

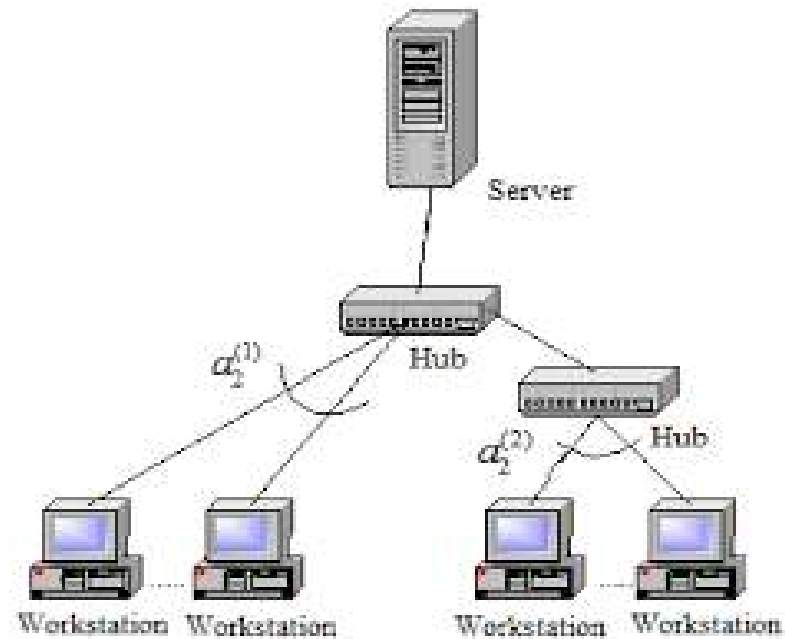
Unit I
Introduction to Computer Network
Midsem:70
Insem:30

Introduction

- 1) Network**
- 2) Computer Network**
- 3) Components of Data Communication**
- 4) Challenges for building network**
- 5) Types of Network**

1) Network

- ▶ Network is a communication system which support many users
- ▶ **The interconnection of one station to many station is called networking**



2) Computer Network

- ▶ **It is a group of interconnected computers .It allows computer to communicate with each other and to share resources and information.**
- ▶ Connection between computer can be done with fibre optics,copper wire,microwave or communication satellite.
- ▶ Data is transferred in the form of packets .

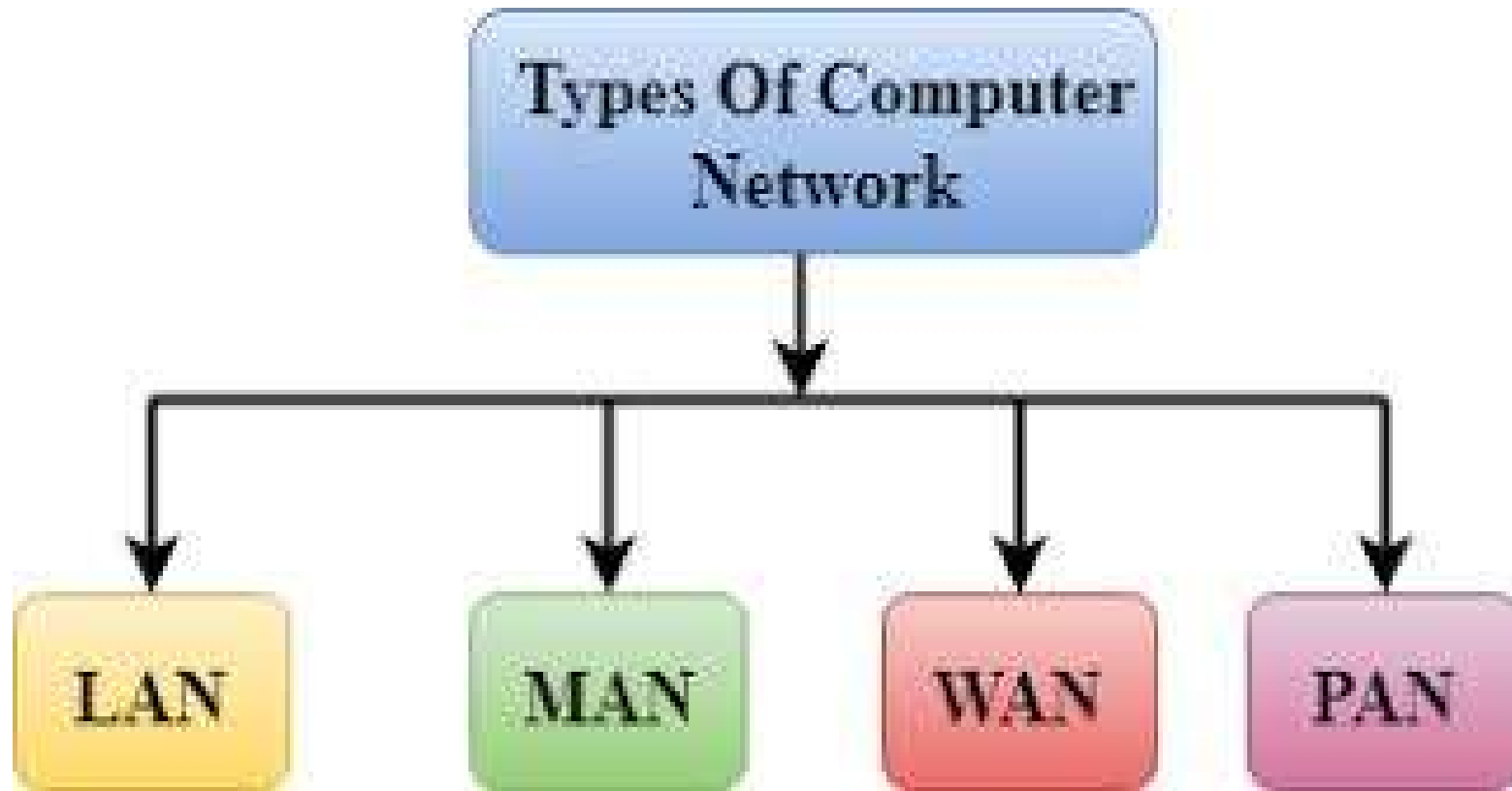
3) Components of Data Communication

- ▶ 1) sender
- ▶ 2) receiver
- ▶ 3) Transmission medium
- ▶ 4) protocol : programmer and network are connected together by certain rules called protocol
- ▶ 5) Message: It is actual data or information to be sent.

4) Challenges for building network

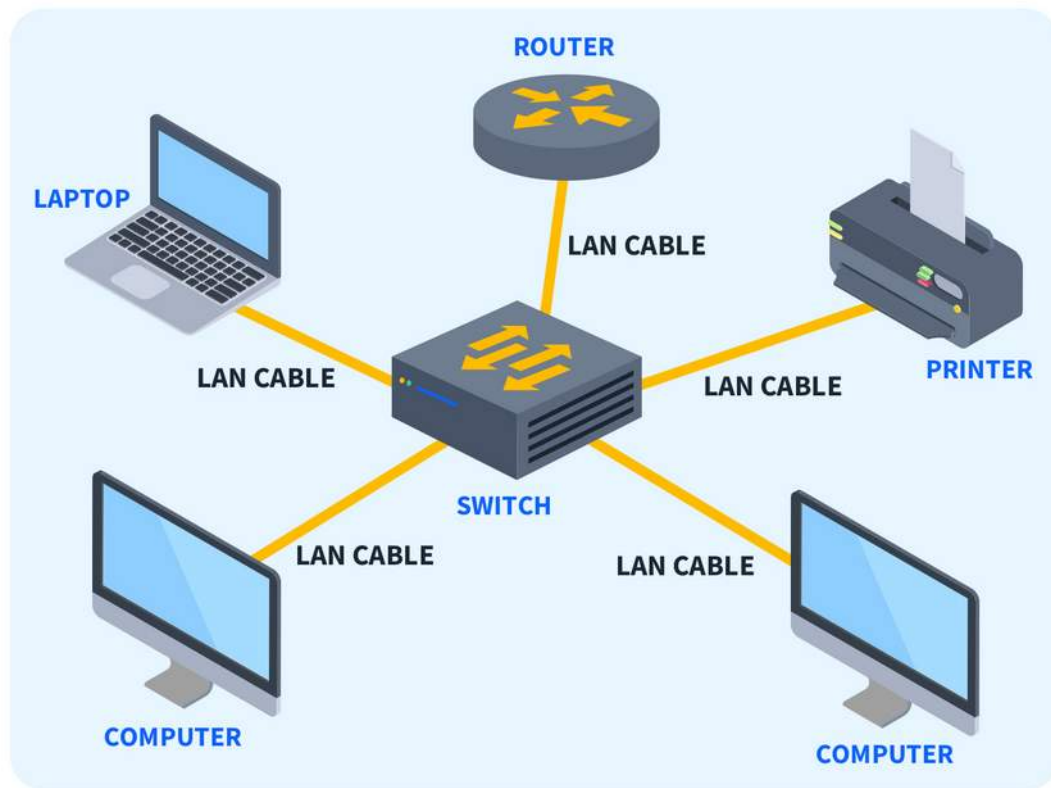
- ▶ 1) Scalability of network
- ▶ 2) security in computer network
- ▶ 3) Reliability
- ▶ 4) privacy
- ▶ 5) protocol


5) Types of Network



1) LAN

- ▶ LAN stands for **Local Area Network**
- ▶ It is designed **for small physical areas** such as office, group of building, or a small factory
- ▶ LAN are widely used because it is **easy to design and troubleshoot.**
- ▶ **Personal computer & workstations** are connected to each other through LAN's
- ▶ We can use **different types of topologies through LAN.** these are star, ring ,bus , trees
- ▶ LAN can be simple network like **connecting two computers to share files & network**



- 
- ▶ **Applications of LAN**
 - ▶ File transfer & access
 - ▶ Personal computing
 - ▶ Office Automation
 - ▶ Distributed Computing
 - ▶ Word & text processing



- ▶ **Advantages**

- ▶ Cost reduction

- ▶ Increased information exchange

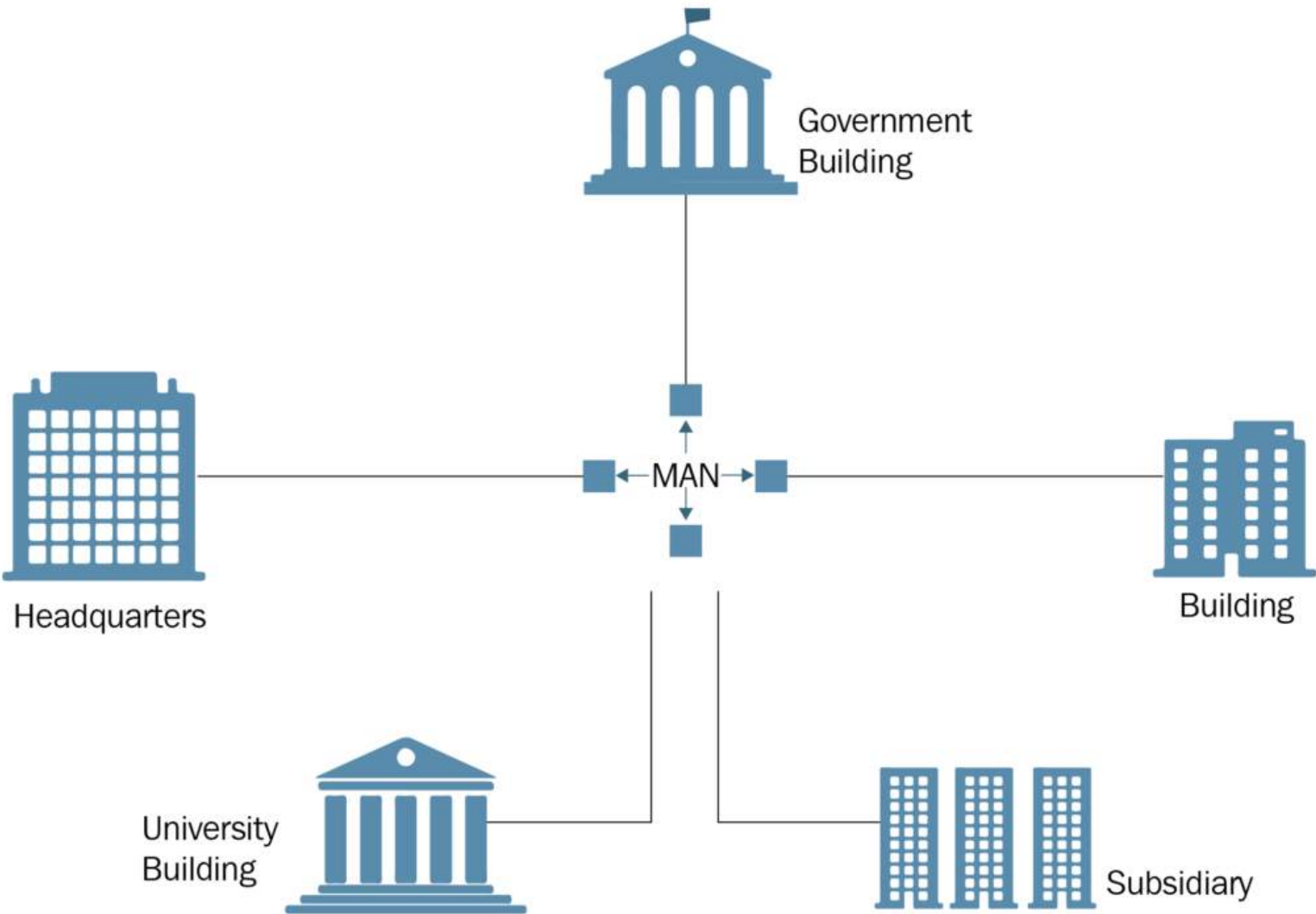
- ▶ Automate communication

- ▶ **Disadvantages:**

- ▶ Networks are difficult to setup & need to maintain by skill technicians.

- ▶ If file server develops a serious fault all the users are affected.

MAN(Metropolitan Area Network)



- ▶ A metropolitan area network (MAN) is a computer network that **connects computers within a metropolitan area,**
- ▶ which could be a **single large city, multiple cities and towns,** or any given large area with multiple buildings.
- ▶ A MAN is **larger than a local area network (LAN) but smaller than a wide area network (WAN).**
- ▶
example: Some of those are: **Cable TV network.**
Telephone networks. DSL line.

MAN Advantages:

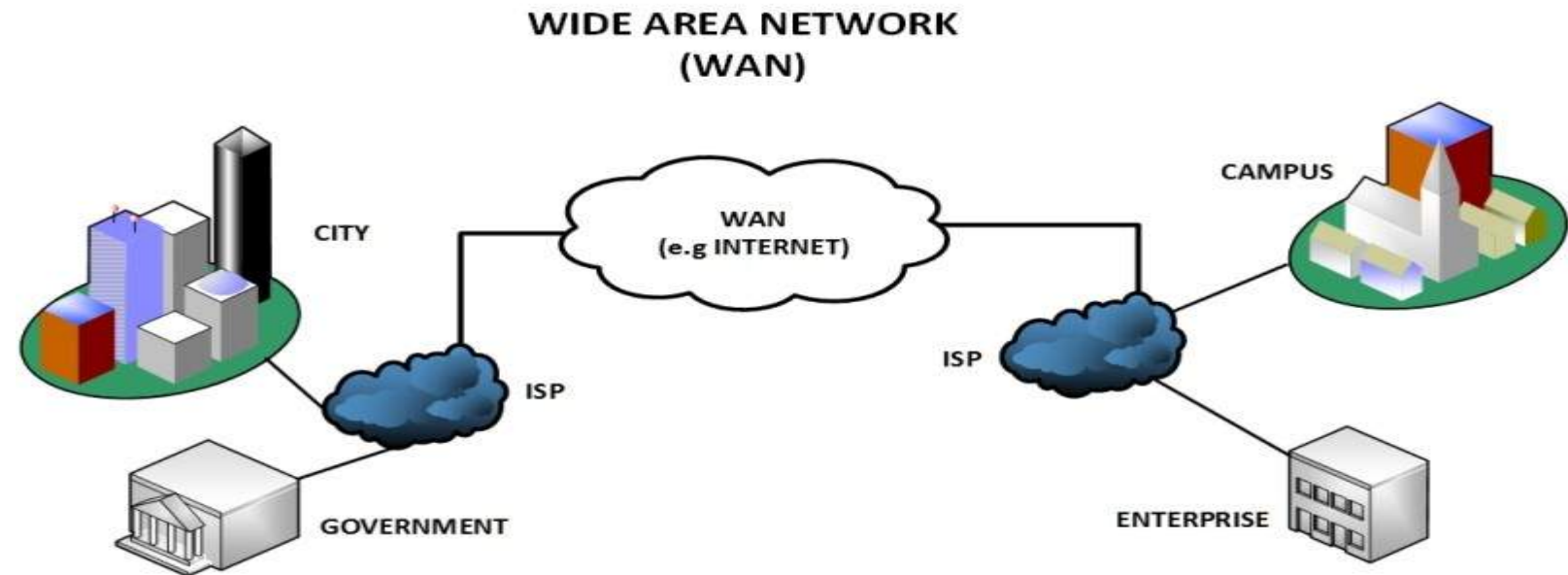
- ▶ It provides **good backbone** for large network.
- ▶ It can send data in **both directions** at the same time.
- ▶ Metropolitan Area Network **allows people to connect LANs.**
- ▶ offers **greater security** than a WAN.

MAN Disadvantages:

- ▶ The **data rate is slow** in a Metropolitan Area Network compared to LAN.
- ▶ Compared to LAN, **more cable is required to set up** a Metropolitan Area Network.
- ▶ this network have multiple LANs, it is **difficult to keep hackers out.**

WAN(Wide Area Network)

- ▶ WAN can be **private or it can be public.**
- ▶ It is used for the network that **covers large distance such as states of country**
- ▶ It is **not easy to design & maintain**
- ▶ **Communication medium used by LAN are PSTN or satellite links**



Advantages and Disadvantages of WAN

Advantages

1. Share Resources
2. Scalability and flexibility
3. Cost reduction
4. Improved security
5. Access to a wide range of services



Disadvantages

1. Increased latency
2. Higher costs
3. Security risks
4. slower Issue
5. Complexity

Comparison of LAN, MAN, WAN

Parameters	LAN	MAN	WAN
Ownership of Network	Private	Private / Public	Private / Public
Geographical Area	1KM to 10 KM	10 KM to 100 KM	Beyond 100 KM
Design and maintenance	Easy	Difficult	Difficult
Propagation Delay	Short	Moderate	Long
Speed	High	Moderate	Low
Fault Tolerance	More Tolerant	Less Tolerant	Less Tolerant
Congestion	Less	More	More
Used for	College, School, Hospital.	Small towns, City.	Country/Continent.

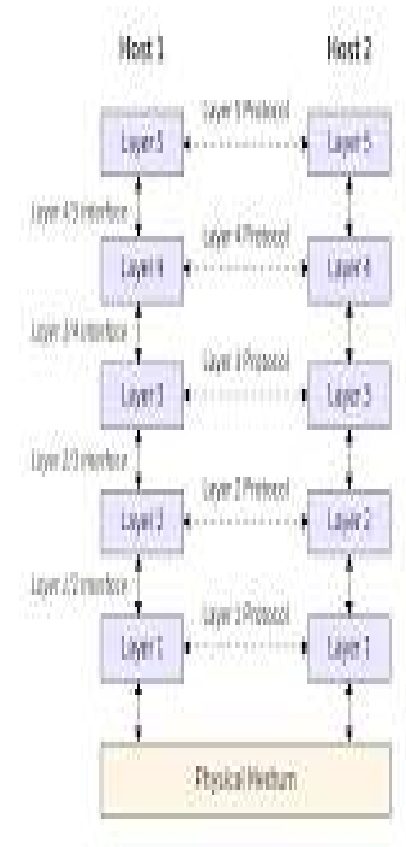
Wireless Network

- ▶ A wireless LAN uses radio waves as its carrier.
- ▶ A wireless local-area network (WLAN) is a group of co located computers
- ▶ or other devices that form a network based on radio transmissions rather than wired connections.
- ▶ A Wi-Fi network is a type of WLAN
- ▶ anyone connected to Wi-Fi while reading this webpage is using a WLAN.



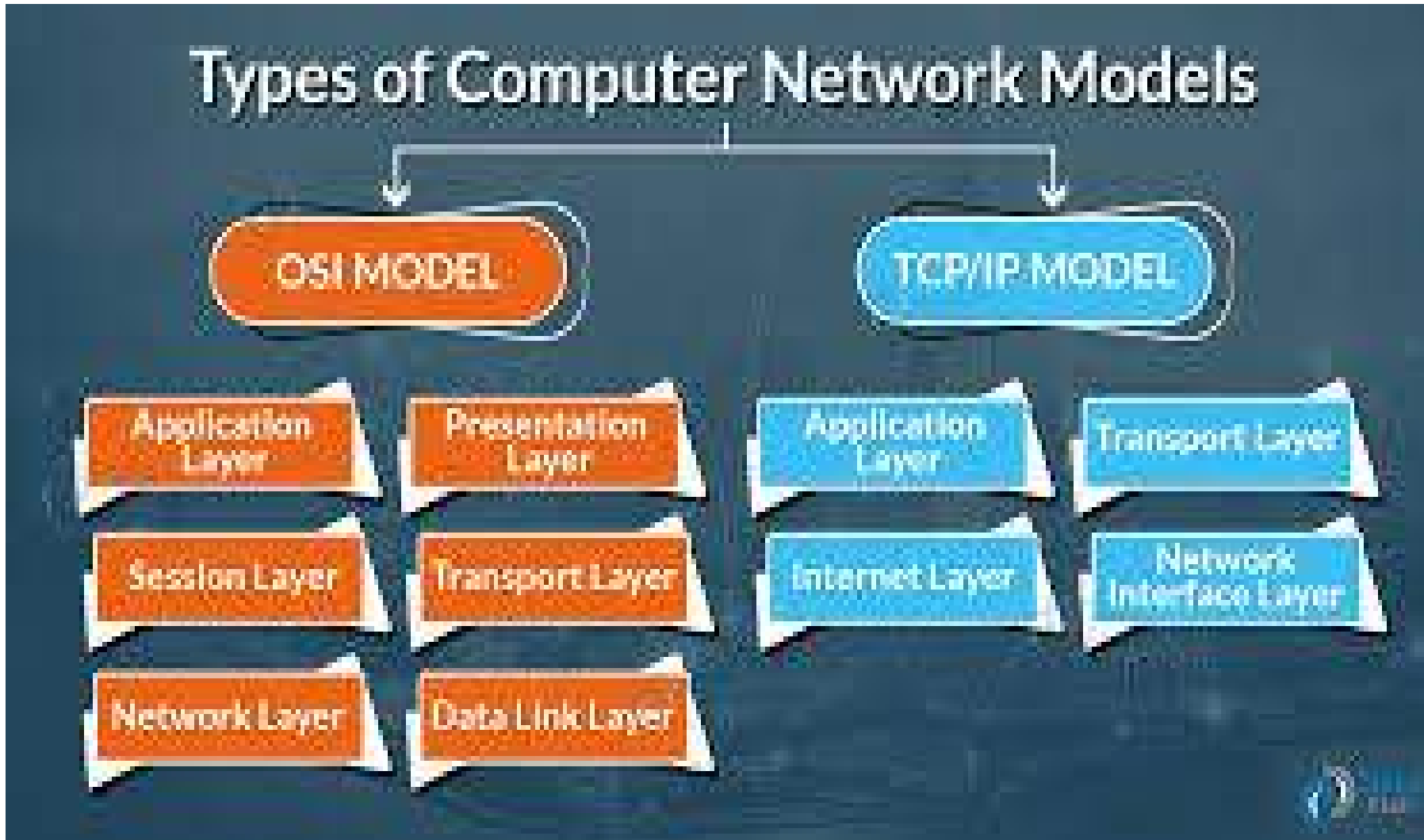
Protocol Hierarchies

- ▶ Most of the **network organized in the form of series of layers or levels** as shown in the figure in order to reduce the design complexity.
- ▶ The purpose of **each layer is to offer certain services to the higher layer.**
- ▶ **Layer n on source machine will communicate with layer n on the destination machines.**
- ▶ The process of establishing a link between two devices to communicate & share information is complicated.



- ▶ **Data transfer**
- ▶ Data is not get transferred directly from layer n of one machine to layer n of other machine.
- ▶ The data is passed onto the lower layer until the lowest layer is reached.
- ▶ Below layer 1 physical medium is lies such as co-axial cable,through which actual data transfer is done.
- ▶ Thi s type of communication is known as virtual communication.

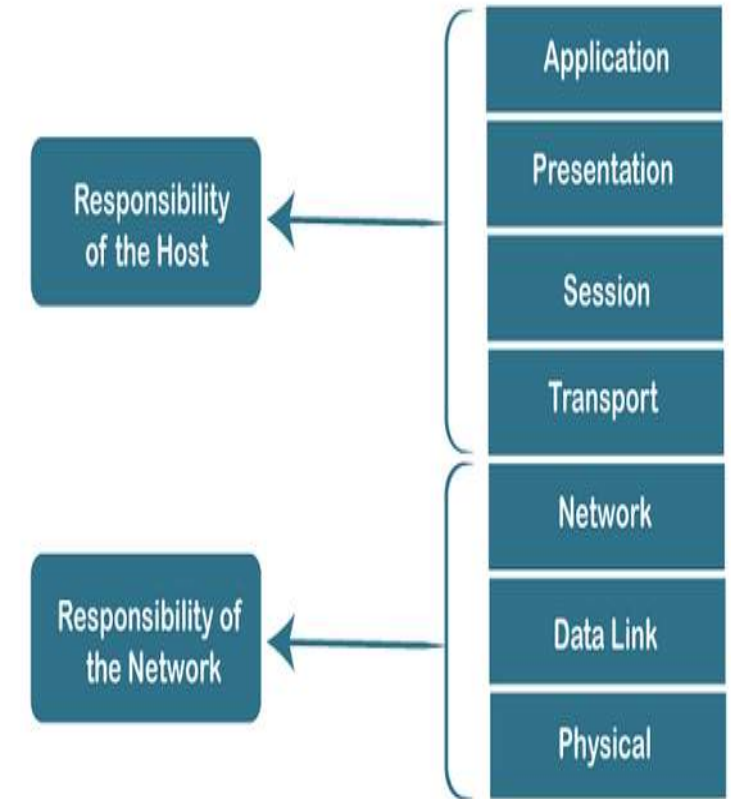
Network Models



OSI Model

- ▶ **OSI stands for Open Systems Interconnection**
- ▶ where open stands to say non-proprietary.
- ▶ 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.**
- ▶ The OSI reference model was developed by **ISO – ‘International Organization for Standardization’, in the year 1984.**
- ▶ The OSI divided into **two part:1)Upper Layer 2)Lower Layer**

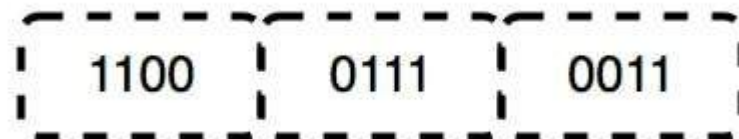
Characteristics of OSI Model



- ▶ The upper layer of **OSI model mainly deals with application related issues.** & they are implemented only in the **S/W.**
- ▶ The lower layer of **OSI model deals with the data transfer issues.** The data link layer & the physical layer implemented in **H/W and S/W.**

Physical Layer - Layer 1

- ▶ 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.**



1100 0111 0011

Functions of 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.

Layer2-Data link layer

- ▶ The data link layer is the **second layer** from the bottom in the OSI (Open System Interconnection) network architecture model.
- ▶ It is responsible for the **node-to-node delivery of data.**
- ▶ Its major role is to **ensure error-free transmission of information.**
- ▶ DLL is also responsible for **encoding, decoding,** and **organizing the outgoing and incoming data.**

Sub-Layers of The Data Link Layer

- ▶ The data link layer is further divided into two sub-layers, which are as follows:

1) Logical Link Control (LLC)

- ▶ the data link layer deals with multiplexing, the flow of data among applications and other services, and **LLC is responsible for providing error messages and acknowledgments** as well.

2) Media Access Control (MAC)

- ▶ MAC sublayer manages the device's interaction, **responsible for addressing frames**, and **also controls physical media access.**

Functions of Data link layer

- ▶ 1)framing
- ▶ 2)physical addressing
- ▶ 3)flow control
- ▶ 4)error control
- ▶ 5)access control

Network Layer - Layer 3

- ▶ 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.

Functions of the Network Layer

- ▶ **Routing:** The network layer protocols determine **which route is suitable from source to destination**
- ▶ **Logical Addressing:** To identify each device inter-network 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.

Transport Layer - Layer 4

- ▶ **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 numbers 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. 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**.

Session Layer - Layer 5

- ▶ This layer is responsible for the **establishment of connection, maintenance of sessions, and authentication**, and also **ensures security**.
- ▶ **Functions of the Session Layer**
- ▶ **Session Establishment, Maintenance, and Termination:** The layer allows the two processes to establish, use, and terminate a connection.
- ▶ **Synchronization:** These synchronization points help to identify the error so that the data is **re-synchronized properly**
- ▶ **Dialog Controller:** The session layer allows two systems to start communication with each other in half-duplex or full-duplex.

Presentation Layer - Layer 6

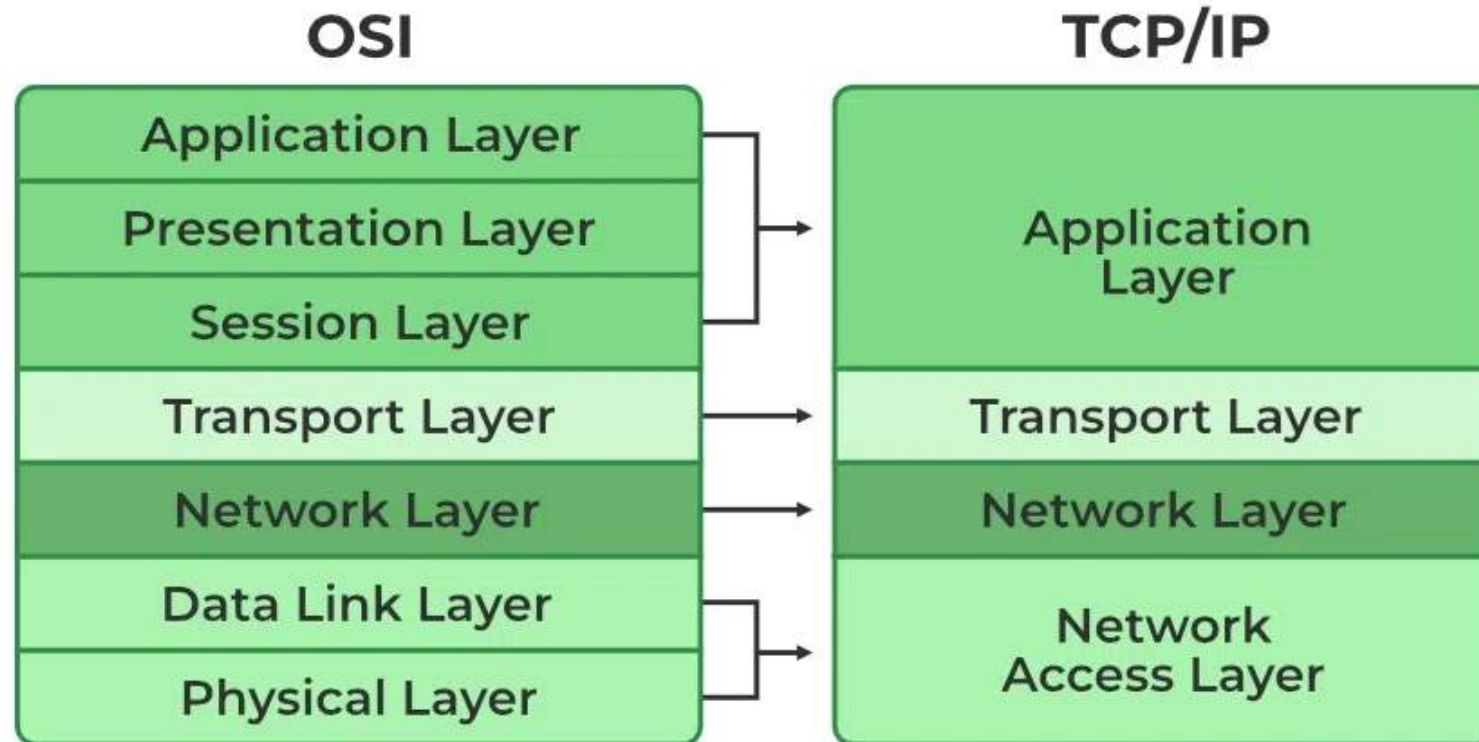
- ▶ The presentation layer is also called the **Translation layer**.
- ▶ The data from the **application layer** is **extracted** here and **manipulated as per the required format to transmit over the network**.
- ▶ **Functions of the Presentation Layer**
 - **Translation:** For example, [ASCII to EBCDIC](#).
 - **Encryption/ Decryption:** The encrypted data is known as the ciphertext and the decrypted data is known as plain text.
 - **Compression: Reduces the number of bits** that need to be transmitted on the network.

Functions of the Application Layer

- ▶ **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.

- ▶ **Application Layer:** Applications create the data.
- ▶ **Presentation Layer:** Data is formatted and encrypted.
- ▶ **Session Layer:** Connections are established and managed.
- ▶ **Transport Layer:** Data is broken into segments for reliable delivery.
- ▶ **Network Layer:** Segments are packaged into packets and routed.
- ▶ **Data Link Layer:** Packets are framed and sent to the next device.
- ▶ **Physical Layer:** Frames are converted into bits and transmitted physically.

TCP/IP model



1. Network Access Layer

- ▶ This layer is responsible for **generating the data and requesting connections.**
- ▶ **“Error prevention” and “framing”** are also provided by this layer. Point-to-Point Protocol (PPP) framing and **Ethernet IEEE 802.2 framing** are **two examples of data-link layer protocols.**

2. Internet Layer

- ▶ It defines the protocols which are responsible for the **logical transmission of data over the entire network.**
- ▶ **IP:** IP stands for **Internet Protocol** and it is responsible for **delivering packets from the source host to the destination** host by looking at the IP addresses in the packet headers. **IP has 2 versions: IPv4 and IPv6.** **IPv4** is the one that **most websites are using currently.** But **IPv6 is growing** as the number of IPv4 addresses is limited in number when compared to the number of users.
- ▶ **ICMP:** ICMP stands for **Internet Control Message Protocol.** It is encapsulated within IP datagrams and is **responsible for providing hosts with information about network problems.**
- ▶ **ARP:** ARP stands for **Address Resolution Protocol.** Its job is **to find the hardware address of a host from a known IP address.** ARP has several types: Reverse ARP, Proxy ARP, Gratuitous ARP, and Inverse ARP.

- ▶ **Example:** Imagine that you are using a computer to send an email to a friend. When you click “send,” the email is broken down into smaller packets of data, which are then sent to the Internet Layer for routing. The Internet Layer assigns an IP address to each packet and uses routing tables to determine the best route for the packet to take to reach its destination. **The packet is then forwarded to the next hop on its route until it reaches its destination. When all of the packets have been delivered, your friend’s computer can reassemble them into the original email message.**
- ▶ In this example, the Internet Layer plays a crucial role in delivering the email from your computer to your friend’s computer. It uses IP addresses and routing tables to determine the best route for the packets to take, and it ensures that the packets are delivered to the correct destination. Without the Internet Layer, it would not be possible to send data across the Internet.

3. Transport Layer

- ▶ The TCP/IP transport layer protocols exchange data receipt **acknowledgments and retransmit missing packets** to ensure that packets arrive in order and without error.
- ▶ **TCP:** Applications can interact with one another using TCP as though they were physically connected by a circuit. TCP transmits data in a way that resembles character-by-character transmission rather than separate packets. **A starting point that establishes the connection, the whole transmission in byte order, and an ending point that closes the connection make up this transmission.**
- ▶ **UDP:** The datagram delivery service is provided by UDP, the other transport layer protocol. **Connections between receiving and sending hosts are not verified by UDP. Applications that transport little amounts of data use UDP** rather than TCP because it eliminates the processes of establishing and validating connections.

4. Application Layer

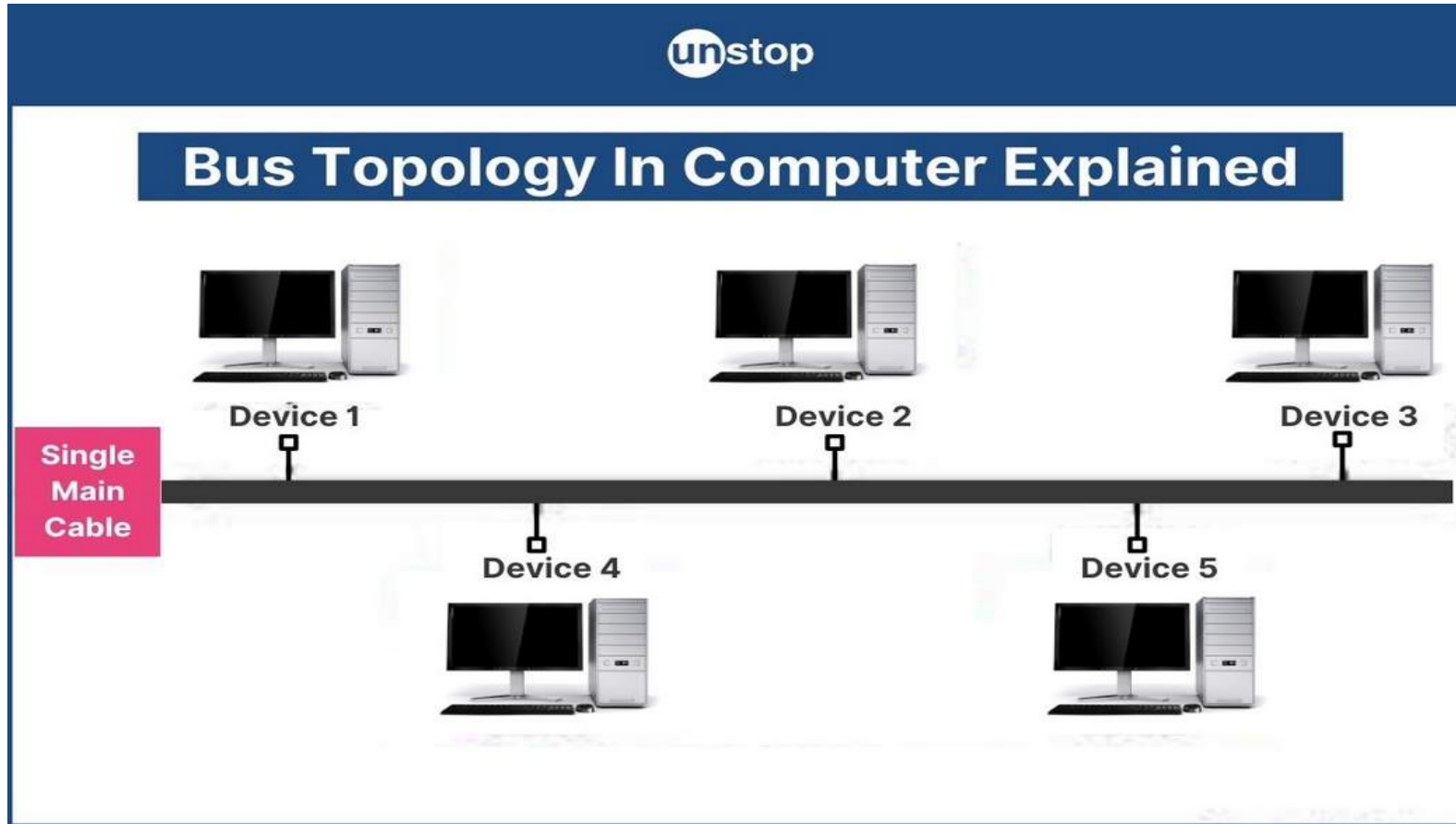
- ▶ This layer is analogous to the transport layer of the OSI model. **It is responsible for end-to-end communication and error-free delivery of data.**
- ▶ **HTTP and HTTPS:** HTTP stands for Hypertext transfer protocol. It is used by the World Wide Web to manage communications between web browsers and servers.. It is efficient in cases where the browser needs to fill out forms, sign in, authenticate, and carry out bank transactions.
- ▶ **SSH:** SSH stands for Secure Shell. It is a terminal emulations software similar to Telnet. The reason SSH is preferred is because of its ability to maintain the encrypted connection. **It sets up a secure session over a TCP/IP connection.**
- ▶ **NTP:** NTP stands for Network Time Protocol. It is used to synchronize the clocks on our computer to one standard time source. It is very useful in situations like bank transactions. Assume the following situation without the presence of NTP. **Suppose you carry out a transaction, where your computer reads the time at 2:30 PM while the server records it at 2:28 PM. The server can crash very badly if it's out of sync.**

- ▶ **Example: Consider a network with two hosts, A and B. Host A wants to send a file to host B. The host-to-host layer in host A will break the file into smaller **segments**, add error correction and flow control information, and then transmit the segments over the network to host B. **The host-to-host layer in host B will receive the segments, check for errors, and reassemble the file. Once the file has been transferred successfully, the host-to-host layer in host B will acknowledge receipt of the file to host A.****
- ▶ In this example, the host-to-host layer is responsible for providing a reliable connection between host A and host B, breaking the file into smaller segments, and reassembling the segments at the destination. It is also responsible for multiplexing and demultiplexing the data and providing end-to-end communication between the two hosts.

Difference between TCP/IP and OSI Model

Parameters	OSI Model	TCP/IP Model
No. of Layers	There are 7 layers.	There are 4 layers.
Acronyms	OSI stands for open system interconnection.	TCP/IP stands for transmission control protocol/internet protocol
Developed by	ISO	Department of Defense (DoD)
Layer Separation	OSI model has a separate Presentation layer and Session layer.	TCP/IP does not have a separate Presentation layer or Session layer.
Protocol implementation	Model was defined before implementation takes place.	Model defines after protocol were implemented.
Model Concept	based on three concept i.e. Service, interface and protocol.	It did not distinguish between service, interface and protocol.
Reliable delivery	It gives guarantee of reliable delivery of packet.	It does not give guarantee of reliable delivery of packet.

Network topology 1) Bus topology



- ▶ A Bus Topology is one of them.
- ▶ **All of the devices in a bus topology network are linked together by a single cable, which is referred to as a “bus” and the cable is known as backbone cable.**
- ▶ **All of the network’s devices can simultaneously receive the same signal due to the shared communication medium** provided by this connection.
- ▶ **Bus topology** carries transmitted data through the cable because data reaches each node,
- ▶ the node checks the destination address (IP address) to determine if it matches their address. then they process further. If the address does not match with the node, the node does nothing more.

Advantages of Bus Topology

- ▶ It is the **easiest network topology** for linearly connecting peripherals or computers.
- ▶ It works **very efficiently** well when there is a small network.
- ▶ The **length of cable required is less** than a star topology.
- ▶ It is **easy to connect or remove devices** in this network without affecting any other device.
- ▶ Very **cost-effective as compared to other network topology** i.e. mesh and star
- ▶ It is **easy to understand** topology.
- ▶ **Easy to expand** by joining the two cables together.

Disadvantages of Bus Topology

- ▶ Bus topology is **not good for large networks**.
- ▶ **Identification of problems becomes difficult** if the whole network goes down.
- ▶ **Troubleshooting individual device issues is very hard**.
- ▶ **Need terminators** are required at both ends of the main cable.

- ▶ If the **main cable is damaged**, the whole network fails or splits into two.
- ▶ **Packet loss is high**.
- ▶ This network topology is **very slow** as compared to other topologies.

Applications of Bus Topology

- ▶ **Local Area Networks (LANs):** Bus topology was traditionally utilized in Ethernet LANs,
- ▶ **Industrial Control Systems:** In industrial control system, bus topology is frequently used for connecting sensors, actuators, and different devices in distributed manipulate systems.
- ▶ **Instrumentation Networks:** Bus topology is appropriate for connecting devices, meters, and records acquisition gadgets in laboratory or commercial environments.
- ▶ **Building Automation Systems:** Bus topology is employed in building automation and HVAC (heating, ventilation, and air conditioning) structures to attach sensors, thermostats, actuators, and other manage devices.
- ▶ **Telecommunications Networks:** Bus topology has traditionally been utilized in telephone networks and early records transmission systems.

2) Ring Topology



- ▶ In this each device is connected to with its **exactly two** neighboring devices,
- ▶ like points on a circle which forms like a ring structure.
- ▶ A number of **repeaters** are used for Ring topology with a large number of nodes to send data and to **prevent data loss** repeaters are used in this network.
- ▶ **In this packets travels from one device to another until they reach the desired destination.** In this data travels in unidirectional forms means in only one direction but it can also do **bidirectional** by having 2 connections between each Network Node, it is called Dual Ring Topology. It is used in LANs and WANs depending on the card of network in the computer.

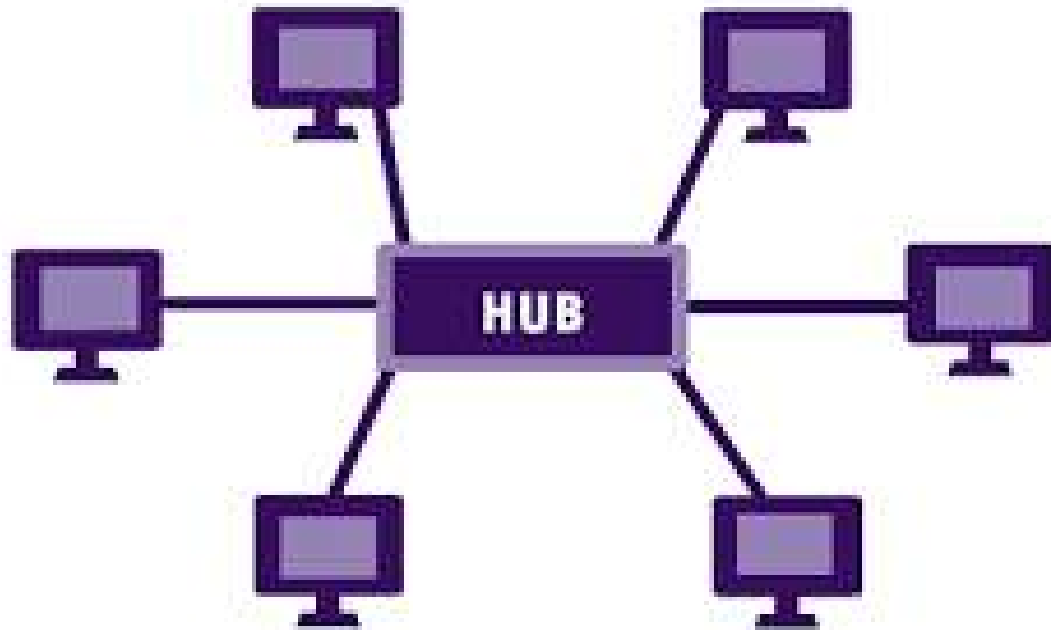
Advantages of Ring topology :

- ▶ In this **data flows in one direction** which reduces the chance of packet collisions.
- ▶ In this topology **additional workstations can be added** after without impacting performance of the network.
- ▶ There is **no need of server** to control the connectivity among the nodes in the topology.
- ▶ It is **cheap to install and expand**.
- ▶ **Speed to transfer the data is very high** in this type of topology.
- ▶ Due to the presence of token passing the **performance of ring topology becomes better than bus topology** under heavy traffic.
- ▶ **Easy to manage**.

Disadvantages of Ring topology :

- ▶ Due to the **Uni-directional Ring**, a **data packet (token) must have to pass through all the nodes.**
- ▶ If **one workstation shuts down**, it affects whole network or if a node goes down entire network goes down.
- ▶ It is **slower in performance** as compared to the bus topology
- ▶ **It is Expensive.**
- ▶ **Addition and removal of any node** during a network is **difficult** and may cause issue in network activity.
- ▶ **Difficult to troubleshoot the ring.**
- ▶ **Total dependence in on one cable.**

3)Star topology



- ▶ **all the nodes in a star topology are connected to the Hub,**
- ▶ **star topology are connected to the central node called the Hub is responsible for the transmission of the data.** For example- when any node wants to transmit data to another node it first transmits data to the central node which then transfers the data to all the nodes on the network. Once the node receives the data then it checks for the destination address if the address matches the data is accepted otherwise data is rejected.

Advantages of Star Topology

- ▶ **It is very reliable** – if one cable or device fails then all the others will still work.
- ▶ It is high-performing as **no data collisions can occur**.
- ▶ **It is less expensive** because each device only needs one I/O port and wishes to be connected to the hub with one link.
- ▶ **Robust in nature.**
- ▶ **Easy fault detection** because the links are often easily identified.
- ▶ **No disruptions to the network when connecting or removing devices.**
- ▶ Each device requires just one **port** i.e. to attach to the hub.
- ▶ **If N devices are connected to each other in star, then the amount of cables required to attach them is N.** So, it's easy to line up.

Disadvantages of Star Topology

- ▶ Requires **more cable than a linear bus.**
- ▶ If the **connecting network device (network switch) fails**, the nodes attached are disabled and can't participate in network communication.
- ▶ **More expensive** than linear bus topology due to the value of the connecting devices (network switches).
- ▶ If the **hub goes down everything goes down**, none of the devices can work without the hub.
- ▶ **Extra hardware is required** (hubs or switches) which adds to the cost.
- ▶ Performance is predicated on the one concentrator i.e. hub.

4) Mesh Topology



- ▶ In mesh, **all the computers are interconnected to every other** during a network.
- ▶ Each **computer not only sends its own signals but also broadcast** data from other computers.
- ▶ **The nodes are connected to every other completely via a dedicated link** during which information is travel from nodes to nodes and there are $N(N-1)/2$ links in mesh
- ▶ **if there are N nodes. Every node features a point-to-point connection to the opposite node.** The connections within the mesh are often wired or wireless.

Advantages of Mesh Topology :

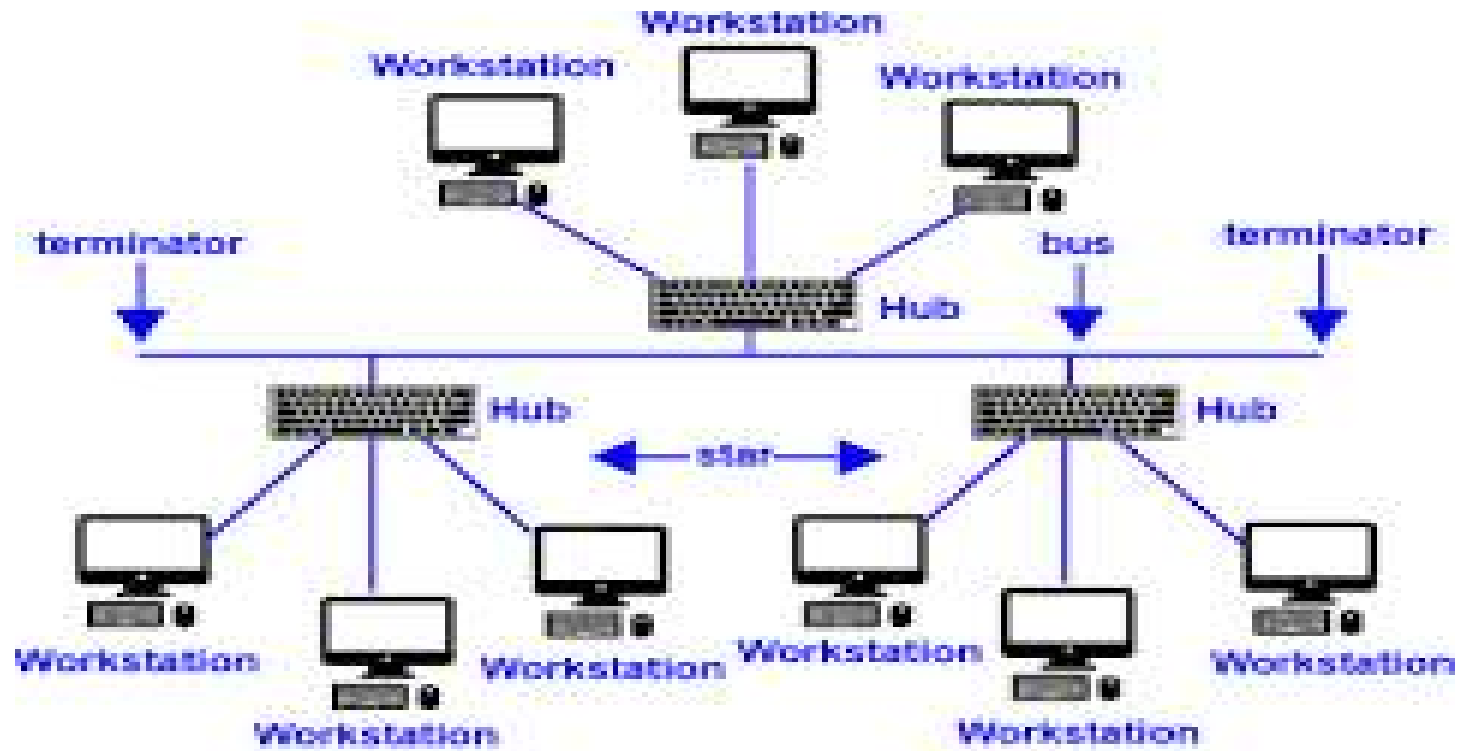
- ▶ **Failure during a single device** won't break the network.
- ▶ **There is no traffic problem** as there is a dedicated point to point links for every computer.
- ▶ **Fault identification** is straightforward.
- ▶ This topology **provides multiple paths to succeed in the destination** and tons of redundancy.
- ▶ It provides **high privacy and security**.
- ▶ **Adding new devices** won't disrupt data transmissions.
- ▶ This topology has **robust features** to beat any situation.
- ▶ A mesh **doesn't have a centralized authority**.

Disadvantages of Mesh

► Topology :

- It's **costly** as compared to the opposite network topologies i.e. **star, bus, point to point topology**.
- Installation is extremely **difficult** in the mesh.
- **Power requirement is higher** as all the nodes will need to remain active all the time and share the load.
- Complex process.
- There is a **high risk** of redundant connections.
- **Maintenance needs** are challenging with a mesh.

5) Tree Topology



TREE TOPOLOGY

- ▶ Tree Topology is a topology which is having a tree structure in which all the computers are connected like the branches which are connected with the tree. In Computer Network, tree topology is called a combination of a Bus and Star network topology. The main advantages of this topology are that it is very flexible and also has better scalability. Tree network topology is considered to be the simplest topology in all the topologies which is having only one route between any two nodes on the network. The pattern of connection resembles a tree in which all branches spring from one root hence (Tree Topology). Tree topology is one of the most popular among the five network topologies.

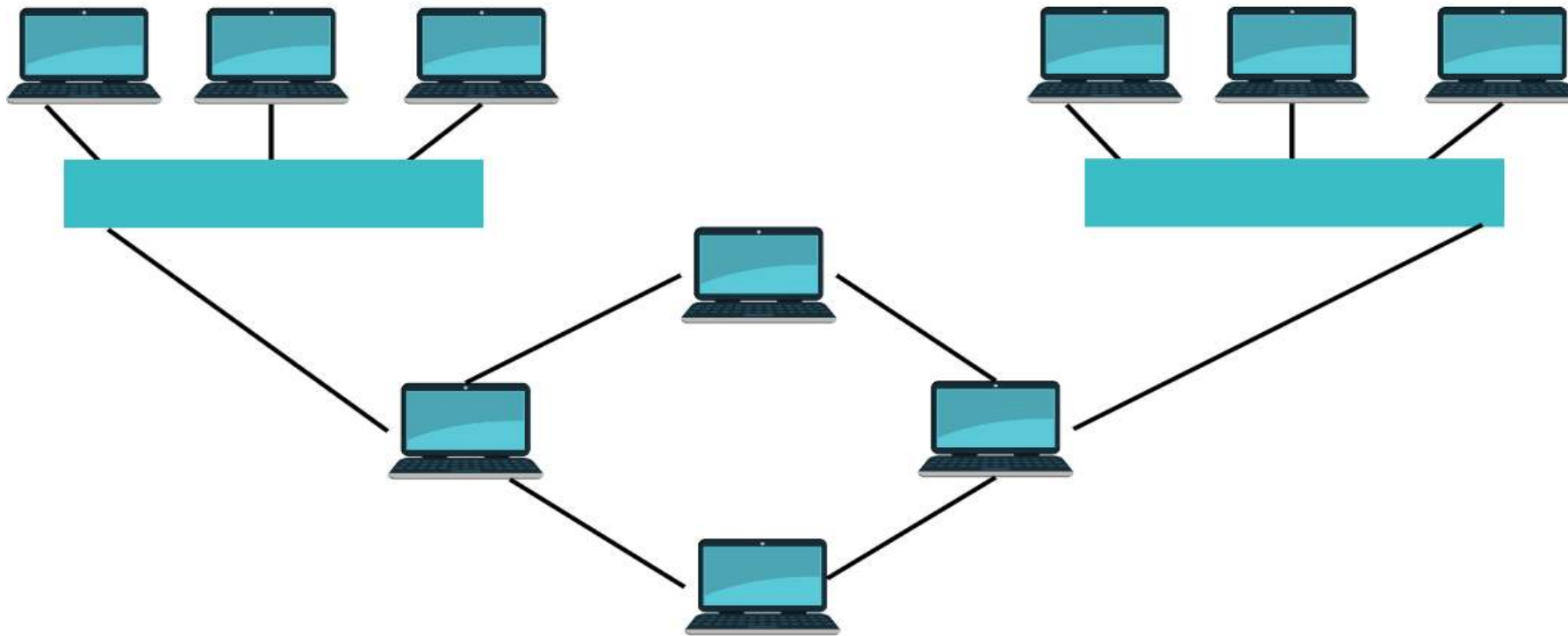
Advantages of Tree Topology :

- ▶ This topology is the combination of bus and star topology.
- ▶ This topology provides a hierarchical as well as central data arrangement of the nodes.
- ▶ As the leaf nodes can add one or more nodes in the hierarchical chain, this topology provides high scalability.
- ▶ The other nodes in a network are not affected if one of their nodes gets damaged or does not work.
- ▶ Tree topology provides easy maintenance and easy fault identification can be done.
- ▶ A callable topology. Leaf nodes can hold more nodes.
- ▶ Supported by several hardware and software vendors.
- ▶ Point-to-point wiring for individual segments.
- ▶ Tree Topology is highly secure.
- ▶ It is used in WAN.
- ▶ Tree Topology is reliable.

Disadvantages of Tree Topology :

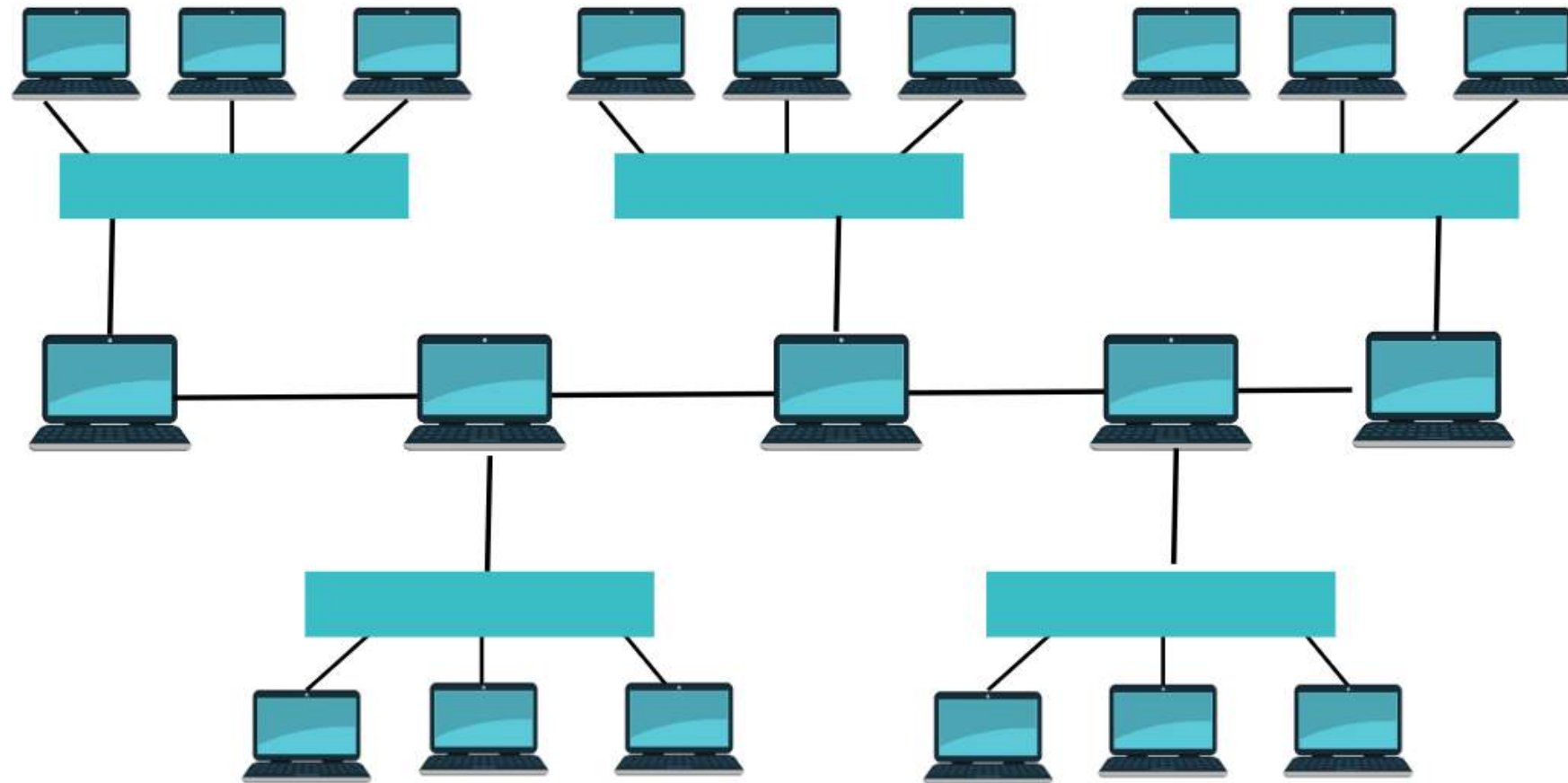
- ▶ This network is very difficult to configure as compared to the other network topologies.
- ▶ The length of a segment is limited & the limit of the segment depends on the type of cabling used.
- ▶ Due to the presence of a large number of nodes, the network performance of tree topology becomes a bit slow.
- ▶ If the computer on the first level is erroneous, the next-level computer will also go under problems.
- ▶ Requires a large number of cables compared to star and ring topology.
- ▶ As the data needs to travel from the central cable this creates dense network traffic.
- ▶ The Backbone appears as the failure point of the entire segment of the network.
- ▶ The establishment cost increases as well.

6)Hybrid Topology . **Star-Ring Hybrid Topology**



- ▶ The combination of star and ring topology forms a star-ring topology.
- ▶ **Two or more than two star topologies are connected together through a ring topology using a wired connection.**
- ▶ **The flow of data in star-ring topology is bidirectional or unidirectional.**
- ▶ **If any node of the original ring topology gets fail the bidirectional data flow provides** that there will be no effect on the rest of the data in network flow.

Star-Bus Hybrid Topology



- ▶ The **combination of star and bus topology is known as star-bus hybrid topology.**
- ▶ **Two or more star topologies are connected together with the help of bus topology** through a wired connection.
- ▶ The bus topology can interrelate different star topologies and offers with a backbone structure.
- ▶ The **entire network is not affected in case of any node failure.**
- ▶ The **failed node can be then easily replaced**
- ▶ offers with a **easy way for adding or deleting the nodes.**
- ▶ The overall network can be easily modified according to the need.

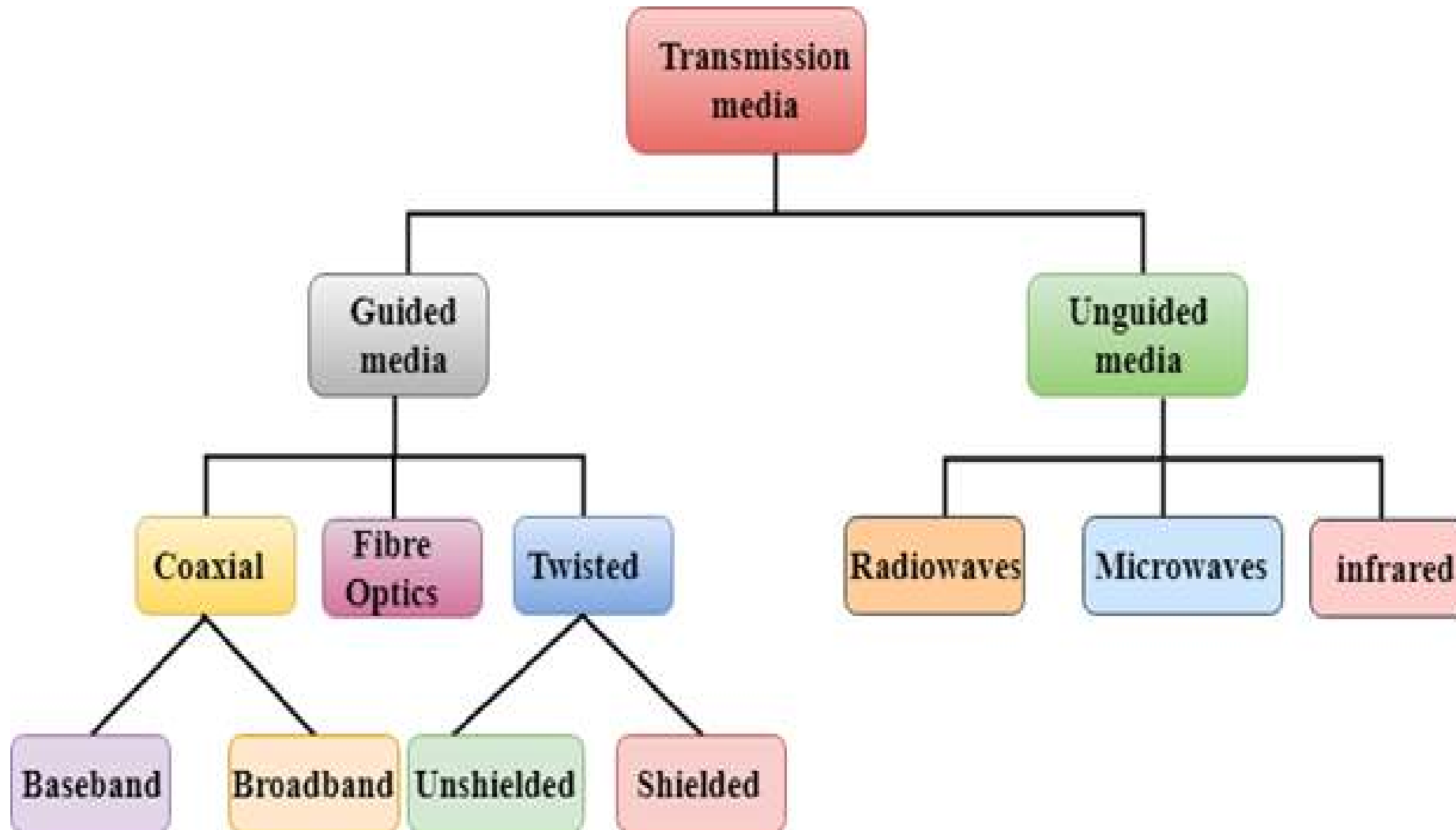
Advantages of Hybrid Topology

- ▶ **Adding a new node or deleting the existing node is easy** in hybrid topologies.
- ▶ **Hybrid topology is more secure, reliable, and scalable** as compared to individual star, ring and mesh topology.
- ▶ **Error detection and troubleshooting is easier** in hybrid topology.
- ▶ When an **organization has a large geographical area utilizing hybrid topology** is considered as better option.
- ▶ **Traffic with large volume is handled** easily by the hybrid topology.
- ▶ **The overall performance and speed is greater** in hybrid topology.

Disadvantages of Hybrid Topology

- ▶ The **design and implementation** of hybrid network topology is **difficult**.
- ▶ More number of **cables** and other **physical devices** are required for **hybrid topology**.
- ▶ The **process of installation of hybrid topology is difficult**.
- ▶ The **overall implementation, setup and process** of hybrid topology is much more costlier.

Classification of transmission media



1. Guided Media

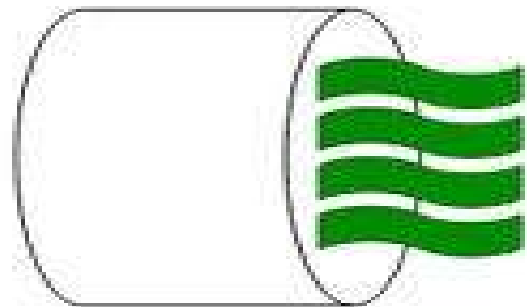
- ▶ **1. Guided Media** is also referred to as Wired or Bounded transmission media. Signals being transmitted are directed and confined in a narrow pathway by using physical links.

Features:

- ▶ High Speed
- ▶ Secure
- ▶ Used for comparatively shorter distances

▶ 1) Twisted Pair Cable

- ▶ 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.(less expensive,easy to install,high speed)**



Unshielded Twisted Pair



- ▶ **Advantages of Unshielded Twisted Pair**

- ▶ Least expensive

- ▶ Easy to install

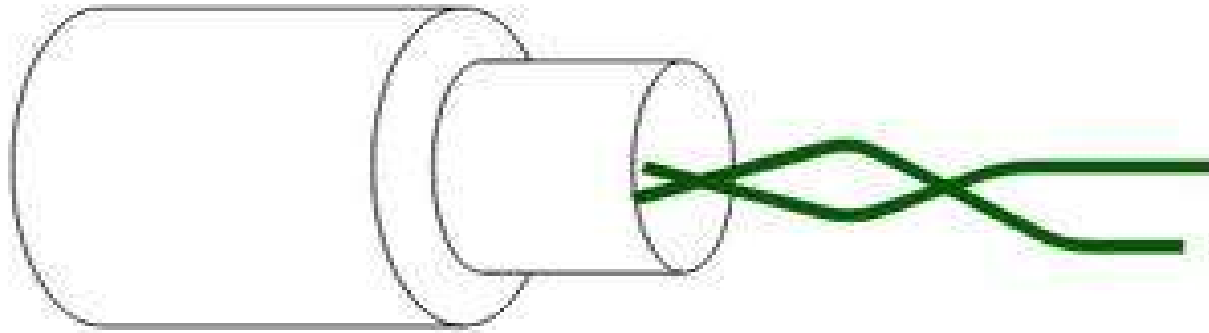
- ▶ High-speed capacity

- ▶ **Disadvantages of Unshielded Twisted Pair**

- ▶ Lower capacity and performance in comparison to STP

- ▶ Short distance transmission due to attenuation

2)Shielded twisted pair



Shielded Twisted Pair

- ▶ **Shielded Twisted Pair (STP):** This type of cable **consists of a special jacket to block external interference.** It is used in **fast-data-rate Ethernet** and in **voice and data channels of telephone lines.**
- ▶ **Advantages of Shielded Twisted Pair**
- ▶ **Better performance** at a higher data rate in comparison to UTP
- ▶ **Eliminates crosstalk**
- ▶ **Comparatively faster**
- ▶ **Disadvantages of Shielded Twisted Pair**
- ▶ Comparatively difficult to install and manufacture
- ▶ More expensive
- ▶ Bulky

2) 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.

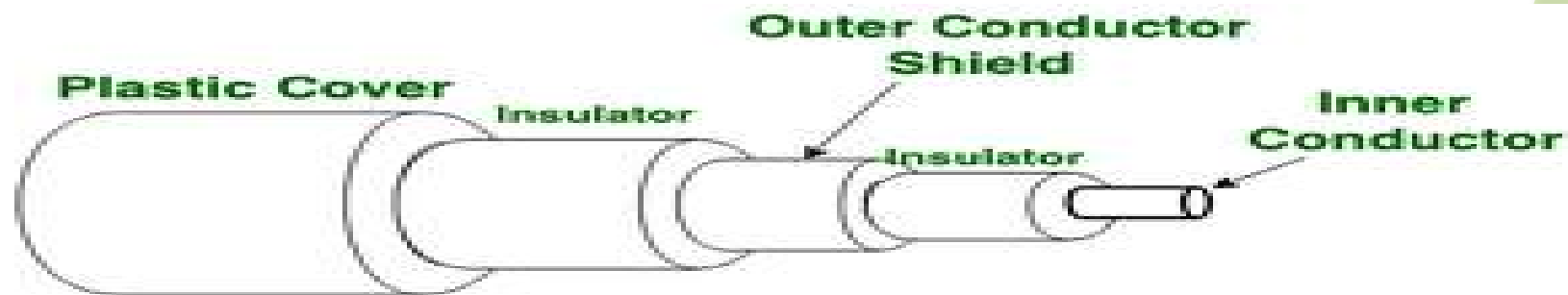


Figure of Coaxial Cable



▶ **Advantages of Coaxial Cable**

▶ Coaxial cables support high bandwidth.

▶ It is **easy to install** coaxial cables.

▶ **Less affected by noise or cross-talk** or electromagnetic interference.

▶ Coaxial cables support **multiple channels**

▶ **Disadvantages of Coaxial Cable**

▶ Coaxial cables are **expensive**.

▶ As a Coaxial cable has **multiple layers it is very bulky**.

▶ There is a chance of breaking the coaxial cable and attaching a “t-joint” by hackers, this compromises the security of the data.

Optical Fibre Cable

- ▶ 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. This supports two modes, namely unidirectional and bidirectional mode.

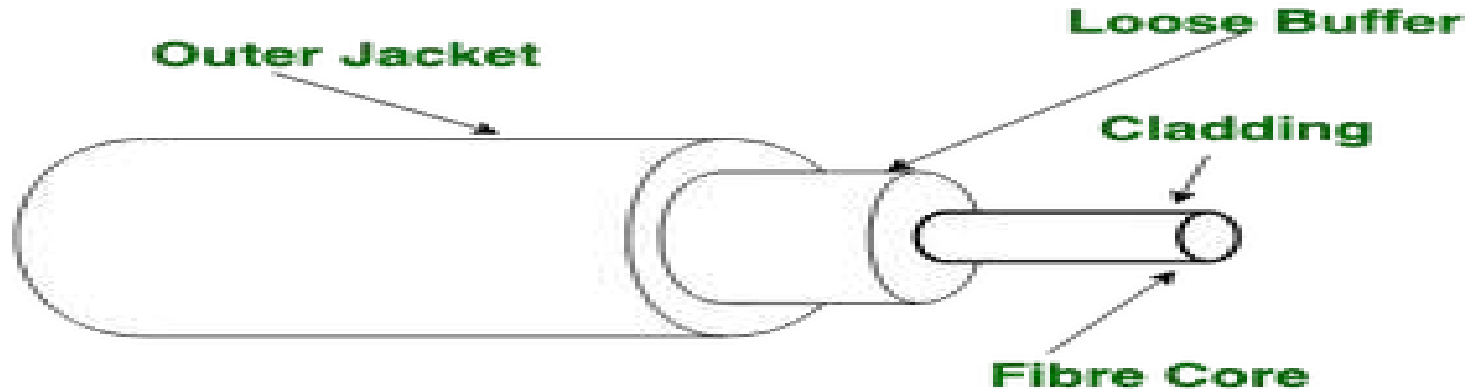


Figure of Optical Fibre Cable



▶ **Advantages of Optical Fibre Cable**

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

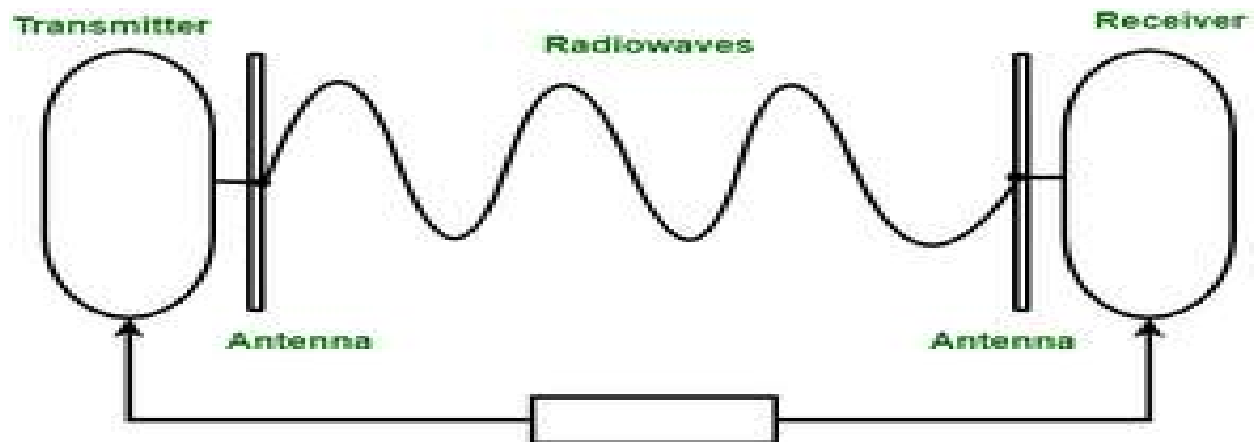
▶ **Disadvantages of Optical Fibre Cable**

- ▶ Difficult to install and maintain
- ▶ High cost
- ▶ Fragile

► **Unguided Media**

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

► Radio waves 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.



► **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. Micro waves are majorly used for **mobile phone communication and television distribution.**

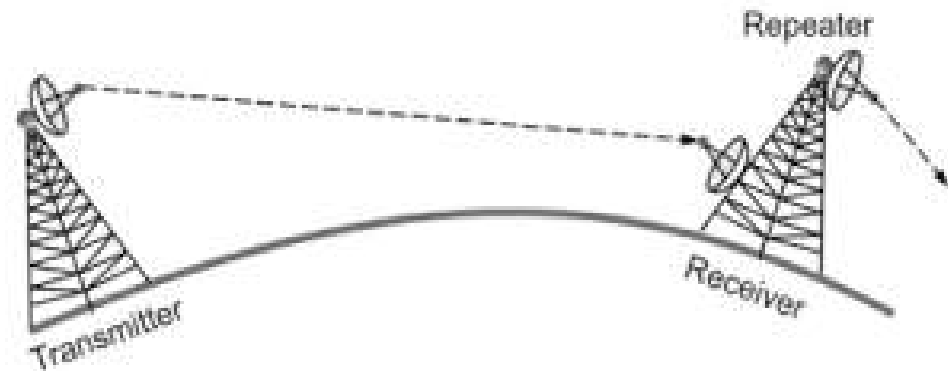


Fig: Microwave Transmission

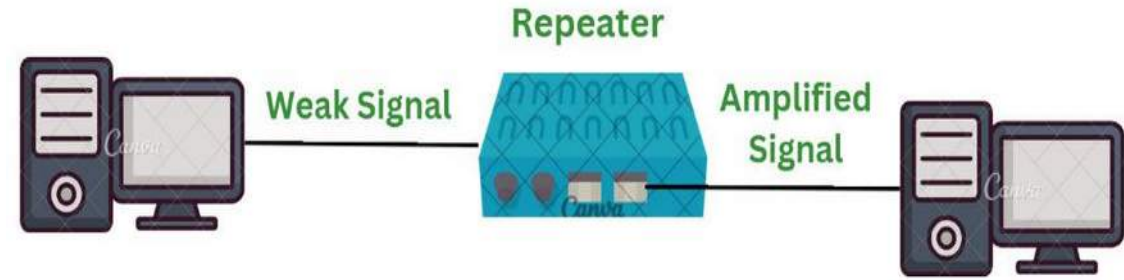
- ▶ **Infrared**
- ▶ **Infrared waves are used for very short distance communication.** They cannot penetrate through obstacles. This prevents interference between systems. Frequency Range:300GHz – 400THz. It is used in **TV remotes, wireless mouse, keyboard, printer, etc.**



Network Connecting devices

- ▶ **1) Repeater**
- ▶ **2) Bridge**
- ▶ **3) Router**
- ▶ **4) Gateway**
- ▶ **5) Hub**
- ▶ **6) Switch**

1. Repeater



A repeater operates at the physical layer.

- ▶ Its job is to amplify the signal over the same network before the signal becomes too weak or corrupted
- ▶ Repeater is a type of network node that amplifies incoming signals and rebroadcasts them over a wider area

2)Bridge

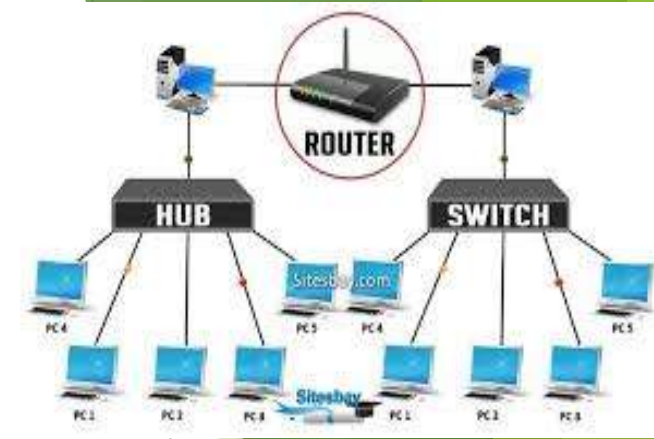
- ▶ A bridge in a computer network is a device used to connect multiple LANs together
- ▶ The bridge is a physical or hardware device but operates at the OSI model's data link layer and is also known as a layer of two switches.
- ▶ Here bridge is used to improve network performance.

Working of Bridges

- ▶ **Receiving Data:** The bridge gets data packets (or frames) from both network segments A and B.
- ▶ **Building a Table:** It creates a table of MAC addresses by looking at where the data is coming from to know which device is on which segment.
- ▶ **Filtering Data:** If the data from network A is meant for a device also on network A, the bridge stops it from going further.
- ▶ **Forwarding Data:** If the data from network A is meant for a device on network B, the bridge sends it to the correct place on network B.
- ▶ **Repeating for Both Sides:** The bridge does the same thing for data coming from network B.

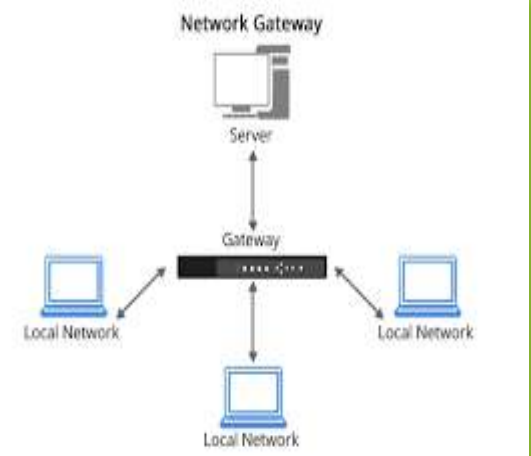
3. Routers

- ▶ A router is a device like a switch that routes data packets based on their IP addresses.
- ▶ The router is mainly a Network Layer device. Routers normally connect LANs and WANs and have a dynamically updating routing table
- ▶ based on which they make decisions on routing the data packets. The router divides the broadcast domains of hosts connected through it.



4) Gateway

- ▶ A gateway, as the name suggests, is a passage to connect two networks
- ▶ that may work upon different networking models.
- ▶ They work as messenger agents that take data from one system, interpret it, and transfer it to another system. Gateways are also called protocol converters and can operate at any network layer.
- ▶ Gateways are generally more complex than switches or routers. A gateway is also called a protocol converter.



5)Hub



- ▶ **Hub** – A hub is a basically multi-port repeater. A hub connects multiple wires coming from different branches, for example, the connector in star topology which connects different stations. Hubs cannot filter data, so data packets are sent to all connected devices.
- ▶ **Types of Hub**
- ▶ **Active Hub:-** These are the hubs that have their power supply and can clean, boost, and relay the signal along with the network.
- ▶ **Passive Hub:-** These are the hubs that collect wiring from nodes and power supply from the active hub. These hubs relay signals onto the network without cleaning and boosting them
- ▶ **Intelligent Hub:-** It works like an active hub and includes remote management capabilities. They also provide flexible data rates to network devices. It also enables an administrator to monitor the traffic passing through the hub and to configure each port in the hub.

6)Switch

- ▶ A switch is a multiport bridge with a buffer and a design that can boost its efficiency and performance.
- ▶ A switch is a data link layer device.
- ▶ The switch can perform error checking before forwarding data, which makes it very efficient as it does not forward packets that have errors and forward good packets selectively to the correct port only.
- ▶ In other words, the switch divides the collision domain of hosts, but the broadcast domain remains the same.

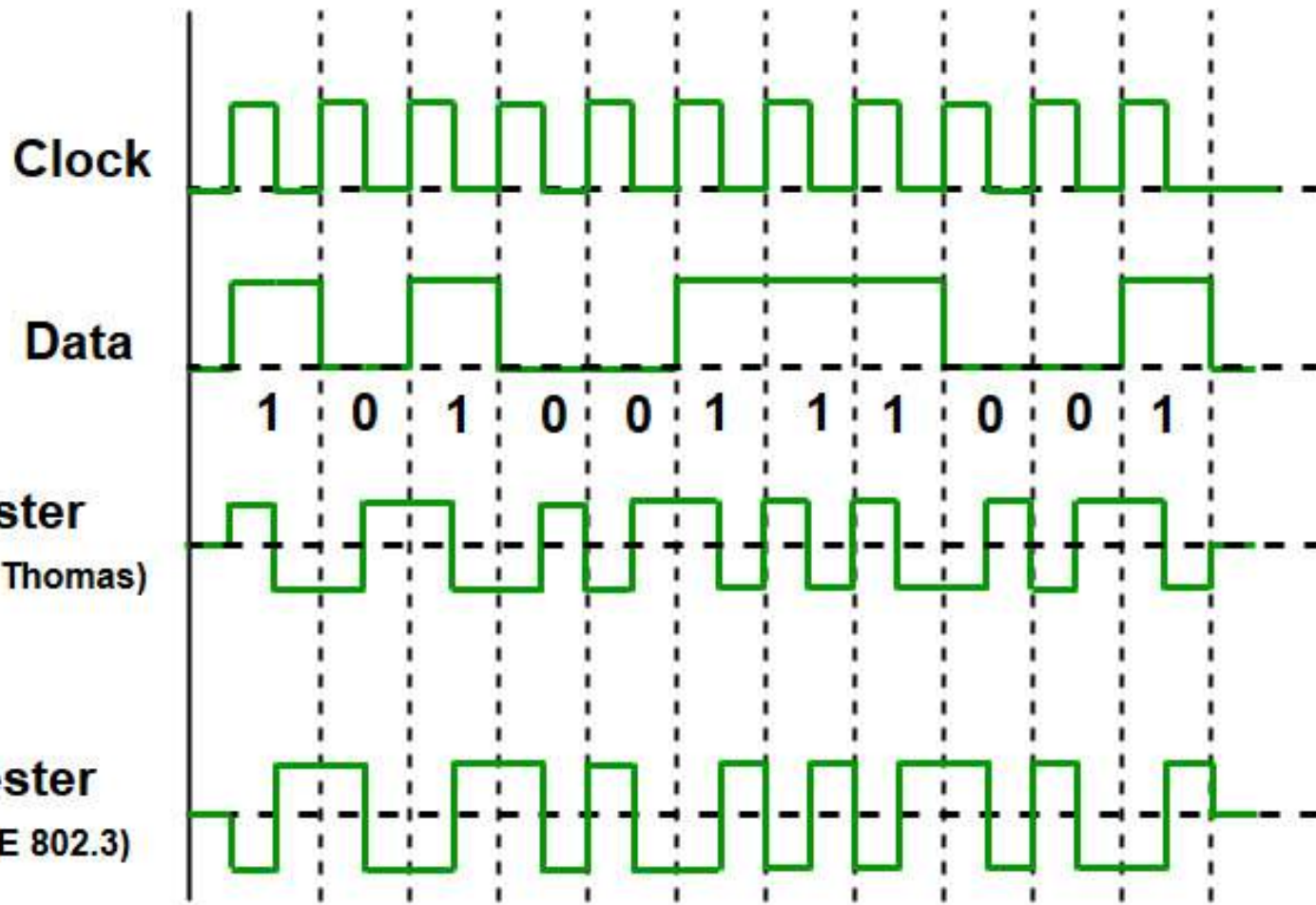
Line Coding

- ▶ **Line coding** is the process of converting digital data to digital signals



1) Manchester Encoding

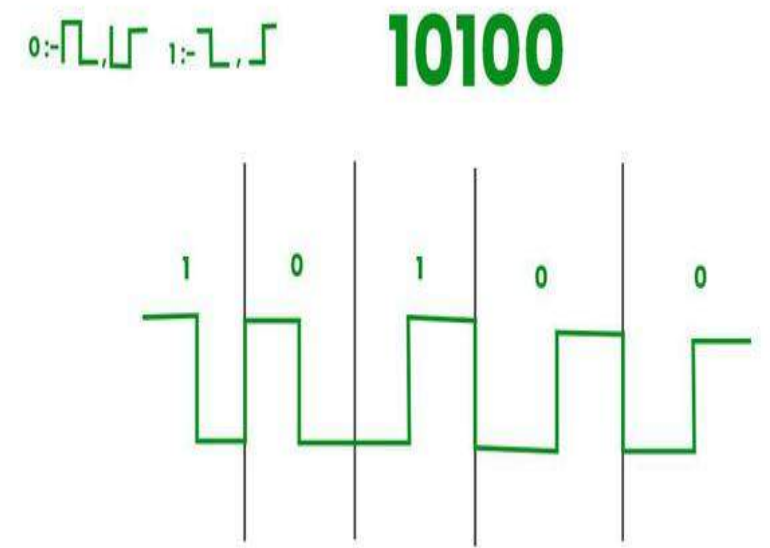
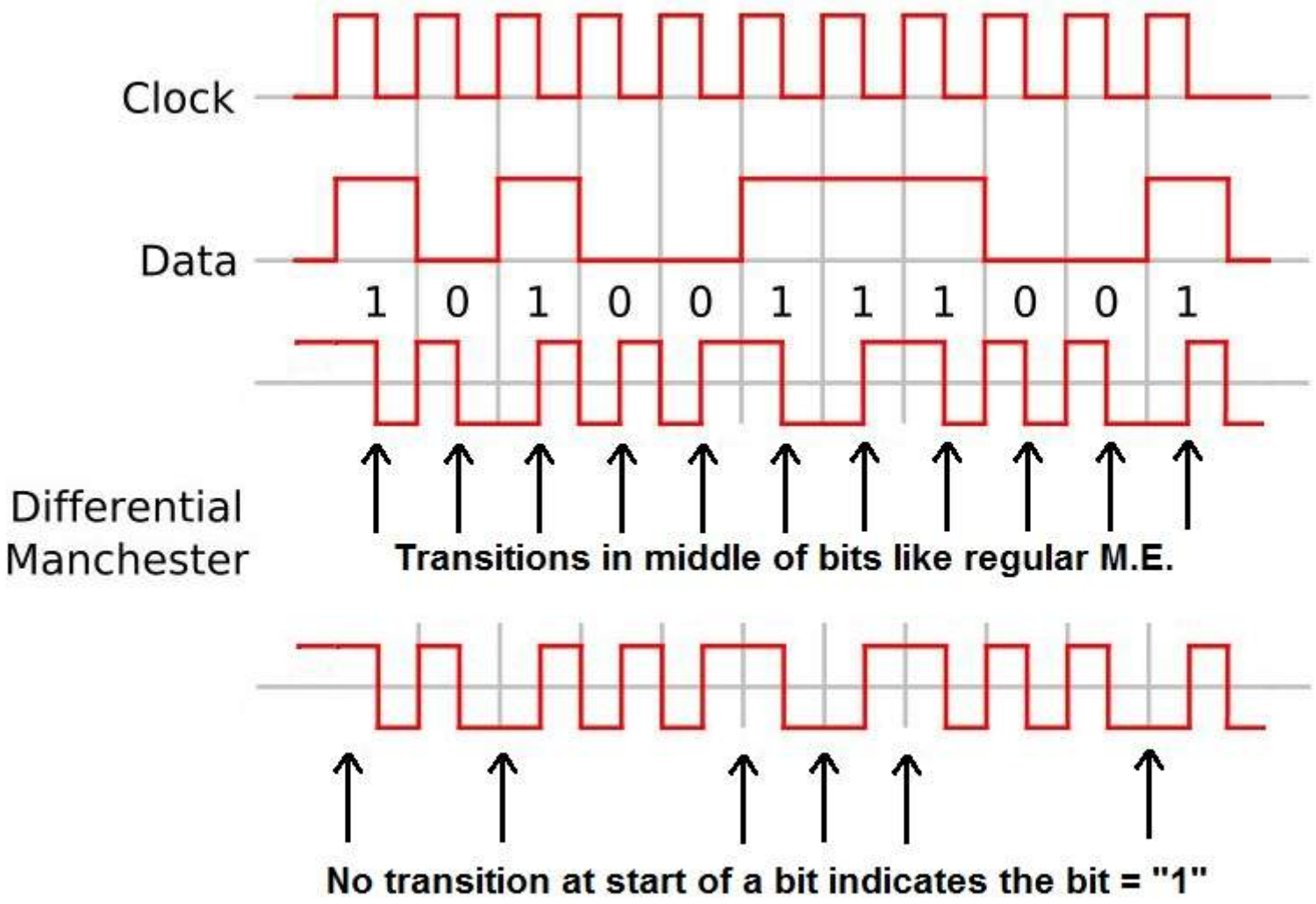
- ▶ Manchester encoding is a method of data transmission used in computer networks and telecommunications.
- ▶ It works by combining the clock and data signals into one stream, making it easier to synchronize the data.
- ▶ Each bit of data is represented by a transition; a change from high to low or low to high in the signal.
- ▶ This helps ensure that the data is correctly interpreted by the receiving device.
- ▶ Manchester encoding is widely used in Ethernet technology and other digital communication systems due to its reliability and simplicity.
- ▶ In Manchester, the duration of a bit is divided into two halves. The voltage remains the same at one level during the first half & moves to the other level.



Manchester
(as per G.E Thomas)

Manchester
(as per IEEE 802.3)

Differential Manchester Encoding



Frequency Hopping Spread Spectrum(FHSS)

► (FHSS) is a state-of-the-art method for transmitting radio signals where carriers rapidly switch among many different frequency channels.

► **Why it is use?**

1)Interference

2)Spying

-**You know the hopping sequence**

(F2,F5,F3,F6,F1,F6,F4)

-**Slow frequency hopping:**Each frequency hop
Several symbols.

-**Fast frequency hopping:**Each symbol transmit several frequency hop.

