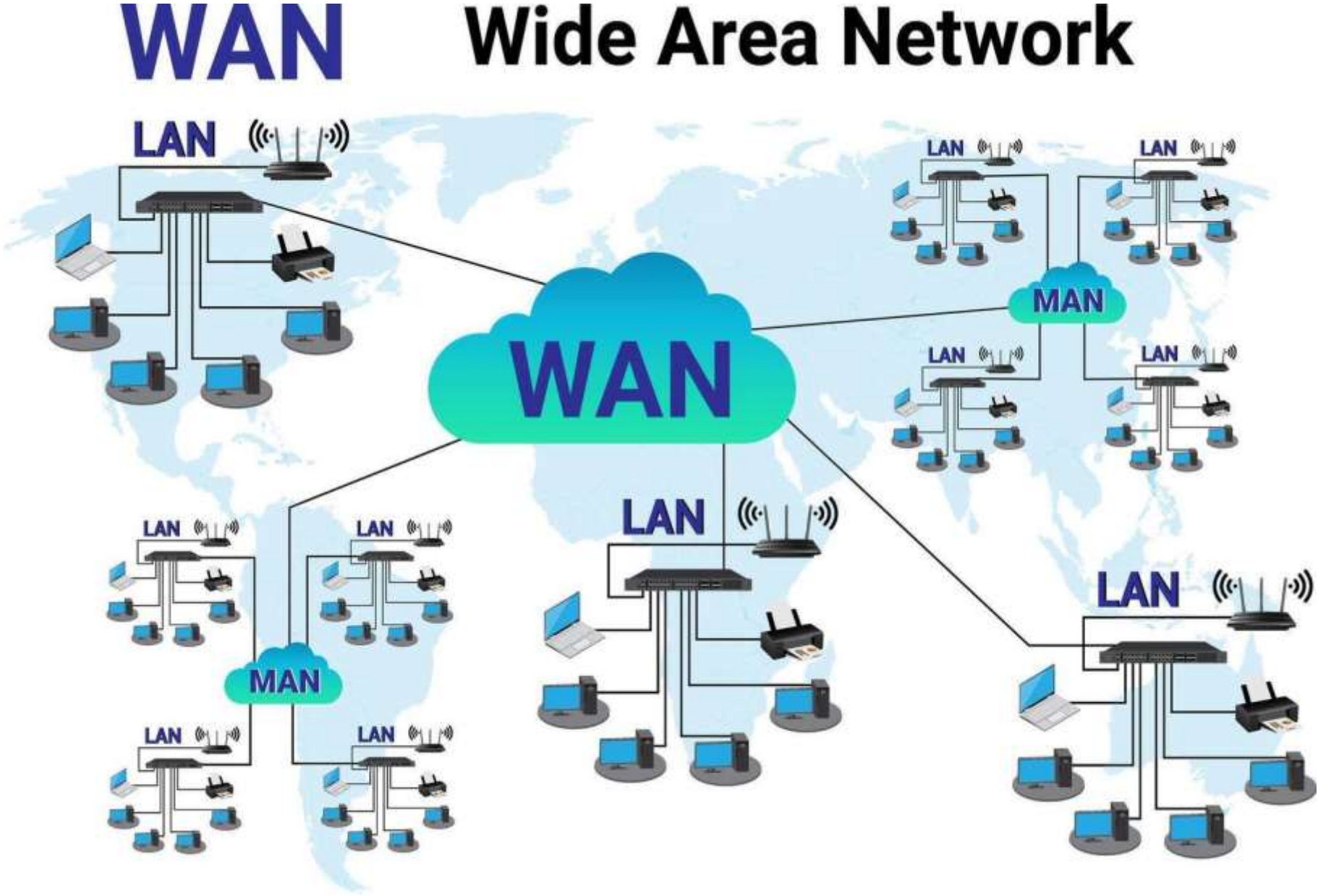
- MAN is used in communication between the banks in a city.
- It can be used in a college within a city.
- It can also be used for communication in the military.

WAN(Wide Area Network)

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

Wide Area Networks

- A LAN interconnects hosts; a WAN interconnects connecting devices such as switches, routers, or modems.
- A WAN is normally created and run by communication companies and leased by an organization that uses it.
- **A point-to-point WAN** is a network that connects two communicating devices through a transmission media (cable or air).
- **Switched WAN** is a combination of several point-to-point WANs that are connected by switches.
- switches, are specialized computers that connect two or more transmission lines


WAN
Wide Area Network
LAN
WAN
MAN
LAN
LAN
LAN
LAN
LAN
LAN
LAN
LAN
MAN
LAN
LAN
LAN

Examples Of Wide Area Network

- **Mobile Broadband:** A 4G network is widely used across a region or country.
- **Last mile:** A telecom company is used to provide the internet services to the customers in hundreds of cities by connecting their home with fiber.
- **Private network:** A bank provides a private network that connects all of its offices. This network is made by using the telephone leased line provided by the telecom company.

Advantages Of Wide Area Network

- **Geographical area:** A Wide Area Network provides a large geographical area. Suppose if the branch of our office is in a different city then we can connect with them through WAN. The internet provides a leased line through which we can connect with another branch.
- **Centralized data:** In case of WAN network, data is centralized. Therefore, we do not need to buy the emails, files or back up servers.
- **Get updated files:** Software companies work on the live server. Therefore, the programmers get the updated files within seconds.
- **Exchange messages:** In a WAN network, messages are transmitted fast. The web application like Facebook, Whatsapp, Skype allows you to communicate with friends.
- **Sharing of software and resources:** In WAN network, we can share the software and other resources like a hard drive, RAM.
- **Global business:** We can do the business over the internet globally.

Disadvantages of Wide Area Network

- **Security issue:** A WAN network has more security issues as compared to LAN and MAN network as all the technologies are combined together that creates the security problem.
- **Needs Firewall & antivirus software:** The data is transferred on the internet which can be changed or hacked by the hackers, so the firewall needs to be used. Some people can inject the virus in our system so antivirus is needed to protect from such a virus.
- **High Setup cost:** An installation cost of the WAN network is high as it involves the purchasing of routers, switches.
- **Troubleshooting problems:** It covers a large area so fixing the problem is difficult.

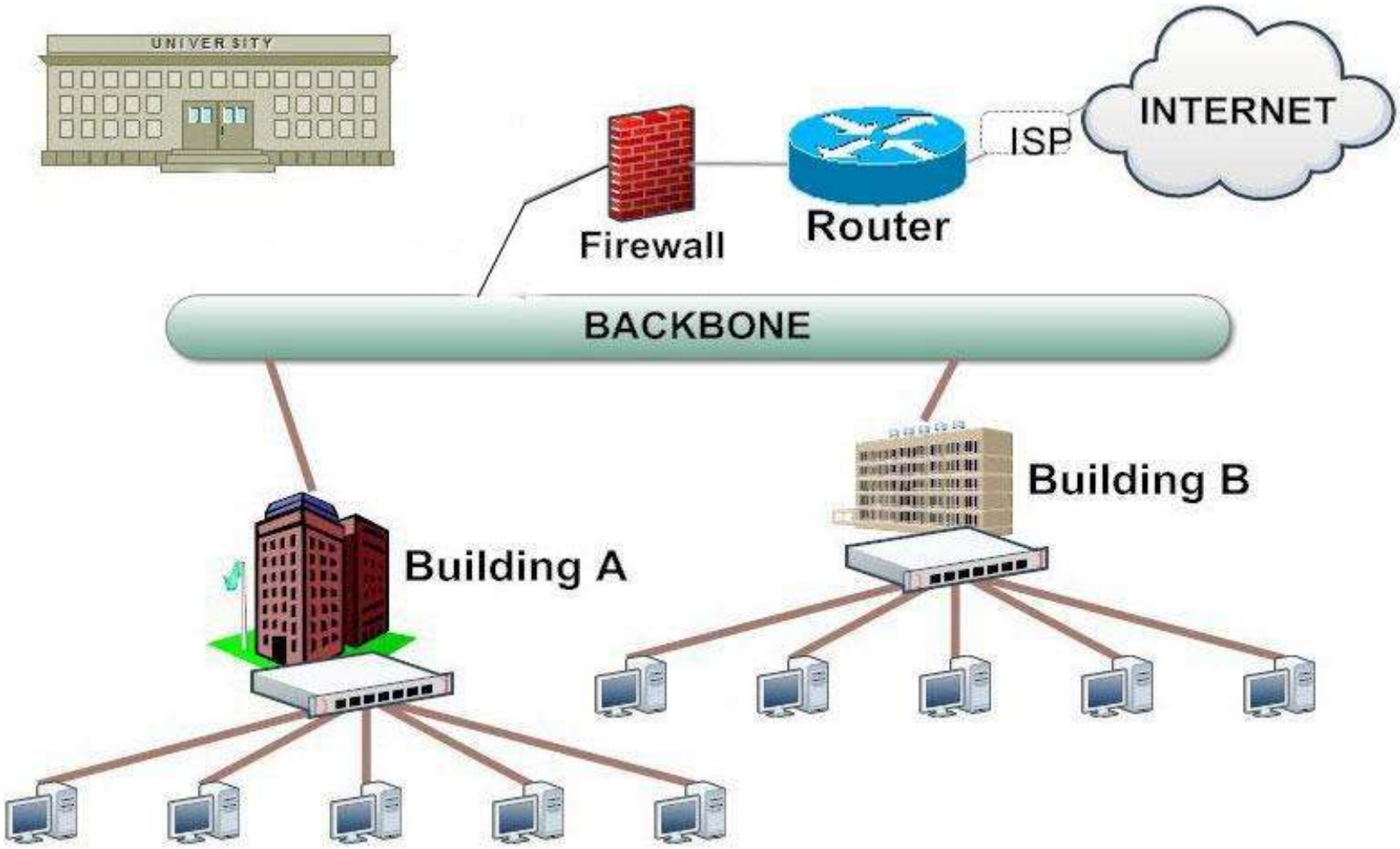
Differences b/w LAN-MAN-WAN

Factor	LAN	MAN	WAN
Scale	Operates in small area such as room, building or a same campus.	Operates in large area or city.	Operates in larger area such as country, continent or entire world.
Ownership	Privately owned	Private or public	Usually public owned, but some large companies have started providing the service under PPP public private partnership
Speed	High	Medium	Low
Error Rate	Low	Moderate	High
Setup Cost	Low	Moderate	High
Maintenance cost	Low	Moderate	High
Transmission Media	Coaxial cable or UTP	Telephone lines	PSTN or Satellite
Applications	Used in offices to connect users system, printer, scanners etc.	Telephone network or Cable TV network in a city.	Used to provide services of internet.

Campus Area Networks

- A Campus Area Network (CAN) is a computer network that connects multiple Local Area Networks (LANs) within a limited geographic area, like a university campus or a corporate office complex. It provides seamless connectivity for devices within its range, spanning buildings or even entire campuses. CANS are often used to provide internet access and allow for efficient sharing of resources.

Campus Area Network



Virtual Private Networks(VPN)

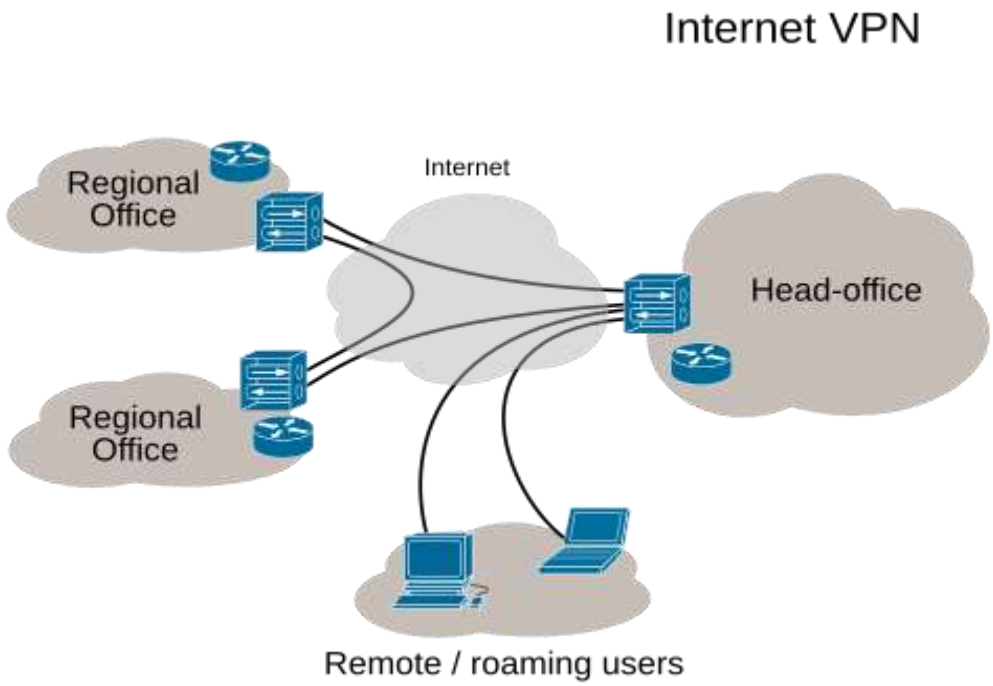
- A **Virtual Private Network (VPN)** is a secure, encrypted connection that allows users to access a private network over a public network (like the internet). It creates a **“virtual tunnel”** between your device and the destination network, keeping your data safe from eavesdropping, tampering, and censorship.

How VPNs Work:

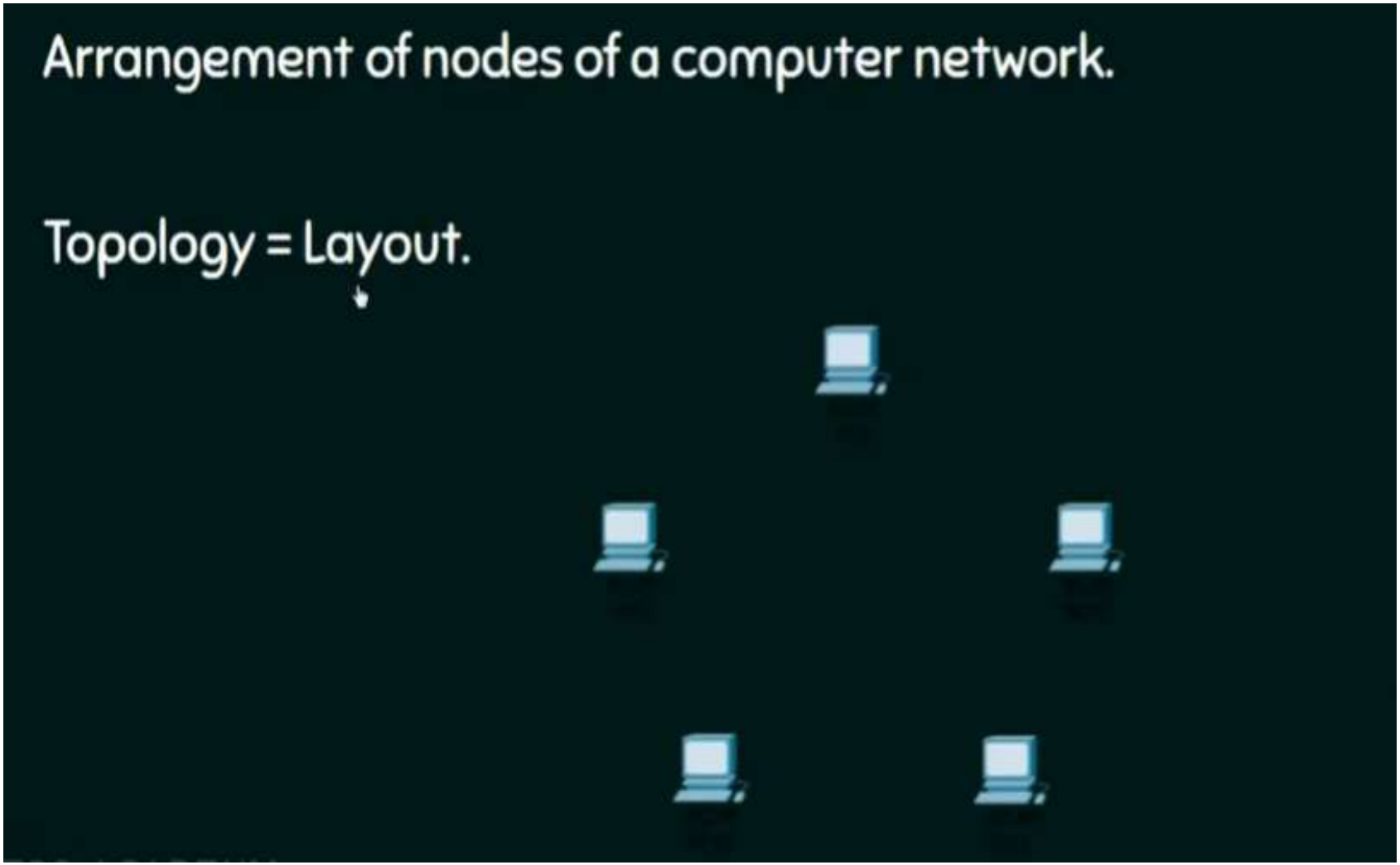
- **User connects to a VPN client (software)** on their device.
- The client encrypts the data before sending it over the internet.
- The data travels through a secure, encrypted "tunnel" to a **VPN server**.
- The VPN server decrypts the data and forwards it to the intended destination.
- The response follows the same route in reverse.

Why Use a VPN?

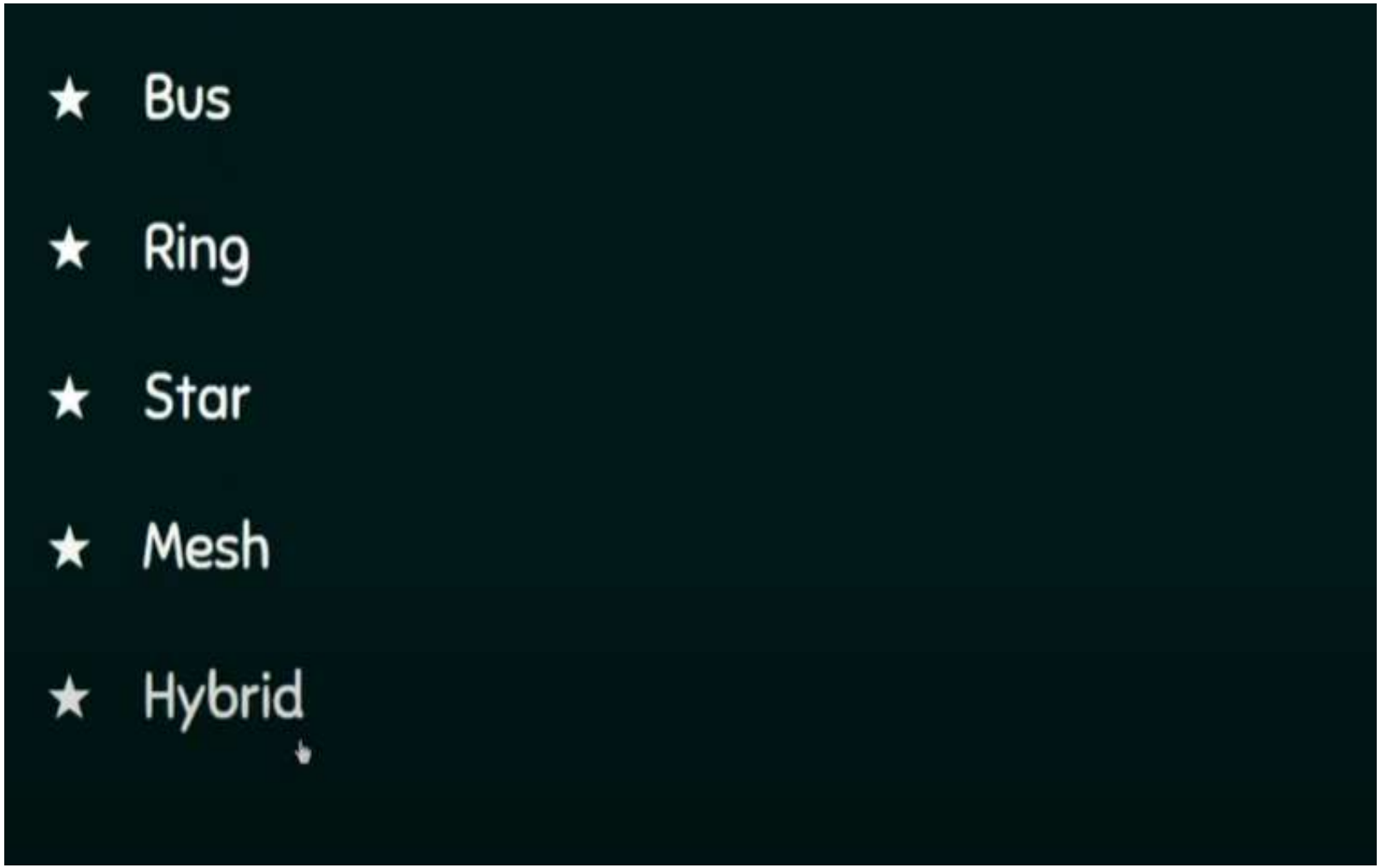
- **Secure data transmission** over untrusted networks (like public Wi-Fi)
- **Access restricted or region-locked content**
- **Bypass censorship and firewalls**
- **Protect identity and online privacy**



Network Topologies



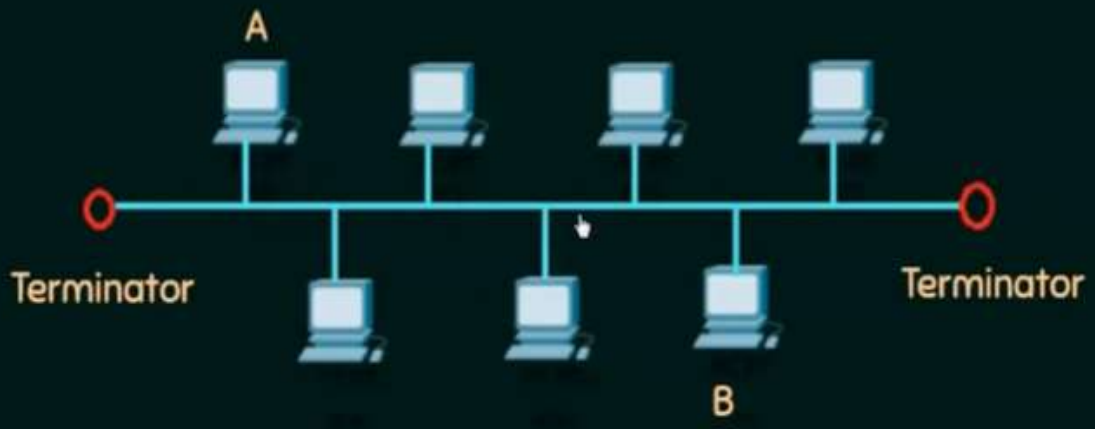
Network Topologies(1)



Network Topologies

Bus topology

- ★ All data transmitted between nodes in the network is transmitted over this common transmission medium and is able to be received by all nodes in the network simultaneously.
- ★ A signal containing the address of the intended receiving machine travels from a source machine in both directions to all machines connected to the bus until it finds the intended recipient.



Network Topologies

BUS TOPOLOGY

Advantages	Disadvantages
Only one wire – Less expensive.	Not fault tolerant (No redundancy).
Suited for temporary network.	Limited cable length.
Node failures does not affect others.	No security.

Network Topologies

RING TOPOLOGY

- ★ A ring topology is a bus topology in a closed loop.
- ★ Peer-to-Peer LAN topology.
- ★ Two connections: one to each of its nearest neighbors.
- ★ Unidirectional.
- ★ Sending and receiving data takes place with the help of a TOKEN.

Network Topologies

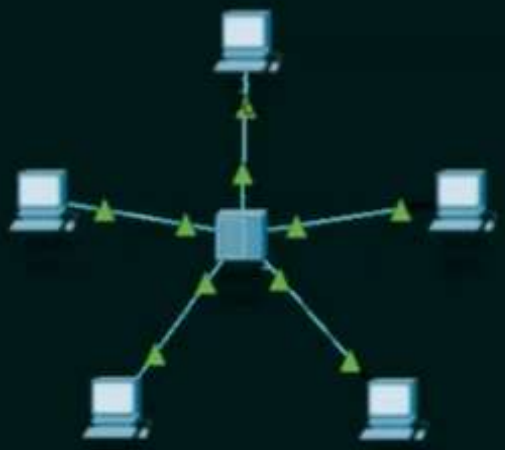
RING TOPOLOGY

Advantages	Disadvantages
Performance better than Bus topology.	Unidirectional. Single point of failure will affect the whole network.
Can cause bottleneck due to weak links.	↑ in load – ↓ in performance.
All nodes with equal access.	No security.

Network Topologies

Star topology

- ★ Every node is connected to a central node called a hub or switch.
- ★ Centralized Management.
- ★ All traffic must pass through the hub or switch.



Network Topologies

STAR TOPOLOGY

Advantages	Disadvantages
Easy to design and implement.	Single point of failure affects the whole network.
Centralized administration.	Bottlenecks due to overloaded switch/Hub.
Scalable.	Increased cost due to switch/hub.

Network Topologies(8)

MESH TOPOLOGY

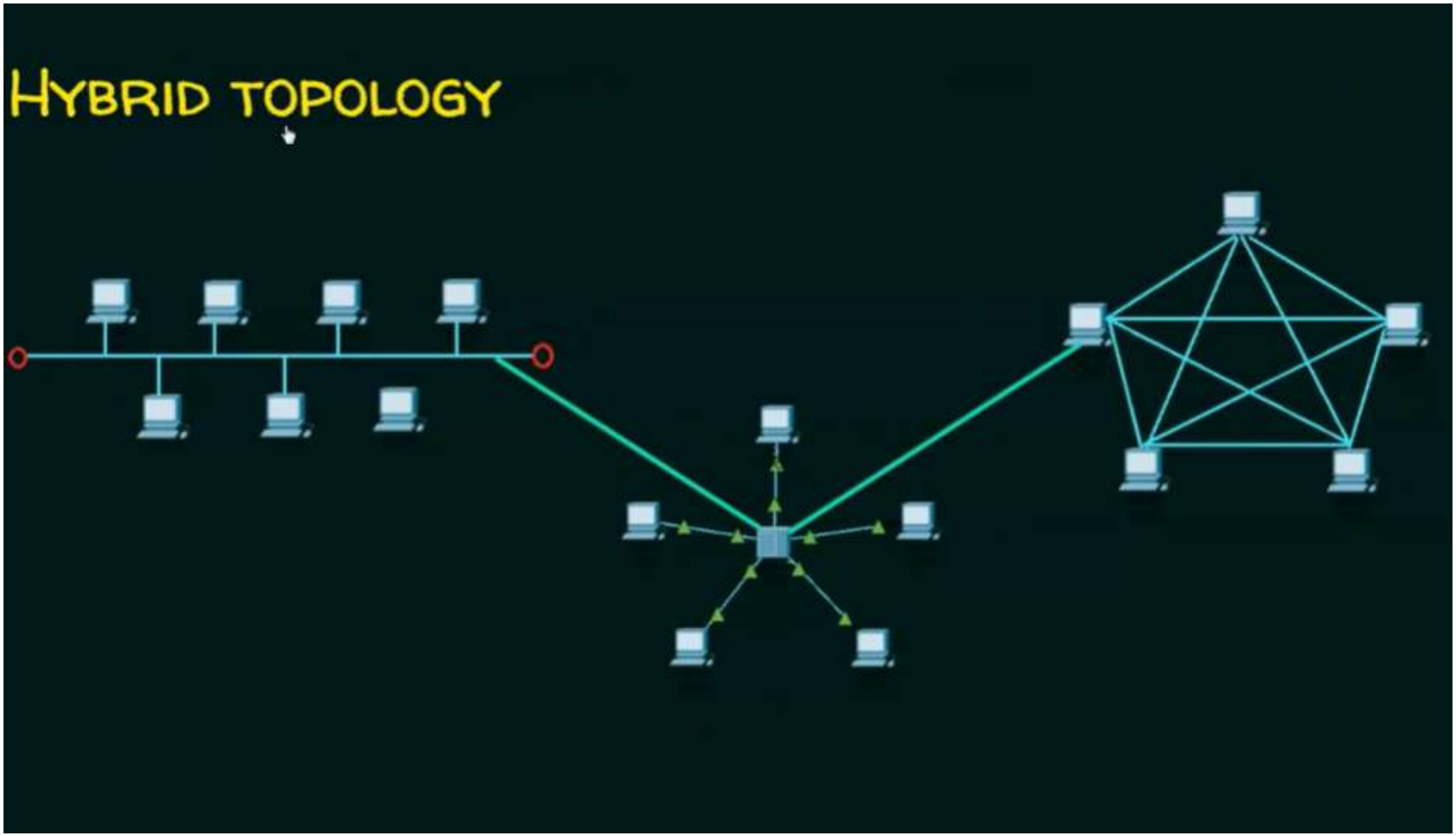
- ★ Each node is directly connected to every other nodes in the network.
- ★ Fault tolerant and reliable.

Network Topologies(9)

MESH TOPOLOGY

Advantages	Disadvantages
Fault tolerant.	Issues with broadcasting messages.
Reliable.	Expensive and impractical for large networks.

Network Topologies(9)

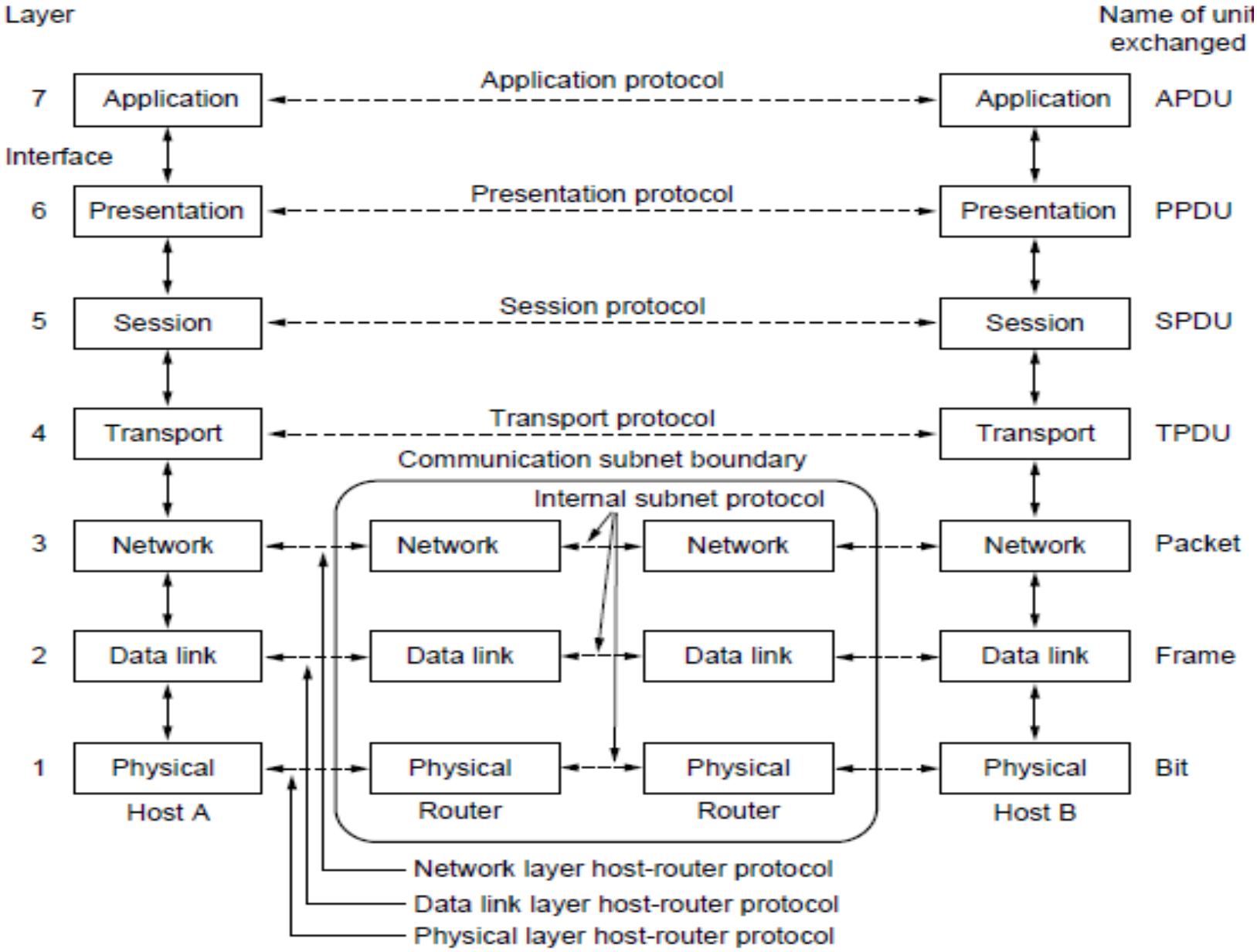


The OSI Reference Model

- The OSI (Open Systems Interconnection) Reference Model, developed by the International Organization for Standardization (ISO), is a conceptual model that standardizes communication between different computer systems. It was created in the late 1970s and published in 1984 to address the challenges of interoperability between diverse networking technologies.

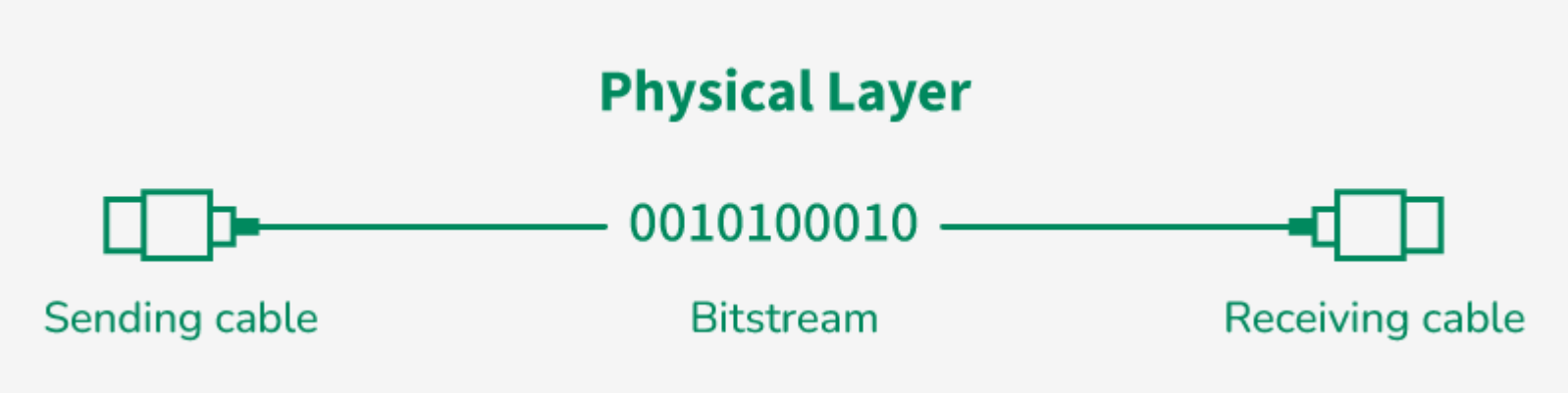
Principles for the seven layers

- Layers created for different abstractions
- Each layer performs well-defined function
- Function of layer chosen with definition of international standard protocols in mind
- Number of layers optimum


Layer
Name of unit exchanged
7
Application
Application protocol
Application
APDU
Interface
6
Presentation
Presentation protocol
Presentation
PPDU
5
Session
Session protocol
Session
SPDU
4
Transport
Transport protocol
Transport
TPDU
Communication subnet boundary
Internal subnet protocol
3
Network
Network
Network
Network
Packet
2
Data link
Data link
Data link
Data link
Frame
1
Physical
Physical
Physical
Physical
Bit
Host A
Router
Router
Host B
Network layer host-router protocol
Data link layer host-router protocol
Physical layer host-router protocol

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.** Physical Layer 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. Common physical layer devices are Hub, Repeater, Modem, and Cables.



Functions of the Physical Layer

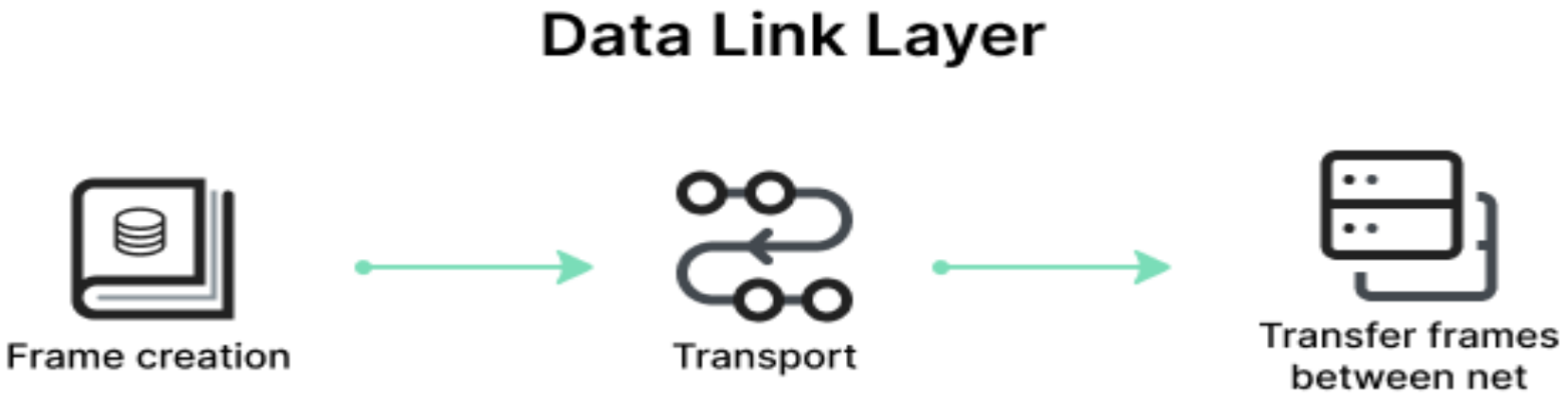
- **Bit Synchronization:** The physical layer provides the synchronization of the bits by providing a clock. This clock controls both sender and receiver thus providing synchronization at the bit level.
- **Bit Rate Control:** The Physical layer also defines the transmission rate i.e. the number of bits sent per second.
- **Physical Topologies:** Physical layer specifies how the different, devices/nodes are arranged in a network i.e. bus topology, star topology, 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.

Layer 2: Data Link Layer (DLL)

- 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. Packet in the Data Link layer is referred to as Frame**.** Switches and Bridges are common Data Link Layer devices.
- The Data Link Layer is divided into two sublayers:
- Logical Link Control (LLC)
- 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.

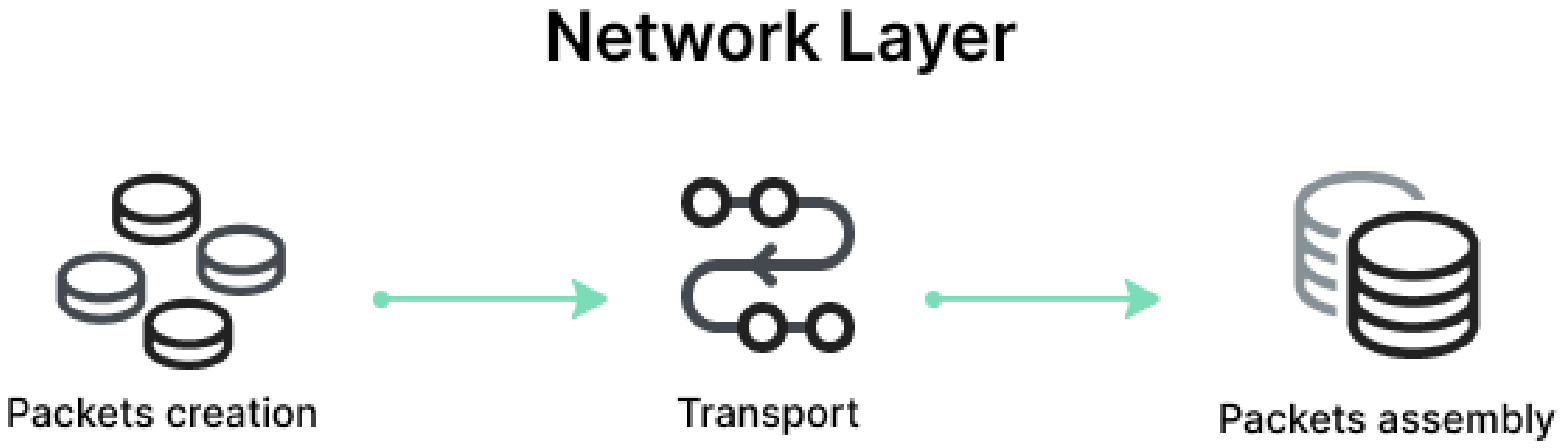
Functions of the Data Link Layer

- Framing is 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.



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 and receiver's IP address are placed in the header by the network layer. Segment in the Network layer is referred to as Packet**.** Network layer is implemented by networking devices such as routers and switches.



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 inter-network uniquely, the network layer defines an addressing scheme. The sender and receiver's IP addresses are placed in the header by the network layer. Such an address distinguishes each device uniquely and universally.

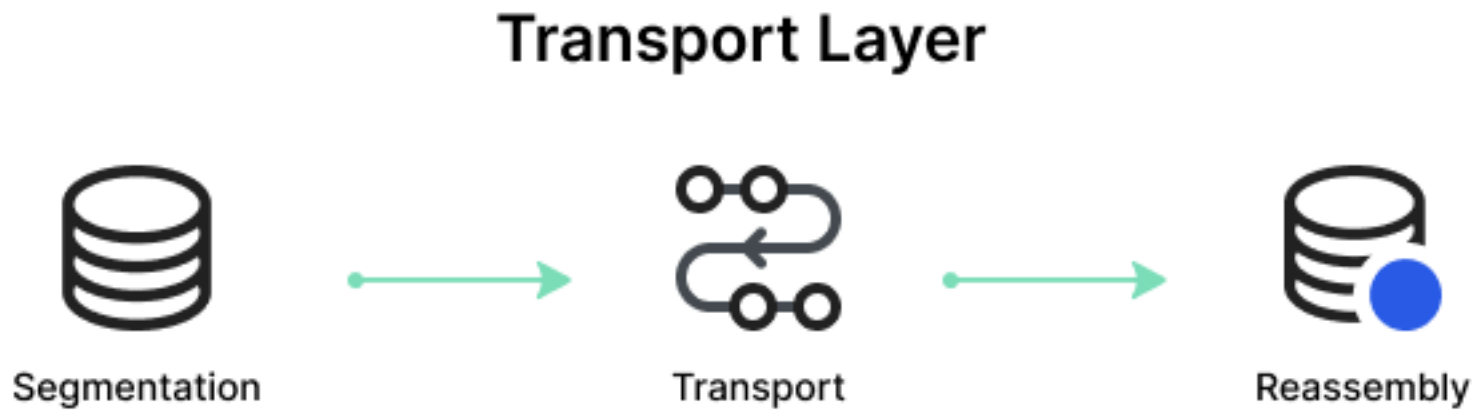
Layer 4: Transport Layer

- 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. Protocols used in Transport Layer are TCP, UDP NetBIOS, PPTP.
- **At the sender's side**, the transport layer receives the formatted data from the upper layers, performs **Segmentation**, and also implements **Flow and error control** to ensure proper data transmission. It also adds Source and Destination port number in its header and forwards the segmented data to the Network Layer.

- **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.

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.



Layer 5: Session Layer

- Session Layer in the OSI Model is responsible for the establishment of connections, management of connections, terminations of sessions between two devices. It also provides authentication and security. Protocols used in the Session Layer are NetBIOS, PPTP.

Functions of the Session Layer

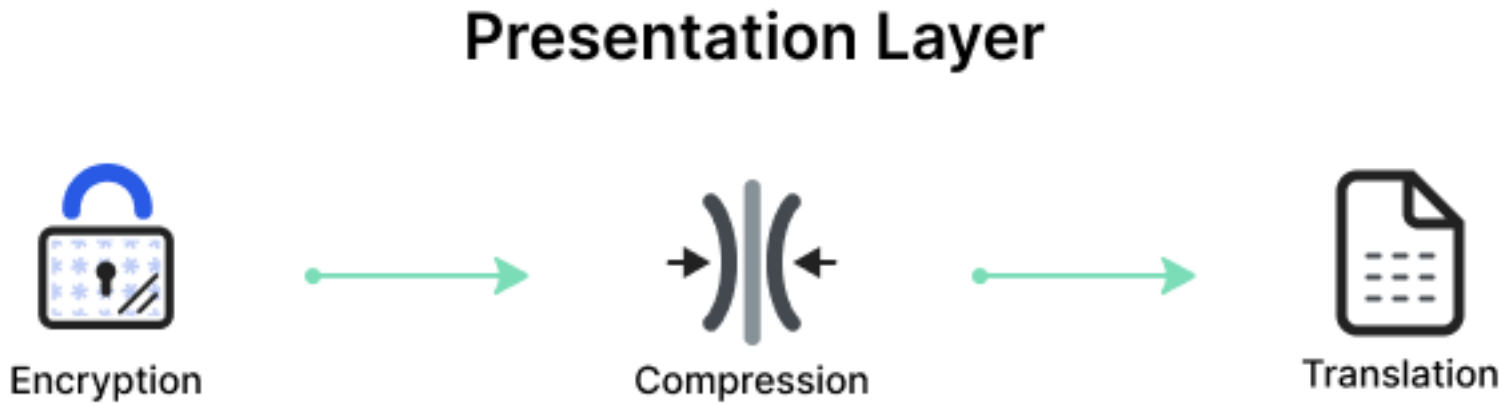
- **Session Establishment, Maintenance, and Termination:** The layer allows the two processes to establish, use, and terminate a connection.
- **Synchronization:** This layer allows a process to add checkpoints that are considered synchronization points in the data. These synchronization points help 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.

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.

Functions of the Presentation Layer

- **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.



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 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. Protocols used in the Application layer are SMTP, FTP, DNS, etc.

Functions of the Application Layer

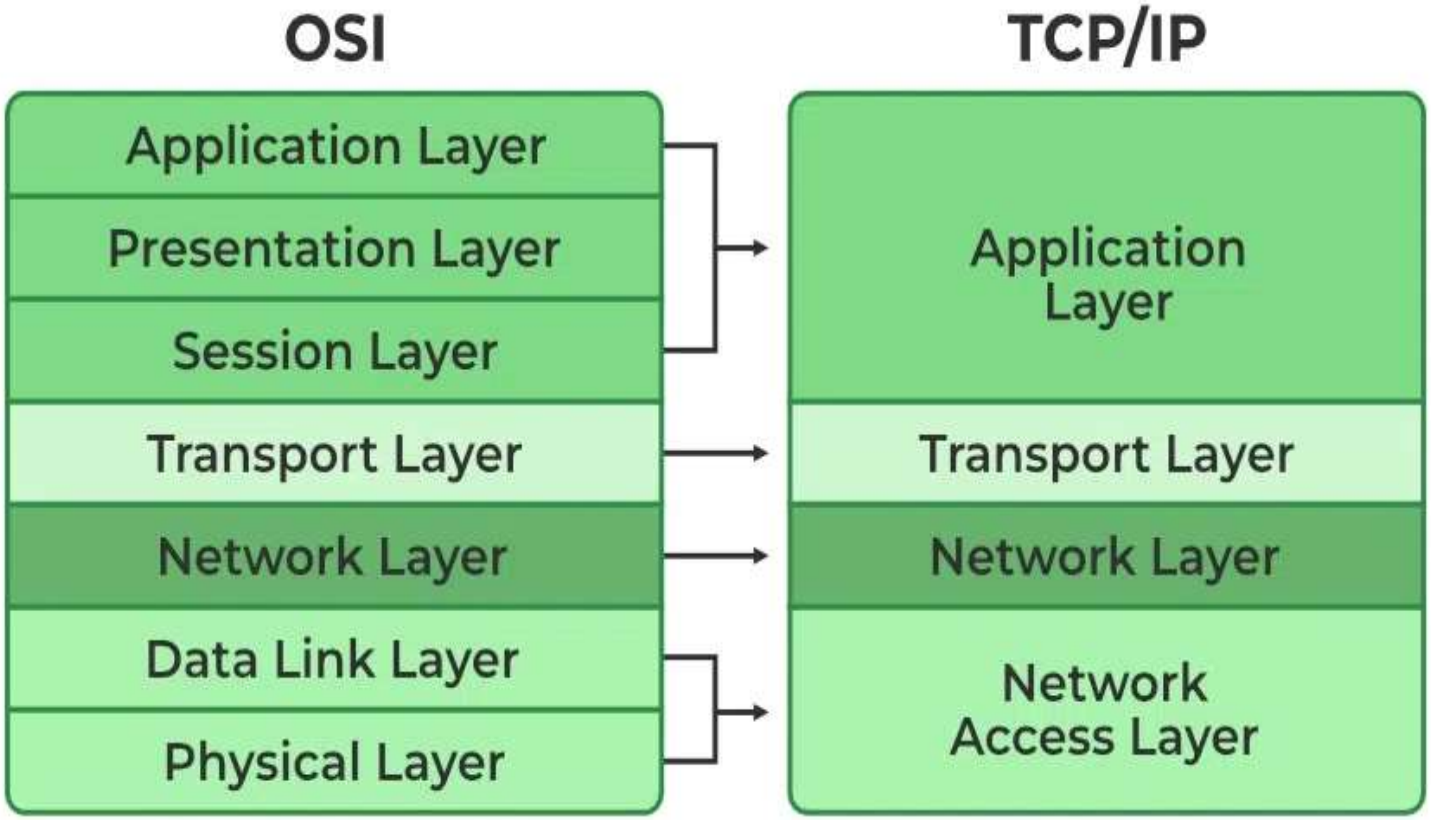
- The main functions of the application layer are given below.
- **Network Virtual Terminal (NVT):** It allows a user to log on to a remote host.
- **File Transfer Access and Management (FTAM):** This application allows a user to access files in a remote host, retrieve files in a remote host, and manage 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.

TCP/IP Model

- TCP/IP was designed and developed by the Department of Defense (DoD) in the 1970s and is based on standard protocols
- The TCP/IP model (Transmission Control Protocol/Internet Protocol) is a four-layer networking framework that enables reliable communication between devices over interconnected networks. It provides a standardized set of protocols for transmitting data across interconnected networks, ensuring efficient and error-free delivery. Each layer has specific functions.

Layers of TCP/IP Model

- It's composed of four interconnected layers compared to the seven layers in the OSI model. Each layer performs a specific task on the data that is being transmitted over the network channel, and data moves from one layer to another.
- Application Layer
- Transport Layer(TCP/UDP)
- Network/Internet Layer(IP)
- Network Access Layer


OSI
TCP/IP
Application Layer
Presentation Layer
Session Layer
Transport Layer
Network Layer
Data Link Layer
Physical Layer
Application Layer
Transport Layer
Network Layer
Network Access Layer

1. Application Layer

- The Application Layer is the closest to the end user and is where applications and user interfaces reside. It serves as the bridge between user programs and the lower layers responsible for data transmission.
- **Function:** Provides services and interfaces for end-user applications to access network resources.
- **Key responsibilities:**
  - Supports application protocols like HTTP, FTP, SMTP, DNS, etc.
  - Enables communication between software applications across networks.
  - Handles data formatting, encryption, and session management.

2. Transport Layer

- This layer ensures data is delivered reliably and in the correct order between devices. The two main protocols in this layer are TCP (Transmission Control Protocol) and UDP (User Datagram Protocol).
- **Function:** Ensures reliable or unreliable delivery of data between hosts.
- **Key responsibilities:**
  - TCP (Transmission Control Protocol): Provides reliable, connection-oriented delivery with error checking, retransmission, and flow control.
  - UDP (User Datagram Protocol): Provides faster, connectionless transmission without guarantees.
  - Manages flow control and segmentation/reassembly of data.

3. Internet Layer

- It handles the routing of data packets across networks. It uses the Internet Protocol (IP) to assign unique IP addresses to devices and decide the most efficient path for data to reach its destination.
- **Function:** Determines the best path for data to travel across networks.
- **Key responsibilities:**
  - IP (Internet Protocol)**:** Provides addressing and routing.
  - Handles packet forwarding, fragmentation, and logical addressing (IP addresses).
  - Involves protocols like IP, ICMP (for diagnostics), and ARP (for address resolution).

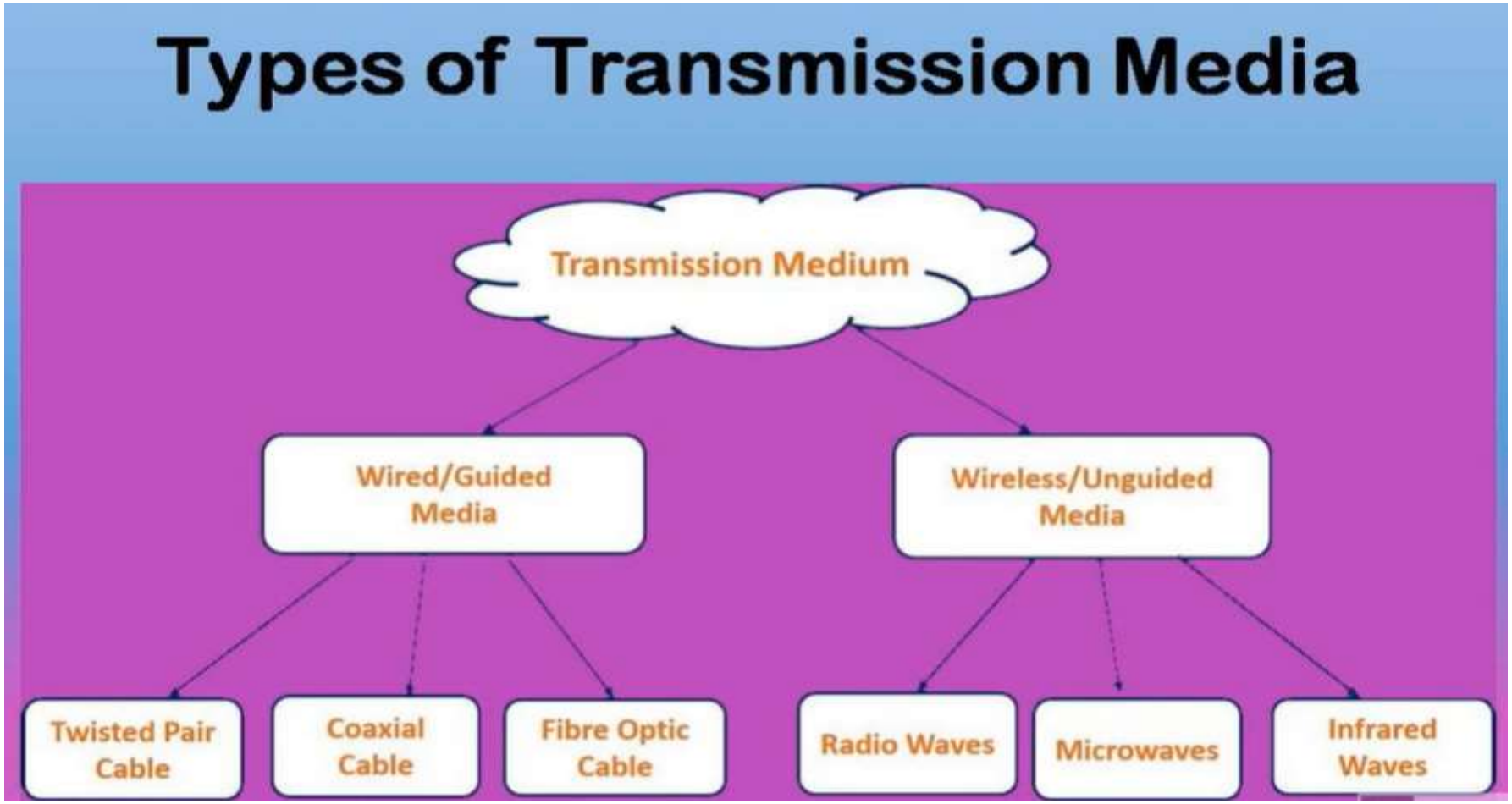
4. Network Access Layer

- This layer is the lowest layer in the model and responsible for the physical connection between devices within the same network segment.
- **Function:** Manages the physical transmission of data over the network hardware.
- **Key responsibilities:**
  - Handles how data is physically sent over cables, Wi-Fi, etc.
  - Manages MAC addressing, framing, and error detection at the physical link.
  - Includes Ethernet, Wi-Fi, and other data link technologies.

Comparison of the OSI and TCP/IP Reference Models

TCP/IP	OSI
Implementation of OSI model	Reference model
Model around which Internet is developed	This is a theoretical model
Has only 4 layers	Has 7 layers
Considered more reliable	Considered a reference tool
Protocols are not strictly defined	Stricter boundaries for the protocols
Horizontal approach	Vertical approach
Combines the session and presentation layer in the application layer	Has separate session and presentation layer
Protocols were developed first and then the model was developed	Model was developed before the development of protocols
Supports only connectionless communication in the network layer	Supports connectionless and connection-oriented communication in the network layer
Protocol dependent standard	Protocol independent standard

Transmission Media



➢**A transmission medium can be broadly defined as anything that can carry information from a source to a destination.**

Guided Medium/Media

- **A signal traveling along any of these media is directed and contained by the physical limits of the medium.**
- **It guides signal through solid physical path**

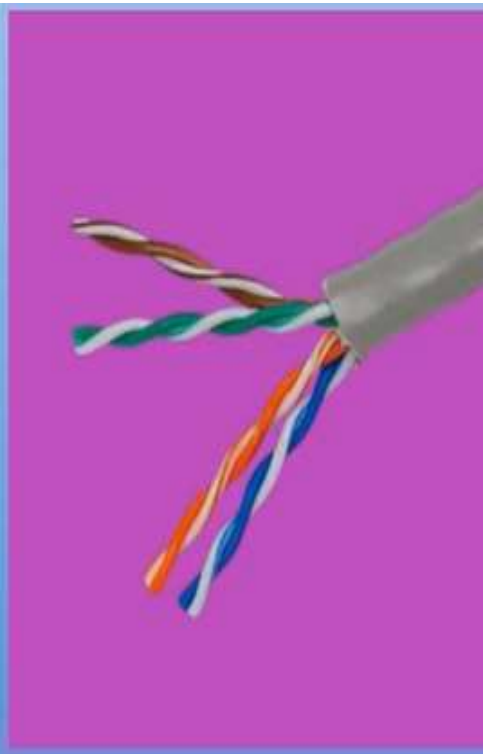
Objective

Transmission Media

- Wired Transmission Media

1. Twisted Pair Cable
2. Coaxial Cable
3. Optical Fibre Cable

Twisted Pair Cable

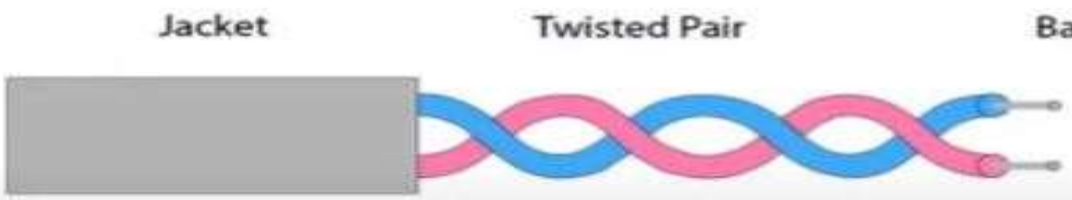


+ Its made up of two separate insulated copper wires which are twisted together and run in parallel
+ Upto 25 pairs of cable can be put in a single sheath
+ The twist around the wires helps to reduce the noise and disturbance in the signals
+ It is very cheap,light weight and easy to install and is widely used in telephone lines.

Twisted Pair Cable

—Signals cannot travel long distances
—Very thin and breaks easily
—Cannot be used for broadband connections

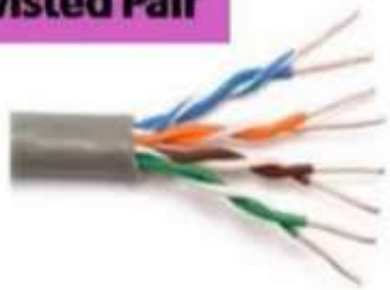
Twisted pair:



Types of Twisted Pair Cable

UTP & STP

Unshielded Twisted Pair



UTP Cable

STP Cable

Shielded Twisted Pair

- The most common twisted pair cable used in communications is referred to as unshielded twisted-pair (UTP).
- IBM has also produced a version of twisted-pair cable for its use, called shielded twisted-pair (STP). STP cable has a metal foil or braided mesh covering that encases each pair of insulated conductors.

- **Unshielded Twisted pair:**
- 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.

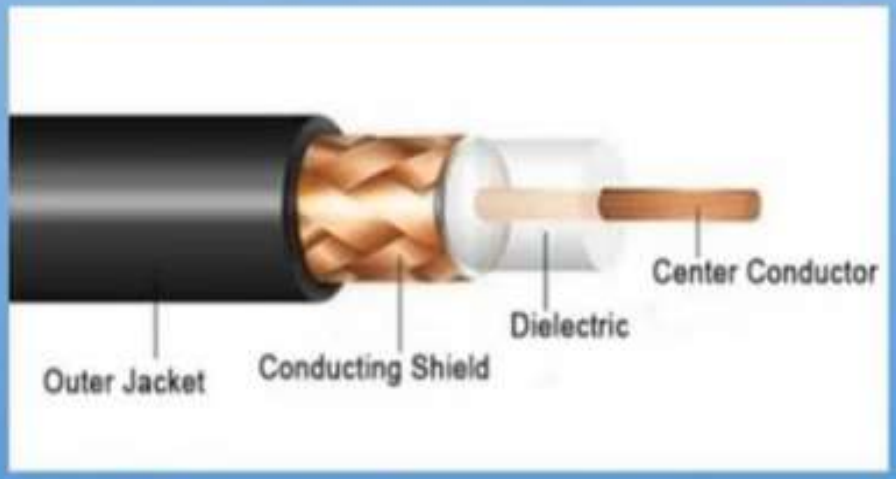
- **Unshielded Twisted pair:**
- **Advantages Of Unshielded Twisted Pair:**
- It is cheap.
- Installation of the unshielded twisted pair is easy.
- It can be used for high-speed LAN.
- **Disadvantage:**
- This cable can only be used for shorter distances because of attenuation.

- **Shielded Twisted pair:**
- **Characteristics Of Shielded Twisted Pair:**
- The cost of the shielded twisted pair cable is not very high and not very low.
- An Installation of STP is easy.
- It has higher capacity as compared to unshielded twisted pair cable.
- It has a higher attenuation.
- It is shielded that provides the higher data transmission rate.

Coaxial Cable

A coaxial cable is a type of shielded and insulated copper cable that is used in cable TV, telephone and computer networks .

Coaxial Cable



*It consists of **four** primary components, as follows:*

A core **copper wire** at its centre.

This copper wire is surrounded by a **plastic insulator or dielectric**

Over this is a **mesh shield** which is made up of a conducting material.

The last layer called as the **outer jacket** is made of Teflon or plastic coating.

Advantages of using Coaxial Cable

+ Provide excellent noise immunity

+ Signals can travel longer distances at higher speed

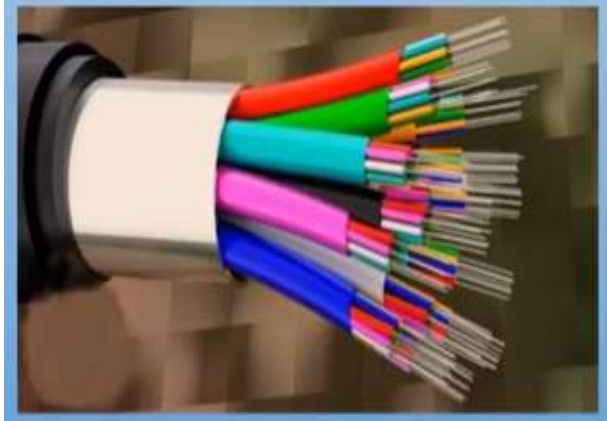
+Easy to install and maintain

Coaxial Cable

- The bandwidth possible depends on the cable quality, length and signa-to-noise ratio of the data signal.
- Modern cables have a bandwidth of close to 1GHz.
- Coaxial cables are widely used for telephone system for long distances lines which are replaced with fiber optics

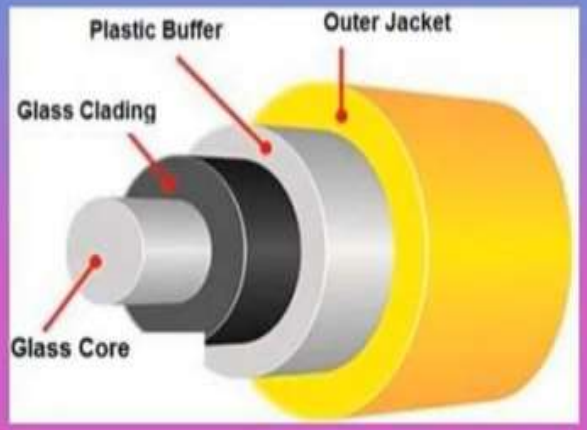
Disadvantages of using Coaxial Cable

- Expensive as compared to Twisted Pair Cable
- It is bulky
- In case of any damage the entire network goes down as a single cable is used for transmission.



Optical Fibre Cable

Is the technology associated with data transmission in the form of light pulses making use of a fiber which is made of plastic or glass.



Features of Optical Fiber Cable

+ It mainly consists of a centre glass core surrounded by several layers of protective material.
+ Carries more information than copper wires .
+ Data travels at a higher speed

- Expensive to install
- More difficult and expensive to splice

- Fiber-Optic Cable Current technology supports two modes **(multimode and single mode)** for propagating light along optical channels, each requiring fiber with different physical characteristics. Multimode can be implemented in two forms: step-index or graded-index
- **The single-mode fiber** itself is manufactured with a much smaller diameter than that of multimode fiber, and with substantially lower density.
- **In multimode step-index fiber**, the density of the core remains constant from the center to the edges.
- **In multimode graded-index fiber**, decreases this distortion of the signal through the cable

- **Fiber Optic:**

- **Greater Bandwidth:**
- The fiber optic cable provides more bandwidth as compared copper.
- Therefore, the fiber optic carries more data as compared to copper cable.•
- **Faster speed:**
- Fiber optic cable carries the data in the form of light.
- This allows the fiber optic cable to carry the signals at a higher speed.
- **Longer distances**:
- The fiber optic cable carries the data at a longer distance as compared to copper cable.
- **Better reliability:** The fiber 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.
- **Thinner** : Fiber optic cable is thinner and lighter in weight

Advantages

- Higher bandwidth.
- Less signal attenuation.
- Resistance to corrosive materials.
- Light weight.
- Greater immunity to tapping.

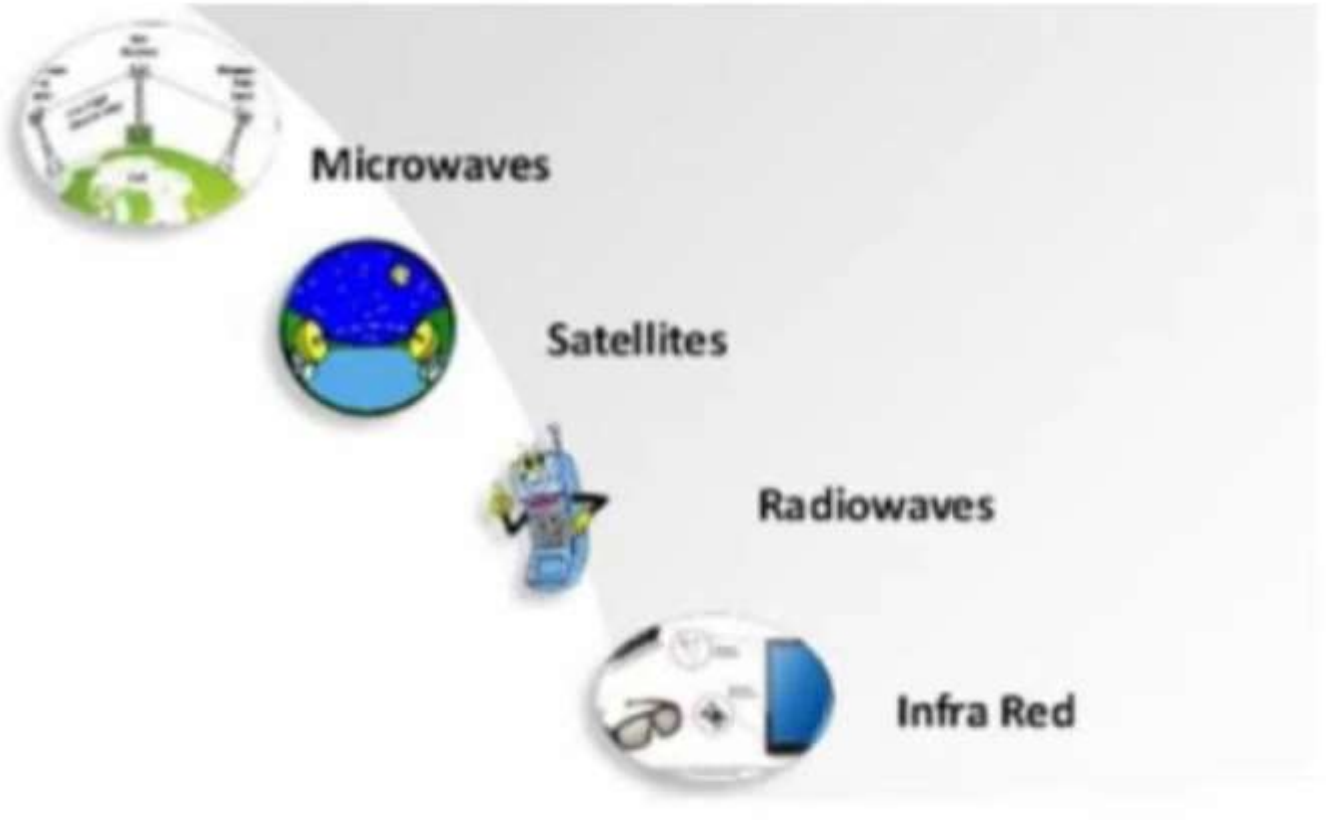
Disadvantages

- Installation and maintenance.
- Unidirectional light propagation.
- Cost.

Applications

- **Twisted-Pair**
- Used in telephone lines to provide voice and data channels.
- The DSL lines that are used by the telephone companies to provide high-data-rate.
- Local-area networks, such **as 10Base-T and 100Base-T**, also use twisted-pair cables.
- **Coax**
- Coaxial cable was widely used in analog telephone networks where a single coaxial network could carry **10,000 voice signals**.
- Later it was used in digital telephone networks where a single coaxial cable could carry digital data up to **600 Mbps**.
- Used in traditional **Ethernet LANs**
- Now a days mostly used in TV communication.
- **Optical-Fibers**
- Used in backbone networks because its wide bandwidth is cost-effective.
- In some TV communications

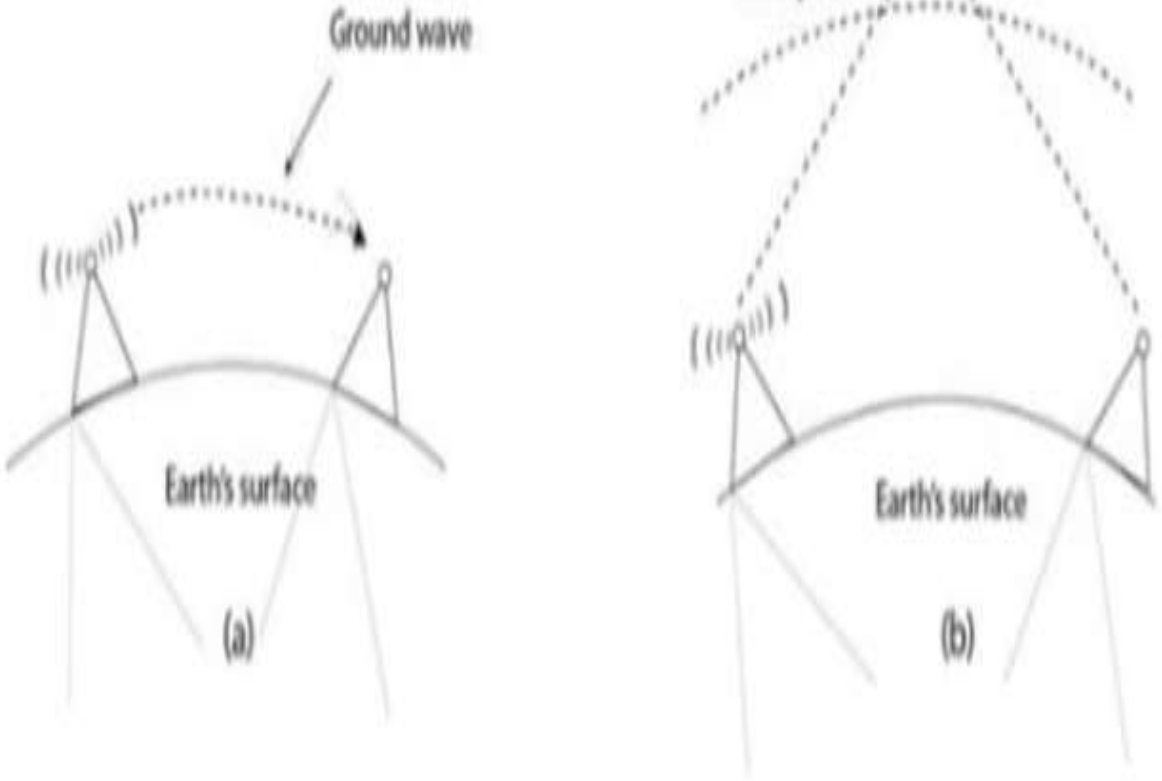
Unguided Transmission Media



- **Unguided medium**
  - **transport electromagnetic waves without using a physical conductor. This type of communication is often referred to as wireless communication**

Unguided Transmission Media

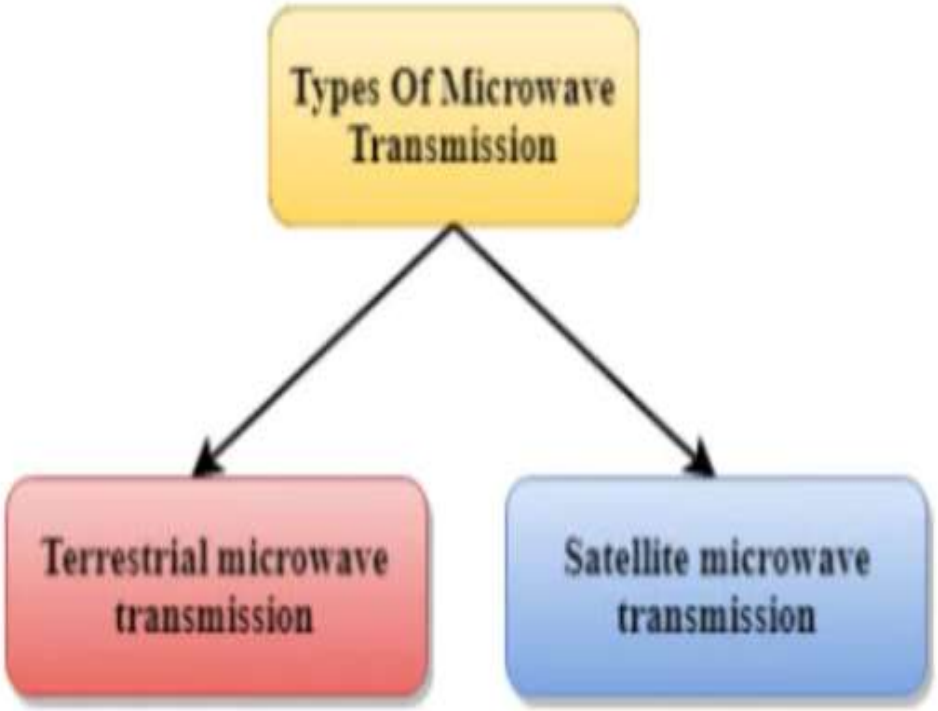
Radio Waves



- Radio Waves are used for **Multicast** Communication when there is one sender and many receivers, such as Radio and television
- Can penetrate through walls
- Highly regulated and omni directional Antenna
- Frequency range between 3KHz and 1GHz
- FM radio, Televison, cardless phones
- **ADVANTAGES**
  - Used in wide Area Networks
  - Mobile cellular Networks
  - These Radio waves are used cover large areas

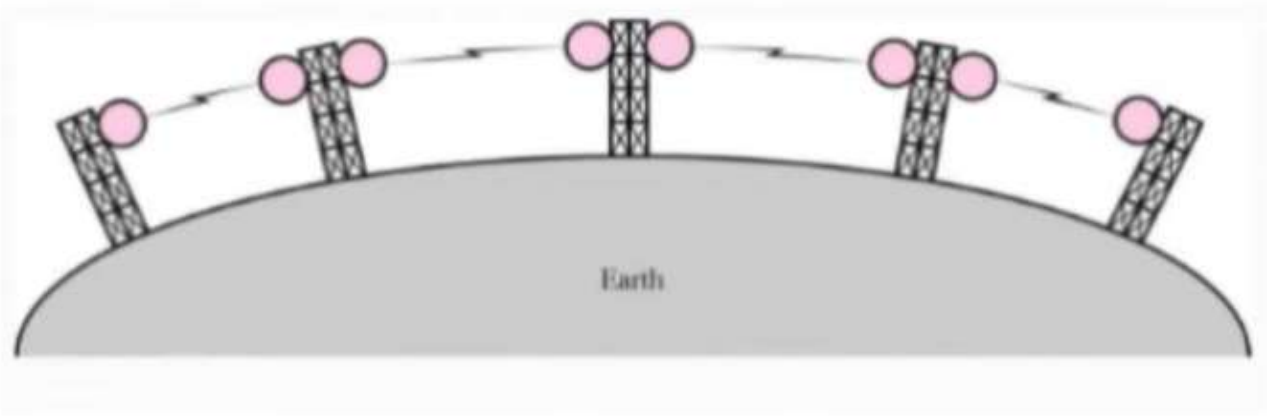
Unguided Transmission Media

Micro Waves



Unguided Transmission Media

Terrestrial Microwave Transmission



- **Terrestrial Microwave Transmission is a technology which is focused on beam.**
- **It is also called ground wave Transmission.**

Terrestrial Microwave Transmission

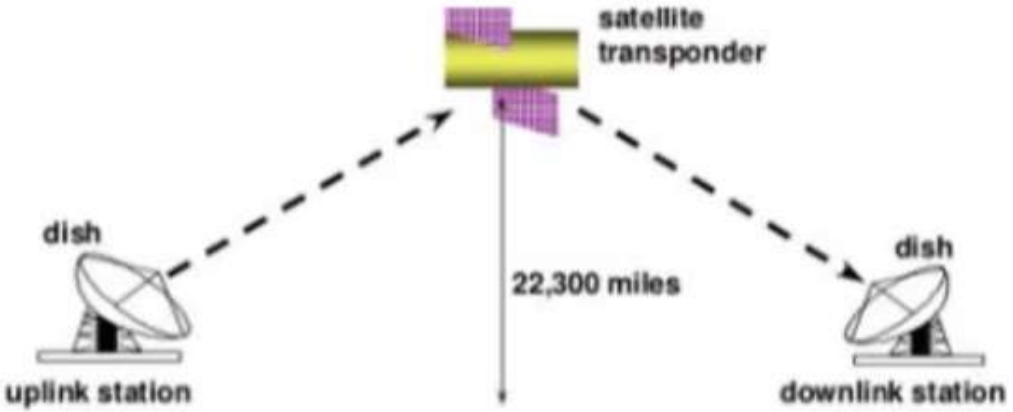
- Characteristics of Microwave:
- **Frequency range:**
  - The frequency range of terrestrial microwave is from 4-6 GHz to 21-23 GHz.
- **Bandwidth:**
  - It supports the bandwidth from 1 to 10 Mbps.
- **Short distance**:
  - It is inexpensive for short distance.
- **Long distance**:
  - It is expensive as it requires a higher tower for a longer distance.
- **Attenuation**:
  - Attenuation means loss of signal.
  - It is affected by environmental conditions and antenna
- It uses directional antennas
- Higher range of frequencies cannot penetrate through walls

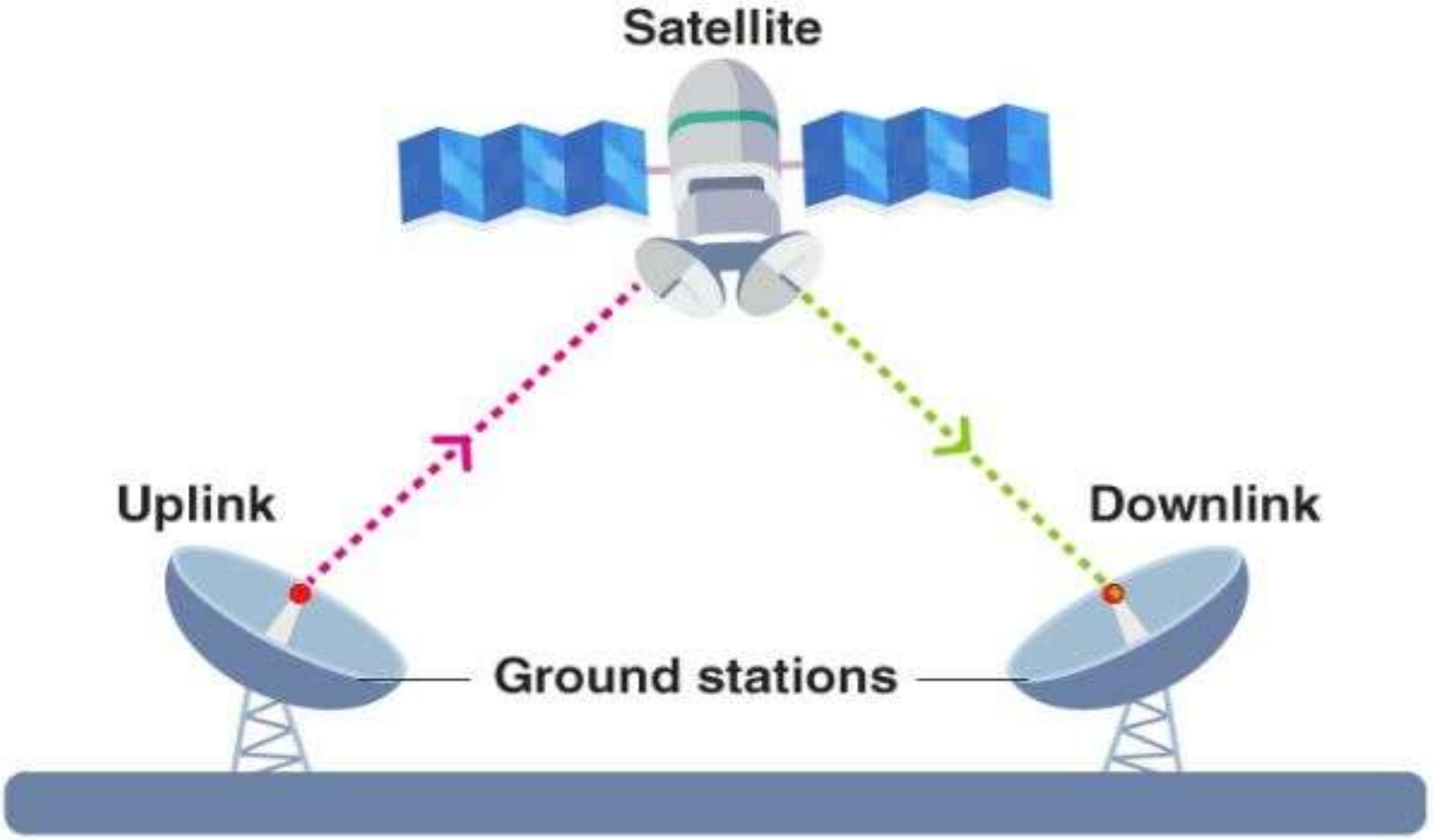
Disadvantages of Microwave transmission:

- **Eavesdropping**: An eavesdropping creates insecure communication. Any malicious user can catch the signal in the air by using its own antenna.
- **Out of phase signal**: A signal can be moved out of phase by using microwave transmission.
- **Susceptible to weather condition**: A microwave transmission is susceptible to weather condition. This means that any environmental change such as rain, wind can distort the signal.
- **Bandwidth limited**: Allocation of bandwidth is limited in the case of microwave transmission.

Unguided Transmission Media

Satellite Microwave Transmission





Satellite communication is transporting information from one place to another using a communication satellite in orbit around the Earth.

Satellite consists of three primary components

- **Uplink**
- **Transponders**
- **Downlink**

- Let's consider an example of signals from a television. In the first stage, the signal from the television broadcast on the other side of the earth is first beamed up to the satellite from the ground station on the earth. This process is known as uplink.
- The second stage involves transponders such as radio receivers, amplifiers, and transmitters. These transponders boost the incoming signal and change its frequency so that the outgoing signals are not altered. Depending on the incoming signal sources, the transponders vary.
- The final stage involves a downlink in which the data is sent to the other end of the receiver on the earth. It is important to understand that usually, there is one uplink and multiple downlinks.

Satellite Microwave Transmission

Advantages of Satellite Microwave Communication:

- The coverage area of a satellite microwave is more than the terrestrial microwave.
- The transmission cost of the satellite is independent of the distance from the centre of the coverage area.
- Satellite communication is **used in mobile and wireless communication applications.**
- It is easy to install.
- It is used in a wide variety of applications such as
- weather forecasting,
- radio
- TV signal broadcasting,
- mobile communication,
- Internet etc.

Satellite Microwave Transmission

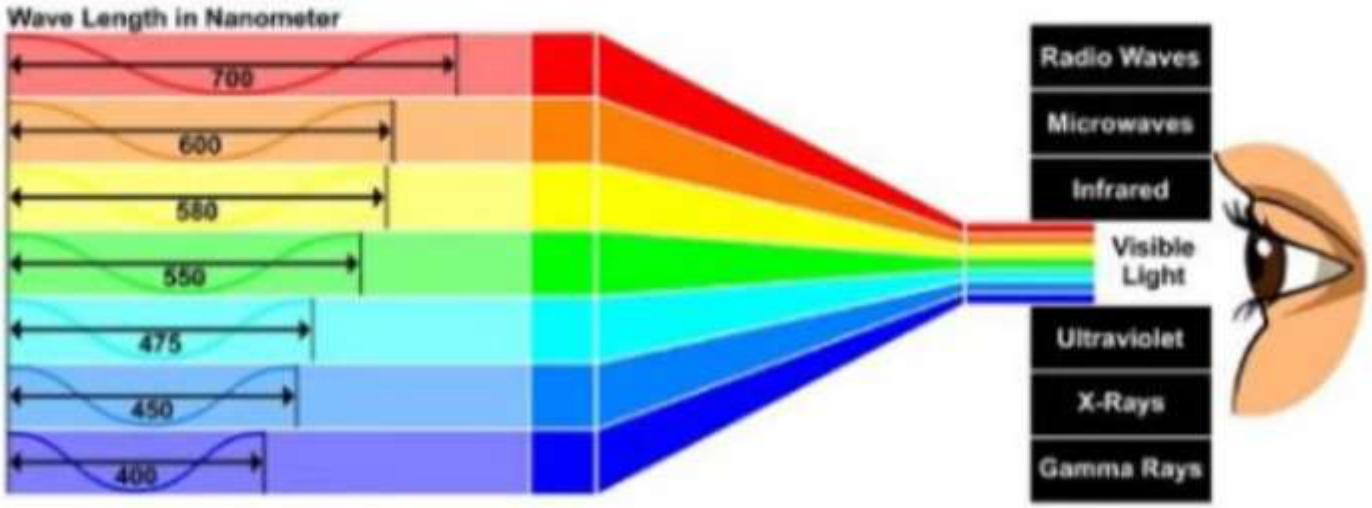
- **Disadvantages Of Satellite Microwave Communication**:
- Satellite designing and development requires more time and higher cost.
- The Satellite needs to be monitored and controlled on regular periods so that it remains in orbit.
- The life of the satellite is about **12-15 years**. Due to this reason, another launch of the satellite has to be planned before it becomes non-functional.

Below is the list of communication satellites along with their applications:

Satellite name	Launch date	Application
GSAT-30	Jan 17, 2020	Communication
GSAT-31	Feb 06, 2020	Communication
GSAT-15	Nov 11, 2015	Communication and navigation
GSAT-10	Sep 29, 2012	Communication and navigation
INSAT-3A	Apr 10, 2003	Communication and climate and environment
KALPANA-1	Sep 12, 2002	Communication and climate and environment

Unguided Transmission Media

Infared Waves:



- Infrared signals can be used for short-range communication using line of sight propagation and that should be in closed area not in open area.
- Examples of infrared waves
- TV Remote
- AC Remote
- Wire less Speakers
- Automatic doors

Infrared Waves:

- **Characteristics Of Infrared:**
- It supports high bandwidth, and hence the data rate will be very high.
- Infrared waves cannot penetrate the walls. Therefore, the Infrared communication in one room cannot be interrupted by the nearby rooms.
- An Infrared communication provides better security with minimum Interference.
- Infrared communication is unreliable outside the building because the sun rays will interfere with the infrared waves.