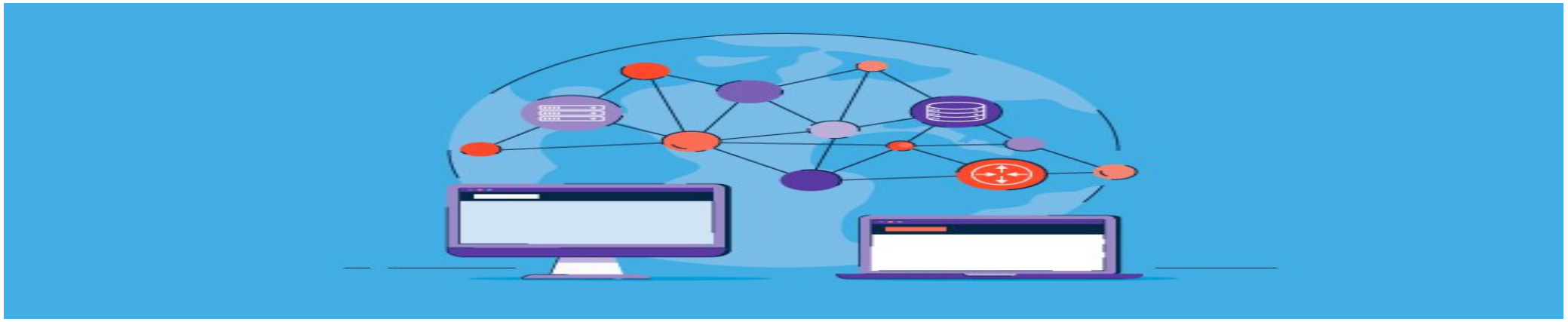


COMPUTER NETWORKS

Introduction

Syllabus

UNIT-I (8 Lectures)

DATA COMMUNICATION : Characteristics, Components, Data flow, Network criteria, Topologies, Network model, Layered tasks, ARPANET, OSI model, TCP/IP protocol suite, Addressing (Text Book 2).

PHYSICAL LAYER: Transmission Media: Guided and unguided, Connecting devices: Hub, switch, bridge, router, Gateway. (Text Book-2).

Learning Outcomes: At the end of the unit the student will be able to

state the characteristics of network components and data flow.(L1)

discuss the network models and protocol stack.(L2)

differentiate transmission media and addressing mechanisms.(L2)

UNIT-II (12 Lectures)

DATA LINK LAYER: Design issues, Error detection and correction, Elementary data link protocols, Sliding window protocols. (Text Book-1).

RANDOM ACCESS: ALOHA, CSMA/CD, CSMA/CA, Controlled access, Channelization, Wired LAN: IEEE Standards, Standard Ethernet, Wireless LAN:IEEE802.11, ATM: architecture,layers (Text Book-2).

Learning Outcomes: At the end of the unit the student will be able to

1. classify error detection and correction techniques. (L2)
2. explain random access and controlled access protocols. (L2)
3. contrast various ATM layers.(L2)

SYLLABUS

UNIT-III (12 Lectures)

NETWORK LAYER: Design issues, Routing algorithms, Internetworking, Network layer in the Internet. (Text Book-1).

CONGESTION CONTROL: Approaches to Congestion Control, Traffic-Aware Routing, Traffic Throttling, Load shedding, traffic shaping. (Text Book-1).

Learning Outcomes: At the end of the unit the student will be able to:

1. describe the design issues and routing algorithms in the network layer. (L2)
2. explain the internet control protocols. (L2)
3. discuss the various congestion control mechanisms (L2)

UNIT-IV (8 Lectures)

TRANSPORT LAYER: Transport services, Elements of transport Protocols, TCP and UDP (Text Book-1).

DELAY-TOLERANT NETWORKING:DTN Architecture, The Bundle Protocol (Text Book-1).

Learning Outcomes: At the end of the unit the student will be able to

1. summarize various transport services available in the transport layer.(L2)
2. differentiateTCP and UDP protocols.(L2)
3. discuss DTN architecture.(L2)

SYLLABUS

UNIT-V (10 Lectures)

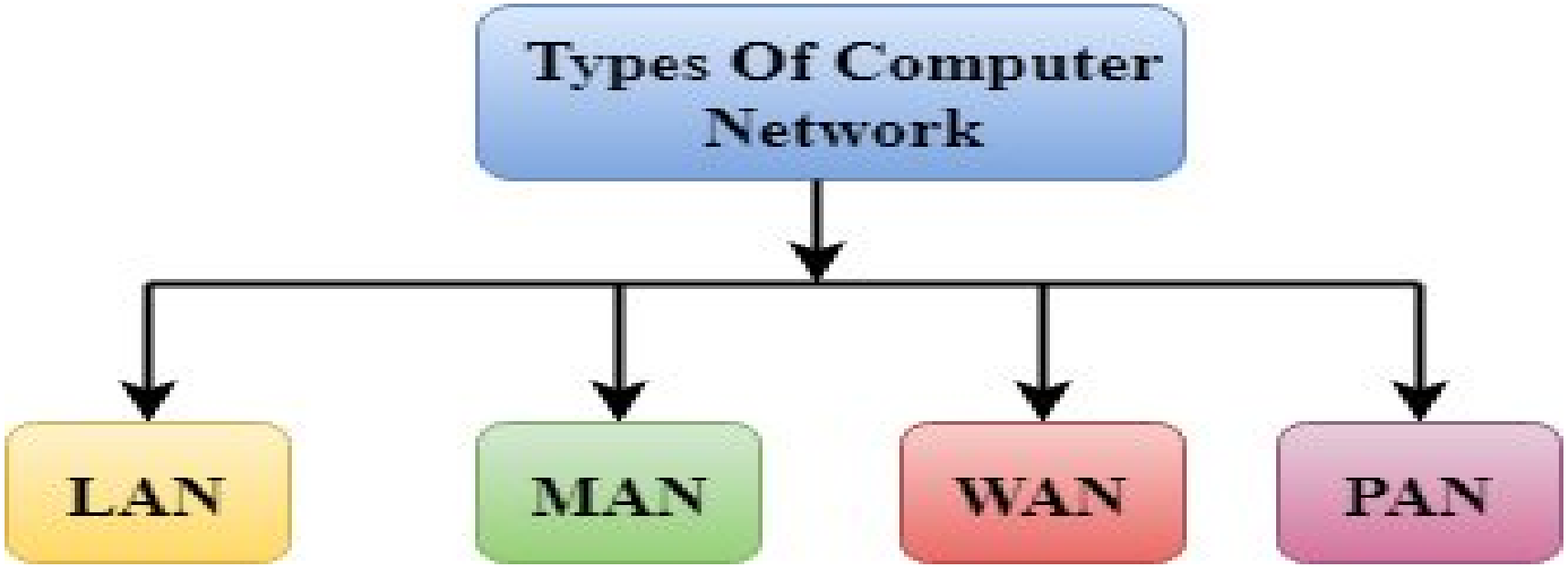
- **APPLICATION LAYER:**Domain Name Space (DNS), SNMP, Electronic mail: MIME, SMTP, IMAP.
- **CONTENT DELIVERY:** Content Delivery Networks, Peer-to-Peer Networks.
- **Learning Outcomes:** At the end of the unit the student will be able to
  1. describe the concepts of DNS. (L2)
  2. explain about electronic mail protocols.(L2)
  3. discuss the content delivery networks.(L2)

Computer Network

- A Computer Network is a connection of two or more Computers through a medium for exchanging information or data communication.
- It is also called as Data Network where you can easily send and receive data to or from a Computing device.

Computer Network Types

- A computer network is a group of computers linked to each other that enables the computer to communicate with another computer and share their resources, data, and applications.



LAN(Local Area Network

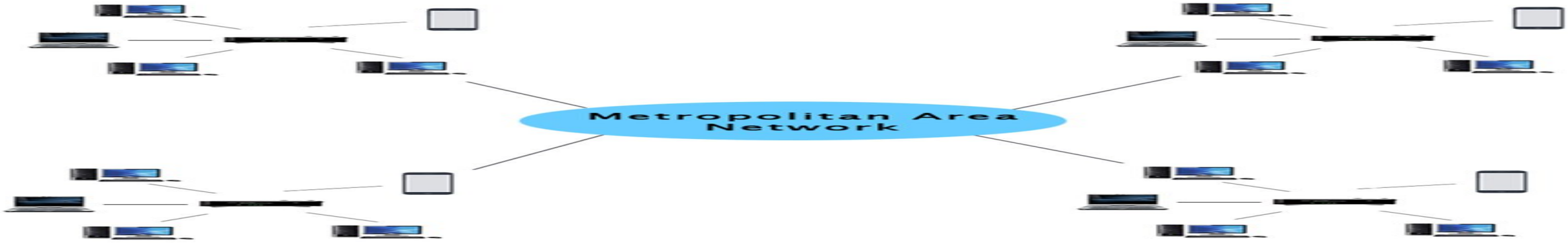
- Local Area Network is a group of computers connected to each other in a small area such as building, office.
- LAN is used for connecting two or more personal computers through a communication medium such as twisted pair, coaxial cable, etc.
- It is less costly as it is built with inexpensive hardware 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.

PAN(Personal Area Network)

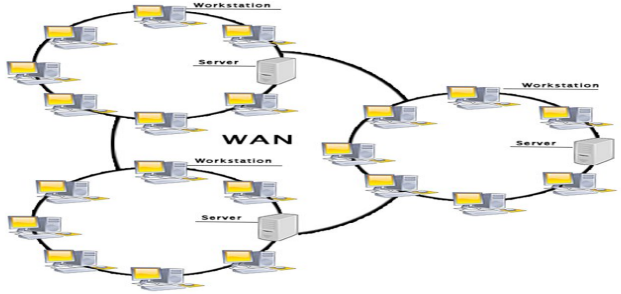
- Personal Area Network is a network arranged within an individual person, typically within a range of 10 meters.
- Personal Area Network is used for connecting the computer devices of personal use is known as Personal Area Network.
- **Thomas Zimmerman** was the first research scientist to bring the idea of the Personal Area Network.
- Personal Area Network covers an area of **30 feet**.
- Personal computer devices that are used to develop the personal area network are the laptop, mobile phones, media player and play stations.

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.



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.

Characteristics of a Computer Network

Computer Network is a linkage of several computers to share an operating framework, hardware, and data through a transmission approach between them.

Elements of a Computer Network

A computer network involves the following elements such as follows

Nodes (Workstations) − The nodes are known as the multiple terminals connected to the network sharing the network resources.

Server − It can assign a specific node as a central node at a well-known and permanent address to support the network. The node supporting the service is called server.

Network Interface Unit − The interpreter which facilitates connecting the server and multiple nodes, is known as the Network Interface Unit. The network interface unit is connected to the server and all departments to maintain the connection.

Features of Computer Network

The main features of computer networks are as follows −

Resource Sharing

- The main feature of the computer network is Resource Sharing. It can generate all the programs, information, and hardware available to anyone on the network without treating the resource's physical area and the user.

Saving Money

- The second feature of a computer network is saving money. Small computers have a better value proportion than larger ones. Mainframes are approximately a method ten times faster than the fastest individual-chip microprocessors, but they cost multiple times more.
- This imbalance has made numerous system designers build systems, including dynamic personal computers, one per customer, with data kept on at least one shared document server machine.

Features of Computer Network

High Reliability

- The third feature is to support high reliability by acquiring a different authority of supply. For example, all files can be recreated on a few machines, and thus if one of them is nonexistent, additional copies could be available

Improve Performance

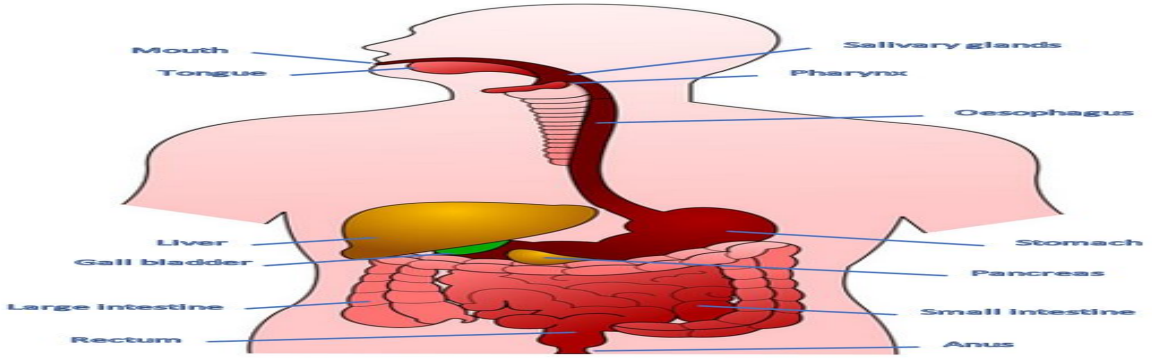
- The fourth feature of a computer network is to improve accessibility and the performance of the system. A system's performance can be improved by adding one or more processors into it as its workload increases.

Features of Computer Network

Communication Medium

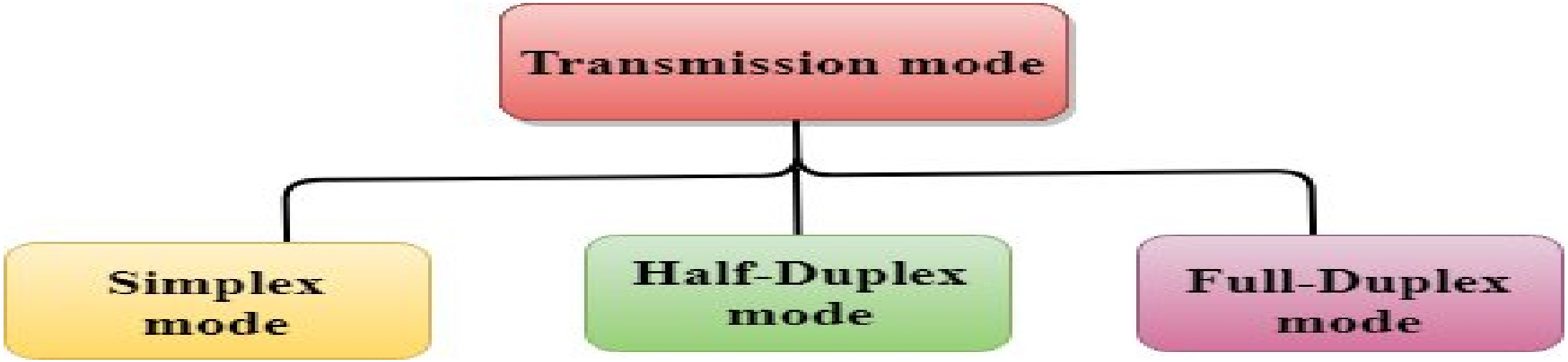
- The fifth feature of the computer network offers a powerful communication medium. The different users on the network can immediately identify a document that has been refreshed on a network.

DATA FLOW

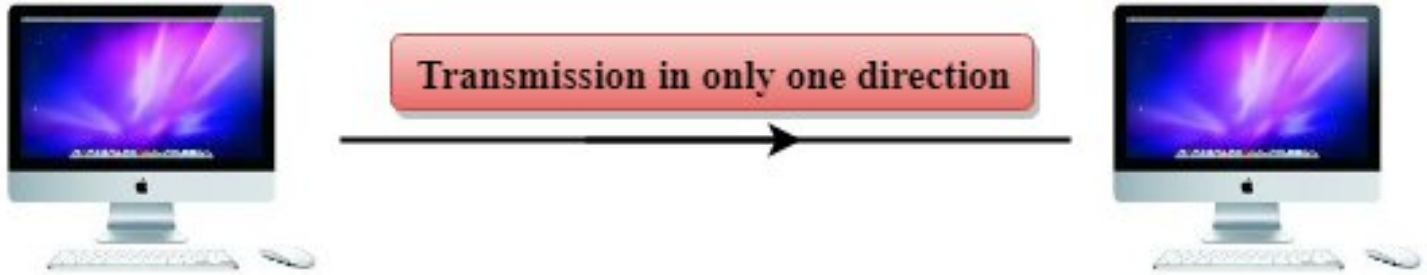


Transmission modes

- The way in which data is transmitted from one device to another device is known as **transmission mode**.
- The transmission mode is also known as the communication mode.
- Each communication channel has a direction associated with it, and transmission media provide the direction. Therefore, the transmission mode is also known as a directional mode.
- The transmission mode is defined in the physical layer.

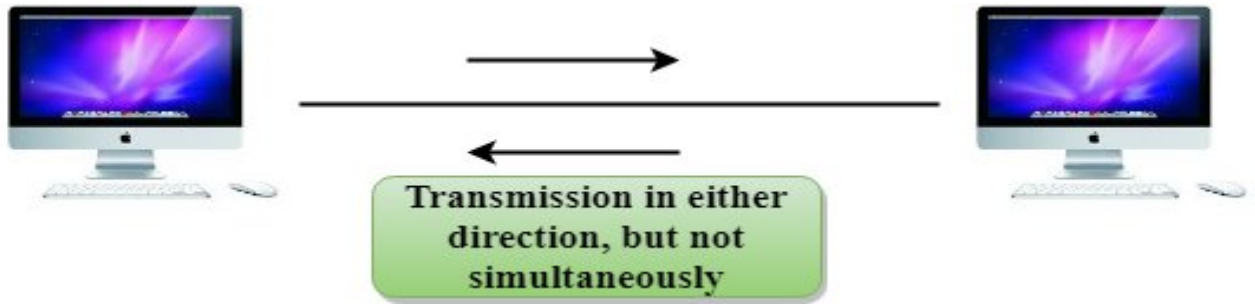


Simplex mode



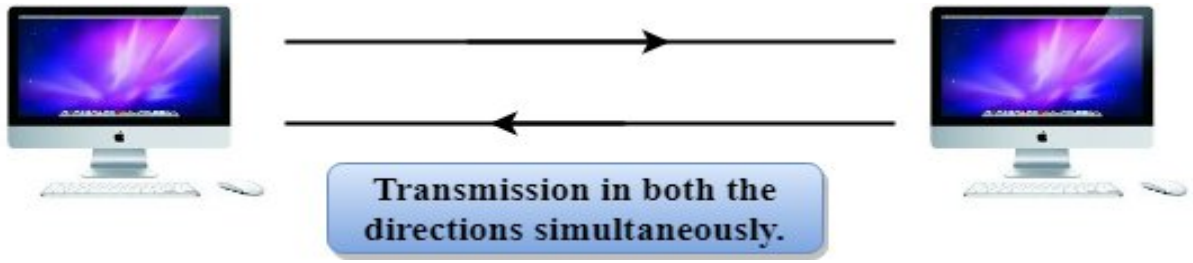
- In Simplex mode, the communication is unidirectional, i.e., the data flow in one direction.
- A device can only send the data but cannot receive it or it can receive the data but cannot send the data.
- This transmission mode is not very popular as mainly communications require the two-way exchange of data. The simplex mode is used in the business field as in sales that do not require any corresponding reply.
- The radio station is a simplex channel as it transmits the signal to the listeners but never allows them to transmit back.
- The main advantage of the simplex mode is that the full capacity of the communication channel can be utilized during transmission.

Half-Duplex mode



- In a Half-duplex channel, direction can be reversed, i.e., the station can transmit and receive the data as well.
- Messages flow in both the directions, but not at the same time.
- The entire bandwidth of the communication channel is utilized in one direction at a time.
- In half-duplex mode, it is possible to perform the error detection, and if any error occurs, then the receiver requests the sender to retransmit the data.
- A **Walkie-talkie** is an example of the Half-duplex mode. In Walkie-talkie, one party speaks, and another party listens. After a pause, the other speaks and first party listens. Speaking simultaneously will create the distorted sound which cannot be understood.

Full-duplex mode



- In Full duplex mode, the communication is bi-directional, i.e., the data flow in both the directions.
- Both the stations can send and receive the message simultaneously.
- Full-duplex mode has two simplex channels. One channel has traffic moving in one direction, and another channel has traffic flowing in the opposite direction.
- The Full-duplex mode is the fastest mode of communication between devices.
- The most common example of the full-duplex mode is a telephone network. When two people are communicating with each other by a telephone line, both can talk and listen at the same time.

Brainstormin g

Clues:

1.I can only receive information — I never respond. 📺

2.I take turns speaking. When I talk, you listen, and vice versa. 🎤

3.We talk at the same time without interrupting each other. 📞

4.I am a school announcement system.

5.I am used by police officers and security guards to coordinate.

6.I am like a normal chat over the phone.

Clue #	Answer (Simplex / Half-Duplex / Full-Duplex)
1	
2	
3	
4	
5	
6	

Network Criteria

The criteria that have to be met by a computer network are:

1.Performance – It is measured in terms of transit time and response time. Transit time is the time for a message to travel from one device to another .Response time is the elapsed time between an inquiry and a response.

Performance is dependent on the following factors:

- The number of users
- Type of transmission medium
- Capability of connected network
- Efficiency of software

Network Criteria

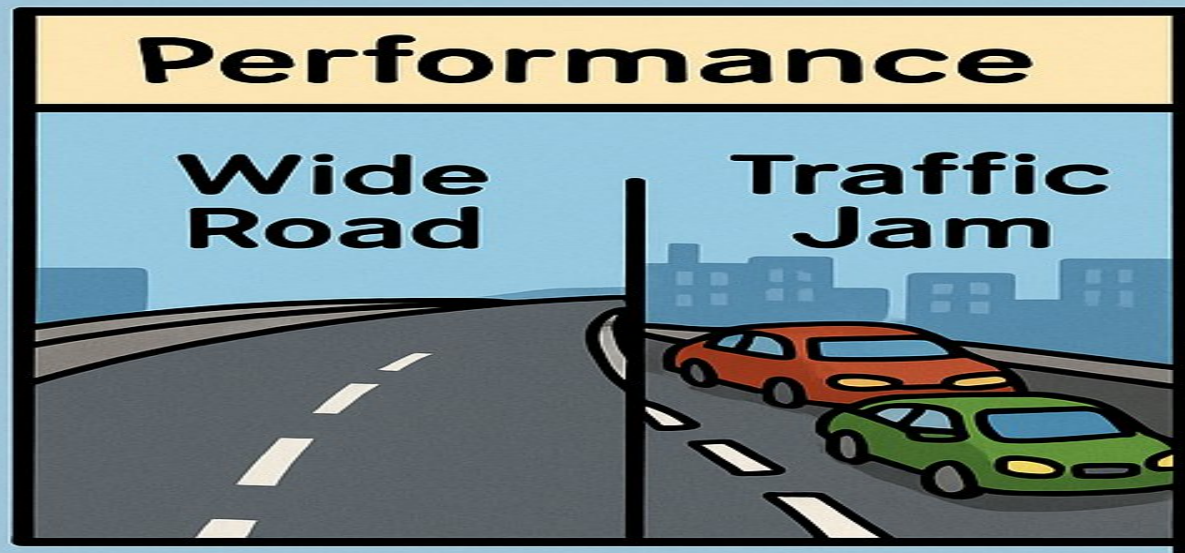
2. Reliability – It is measured in terms of

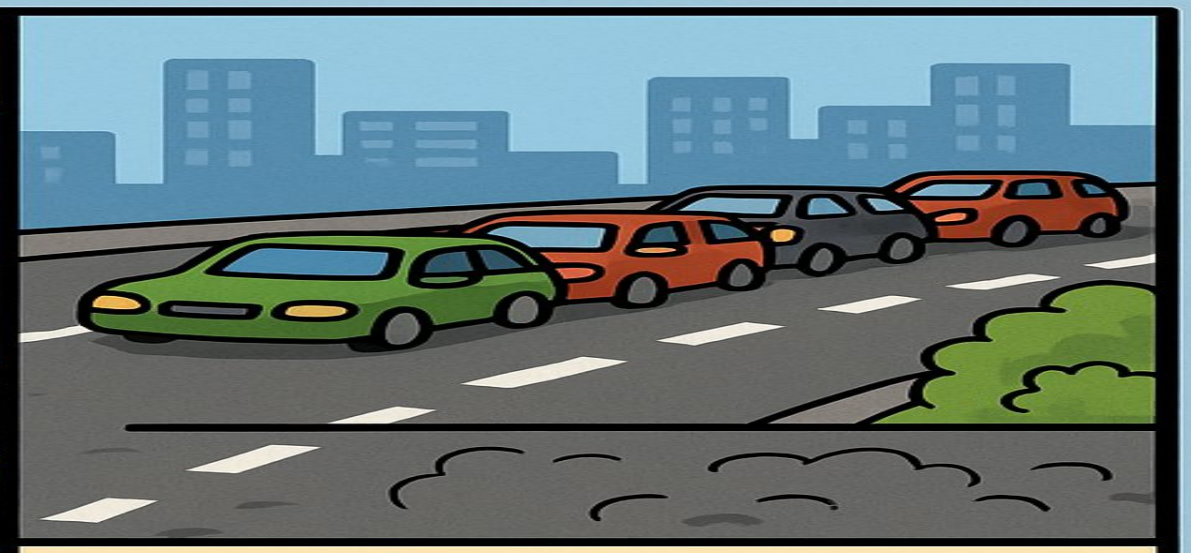
- Frequency of failure
- Recovery from failures
- Robustness during catastrophe

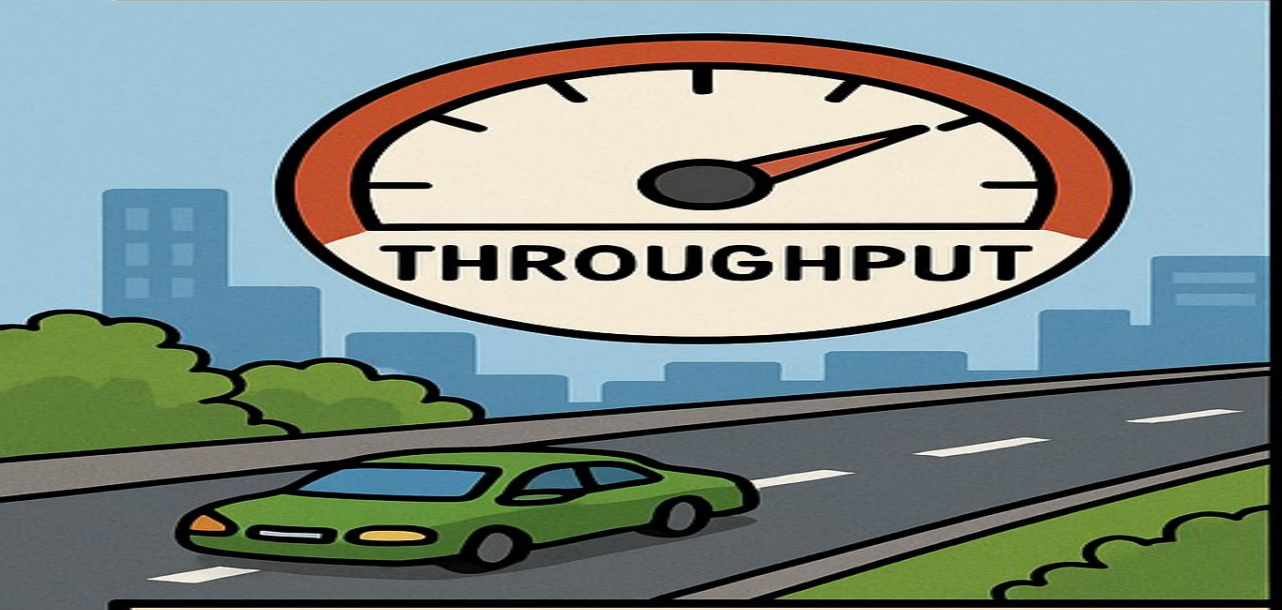
3. Security – It means protecting data from unauthorized access.

NETWORK CRITERIA

Performance

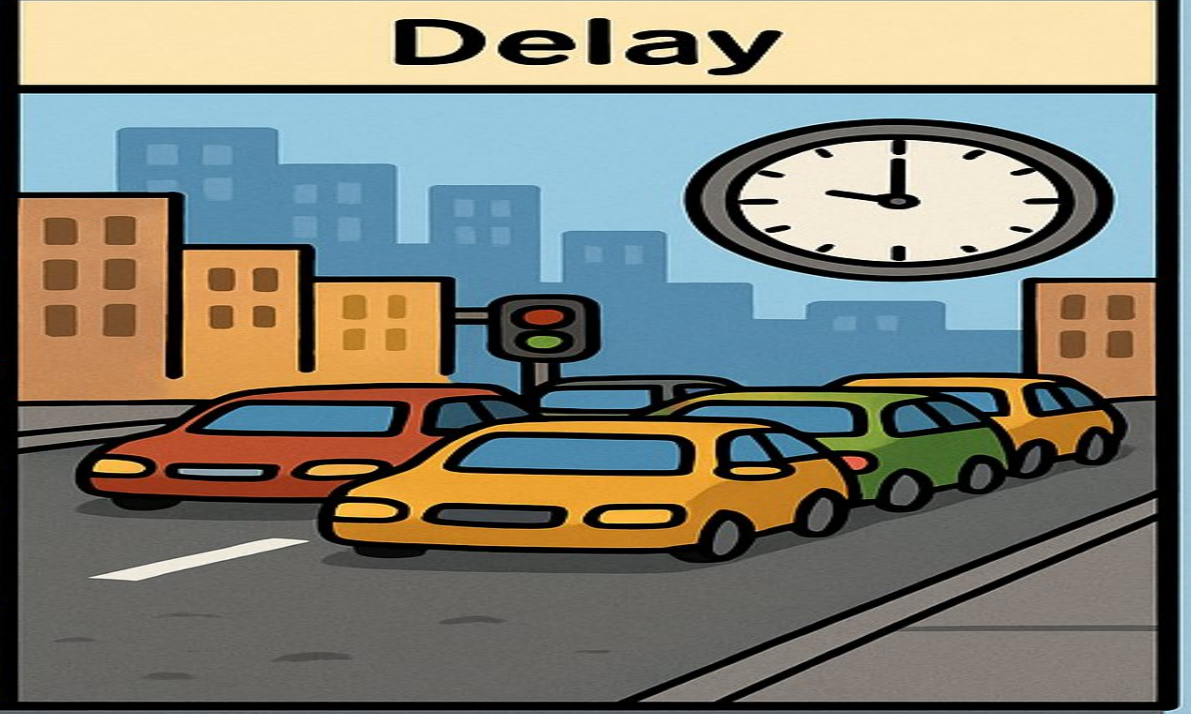






Tnroughput

Delay



Goals of Computer Networks

- The following are some important goals of computer networks:

1. **Resource Sharing –**
   Many organization has a substantial number of computers in operations, which are located apart. Ex. A group of office workers can share a common printer, fax, modem, scanner, etc.

2. **High Reliability –**
   If there are alternate sources of supply, all files could be replicated on two or more machines. If one of them is not available, due to hardware failure, the other copies could be used.

Goals of Computer Networks

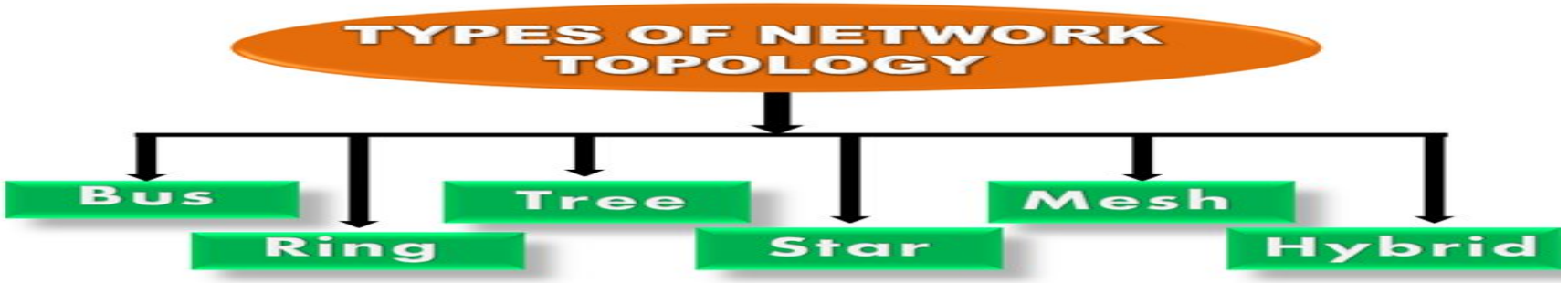
3.Inter-process Communication –

Network users, located geographically apart, may converse in an interactive session through the network. In order to permit this, the network must provide almost error-free communications.

4.Flexible access –

Files can be accessed from any computer in the network. The project can be begun on one computer and finished on another.

Topologies



Topology defines the structure of the network of how all the components are interconnected to each other. There are two types of topology: physical and logical topology.

Types of Network Topology

Physical topology is the geometric representation of all the nodes in a network. There are six types of network topology which are Bus Topology, Ring Topology, Tree Topology, Star Topology, Mesh Topology, and Hybrid Topology.

Bus Topology

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

Advantages of Bus topology

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

Disadvantages of Bus topology

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

Ring Topology

- Ring topology is like a bus topology, but with connected ends.
- The node that receives the message from the previous computer will retransmit to the next node.
- The data flows in one direction, i.e., it is unidirectional.
- The data flows in a single loop continuously known as an endless loop.
- It has no terminated ends, i.e., each node is connected to other node and having no termination point.
- The data in a ring topology flow in a clockwise direction.
- The most common access method of the ring topology is **token passing**.
  - **Token passing:** It is a network access method in which token is passed from one node to another node.
  - **Token:** It is a frame that circulates around the network.

Working of Token passing

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

Advantages of Ring topology

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

Disadvantages of Ring topology

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

Star Topology

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

Advantages of Star topology

- **Efficient troubleshooting:** Troubleshooting is quite efficient in a star topology as compared to bus topology. In a bus topology, the manager has to inspect the kilometers of cable. In a star topology, all the stations are connected to the centralized network. Therefore, the network administrator has to go to the single station to troubleshoot the problem.
- **Network control:** Complex network control features can be easily implemented in the star topology. Any changes made in the star topology are automatically accommodated.
- **Limited failure:** As each station is connected to the central hub with its own cable, therefore failure in one cable will not affect the entire network.
- **Familiar technology:** Star topology is a familiar technology as its tools are cost-effective.
- **Easily expandable:** It is easily expandable as new stations can be added to the open ports on the hub.
- **Cost effective:** Star topology networks are cost-effective as it uses inexpensive coaxial cable.
- **High data speeds:** It supports a bandwidth of approx 100Mbps. Ethernet 100BaseT is one of the most popular Star topology networks.

Disadvantages of Star topology

- **A Central point of failure:** If the central hub or switch goes down, then all the connected nodes will not be able to communicate with each other.

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

Mesh topology

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

Mesh topology is divided into two categories:

- Fully connected mesh topology
- Partially connected mesh topology

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

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

Advantages of Mesh topology

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

Disadvantages of Mesh topology

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

Tree topology

- Tree topology combines the characteristics of bus topology and star topology.
- A tree topology is a type of structure in which all the computers are connected with each other in hierarchical fashion.
- The top-most node in tree topology is known as a root node, and all other nodes are the descendants of the root node.
- There is only one path exists between two nodes for the data transmission. Thus, it forms a parent-child hierarchy.

Advantages of Tree topology

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

Disadvantages of Tree topology

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

Hybrid Topology

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

Advantages of Hybrid Topology

- **Reliable:** If a fault occurs in any part of the network will not affect the functioning of the rest of the network.
- **Scalable:** Size of the network can be easily expanded by adding new devices without affecting the functionality of the existing network.
- **Flexible:** This topology is very flexible as it can be designed according to the requirements of the organization.
- **Effective:** Hybrid topology is very effective as it can be designed in such a way that the strength of the network is maximized and weakness of the network is minimized.

Disadvantages of Hybrid topology

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

Brainstorming

Connect the following images to form a computer network?



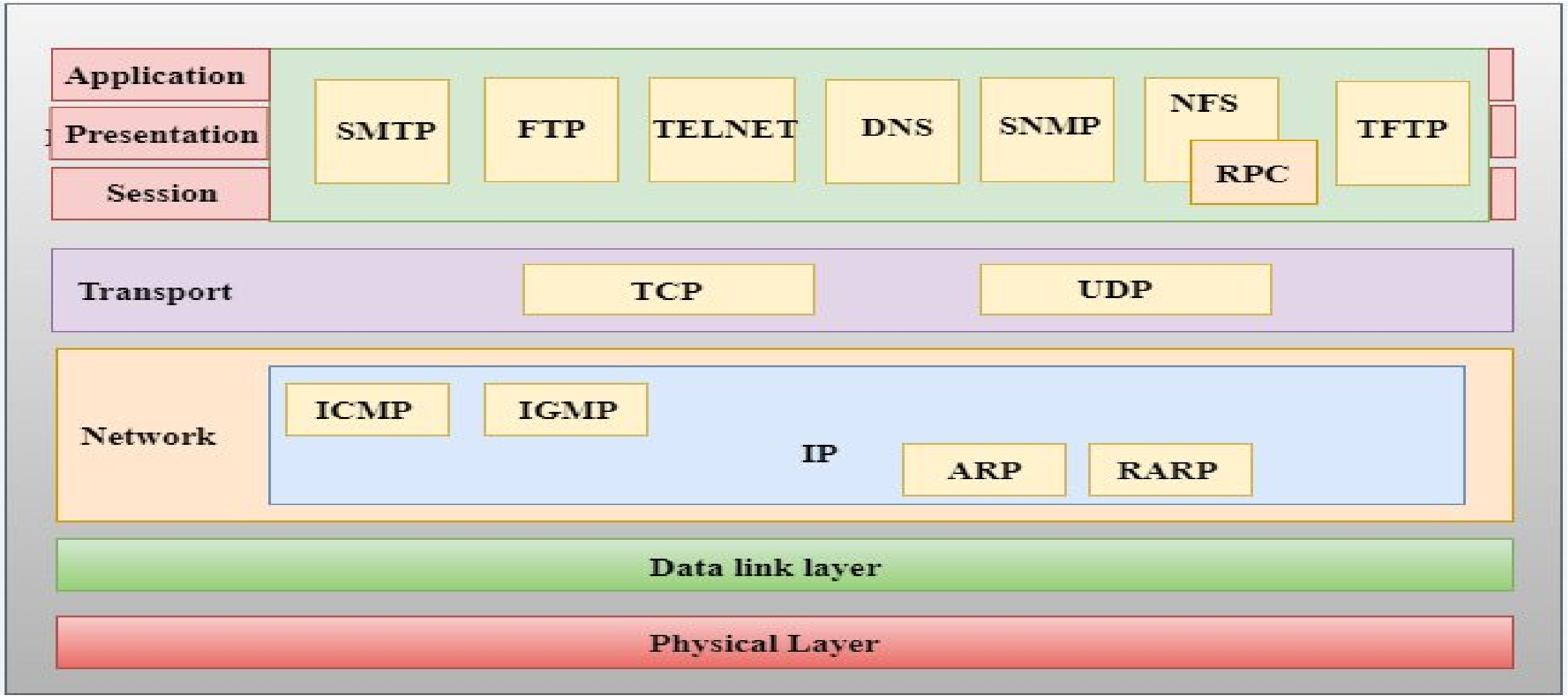





TCP/IP model

- The TCP/IP model was developed prior to the OSI model.
- The TCP/IP model is not exactly similar to the OSI model.
- The TCP/IP model consists of five layers: the application layer, transport layer, network layer, data link layer and physical layer.
- The first four layers provide physical standards, network interface, internetworking, and transport functions that correspond to the first four layers of the OSI model and these four layers are represented in TCP/IP model by a single layer called the application layer.

Functions of TCP/IP layers



Network Access Layer

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

Internet Layer

- An internet layer is the second layer of the TCP/IP model.
- An internet layer is also known as the network layer.
- The main responsibility of the internet layer is to send the packets from any network, and they arrive at the destination irrespective of the route they take.

Following are the protocols used in this layer are

- **IP Protocol:** IP protocol is used in this layer, and it is the most significant part of the entire TCP/IP suite.
- Following are the responsibilities of this protocol
- **IP Addressing:** This protocol implements logical host addresses known as IP addresses. The IP addresses are used by the internet and higher layers to identify the device and to provide internetwork routing.
- **Host-to-host communication:** It determines the path through which the data is to be transmitted.

Following are the protocols used in this layer are

- **Data Encapsulation and Formatting:** An IP protocol accepts the data from the transport layer protocol. An IP protocol ensures that the data is sent and received securely, it encapsulates the data into message known as IP datagram.
- **Fragmentation and Reassembly:** The limit imposed on the size of the IP datagram by data link layer protocol is known as Maximum Transmission unit (MTU). If the size of IP datagram is greater than the MTU unit, then the IP protocol splits the datagram into smaller units so that they can travel over the local network. Fragmentation can be done by the sender or intermediate router. At the receiver side, all the fragments are reassembled to form an original message.

Following are the protocols used in this layer are

- **Routing:** When IP datagram is sent over the same local network such as LAN, MAN, WAN, it is known as direct delivery. When source and destination are on the distant network, then the IP datagram is sent indirectly. This can be accomplished by routing the IP datagram through various devices such as routers.

ARP Protocol

- ARP stands for **Address Resolution Protocol**.
- ARP is a network layer protocol which is used to find the physical address from the IP address.
- **The two terms are mainly associated with the ARP Protocol:**
  - **ARP request:** When a sender wants to know the physical address of the device, it broadcasts the ARP request to the network.
  - **ARP reply:** Every device attached to the network will accept the ARP request and process the request, but only recipient recognize the IP address and sends back its physical address in the form of ARP reply. The recipient adds the physical address both to its cache memory and to the datagram header

ICMP Protocol

- **ICMP** stands for Internet Control Message Protocol.
- It is a mechanism used by the hosts or routers to send notifications regarding datagram problems back to the sender.
- A datagram travels from router-to-router until it reaches its destination. If a router is unable to route the data because of some unusual conditions such as disabled links, a device is on fire or network congestion, then the ICMP protocol is used to inform the sender that the datagram is undeliverable.

ICMP Protocol

- An ICMP protocol mainly uses two terms:
  - **ICMP Test:** ICMP Test is used to test whether the destination is reachable or not.
  - **ICMP Reply:** ICMP Reply is used to check whether the destination device is responding or not.
- The core responsibility of the ICMP protocol is to report the problems, not correct them. The responsibility of the correction lies with the sender.
- ICMP can send the messages only to the source, but not to the intermediate routers because the IP datagram carries the addresses of the source and destination but not of the router that it is passed to.

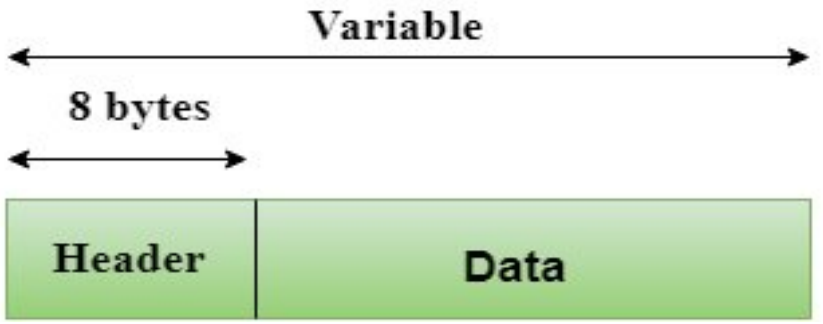
Transport Layer

- The transport layer is responsible for the reliability, flow control, and correction of data which is being sent over the network.
- The two protocols used in the transport layer are **User Datagram protocol and Transmission control protocol**.

User Datagram Protocol (UDP)

- It provides connectionless service and end-to-end delivery of transmission.
- It is an unreliable protocol as it discovers the errors but not specify the error.
- User Datagram Protocol discovers the error, and ICMP protocol reports the error to the sender that user datagram has been damaged.

User Datagram Protocol (UDP)



- **UDP consists of the following fields:**
  Source port address: The source port address is the address of the application program that has created the message.
  Destination port address: The destination port address is the address of the application program that receives the message.
  Total length: It defines the total number of bytes of the user datagram in bytes.
  Checksum: The checksum is a 16-bit field used in error detection.

Header Format

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

Transmission Control Protocol (TCP)

- It provides a full transport layer services to applications.
- It creates a virtual circuit between the sender and receiver, and it is active for the duration of the transmission.
- TCP is a reliable protocol as it detects the error and retransmits the damaged frames. Therefore, it ensures all the segments must be received and acknowledged before the transmission is considered to be completed and a virtual circuit is discarded.
- At the sending end, TCP divides the whole message into smaller units known as segment, and each segment contains a sequence number which is required for reordering the frames to form an original message.
- At the receiving end, TCP collects all the segments and reorders them based on sequence numbers.

Application Layer

- An application layer is the topmost layer in the TCP/IP model.
- It is responsible for handling high-level protocols, issues of representation.
- This layer allows the user to interact with the application.
- When one application layer protocol wants to communicate with another application layer, it forwards its data to the transport layer.
- There is an ambiguity occurs in the application layer. Every application cannot be placed inside the application layer except those who interact with the communication system. For example: text editor cannot be considered in application layer while web browser using **HTTP** protocol to interact with the network where **HTTP** protocol is an application layer protocol.

Following are the main protocols used in the application layer

- **HTTP:** HTTP stands for Hypertext transfer protocol. This protocol allows us to access the data over the world wide web. It transfers the data in the form of plain text, audio, video. It is known as a Hypertext transfer protocol as it has the efficiency to use in a hypertext environment where there are rapid jumps from one document to another.
- **SNMP:** SNMP stands for Simple Network Management Protocol. It is a framework used for managing the devices on the internet by using the TCP/IP protocol suite.
- **SMTP:** SMTP stands for Simple mail transfer protocol. The TCP/IP protocol that supports the e-mail is known as a Simple mail transfer protocol. This protocol is used to send the data to another e-mail address.

Following are the main protocols used in the application layer

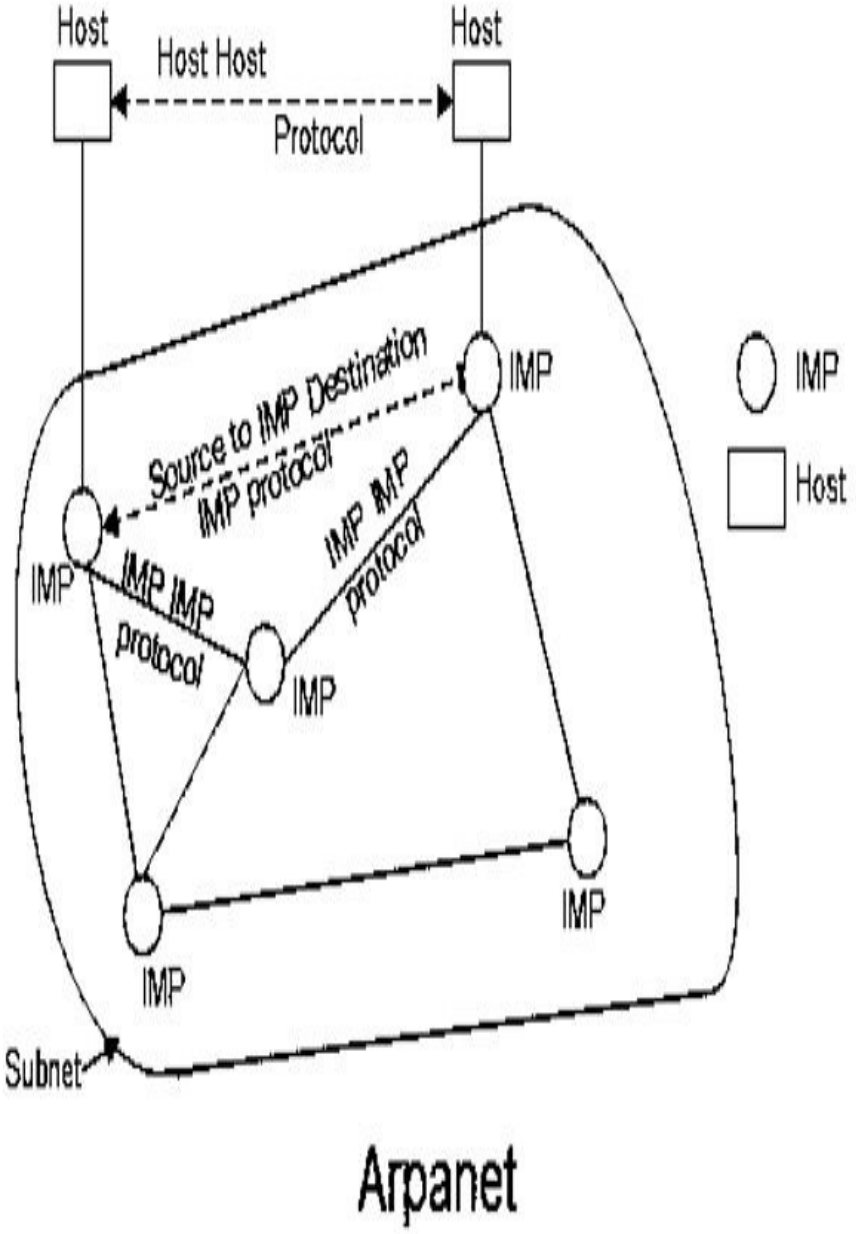
- **DNS:** DNS stands for Domain Name System. An IP address is used to identify the connection of a host to the internet uniquely. But, people prefer to use the names instead of addresses. Therefore, the system that maps the name to the address is known as Domain Name System.
- **TELNET:** It is an abbreviation for Terminal Network. It establishes the connection between the local computer and remote computer in such a way that the local terminal appears to be a terminal at the remote system.
- **FTP:** FTP stands for File Transfer Protocol. FTP is a standard internet protocol used for transmitting the files from one computer to another computer.

ARPANET

- The full form of ARPANET is **Advanced Research Projects Agency NET** was developed under the direction of the US Advanced Research Projects Agency and was based on a concept first published in 1967. With the interconnection of four university computers in 1969, the concept became a modest reality.
- It was the first network to implement the TCP/IP protocol. It was a very early packet switch network. This network became the foundation for the modern day internet.
- The protocols used in Arpanet were later developed for joining multiple networks, which gave rise to the modern day internet. It helps in grouping the data in digital communication to packets. It helps by introducing the protocol suit. Now it is the foundation for the internet we are using now.

Characteristics

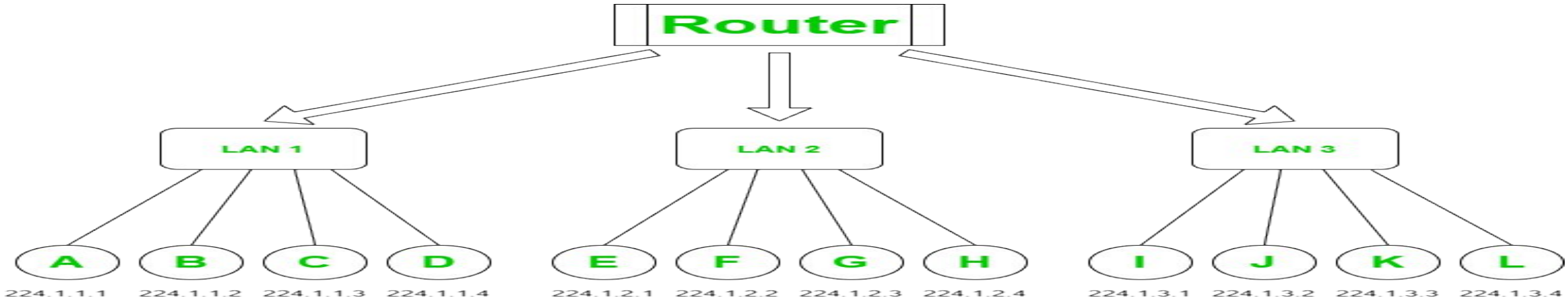
- Risk-taking
- Experimental
- Dynamic
- A head of industry at time
- Part of changing the way computing was done
- Building a new discipline.



Arpanet

Addressing

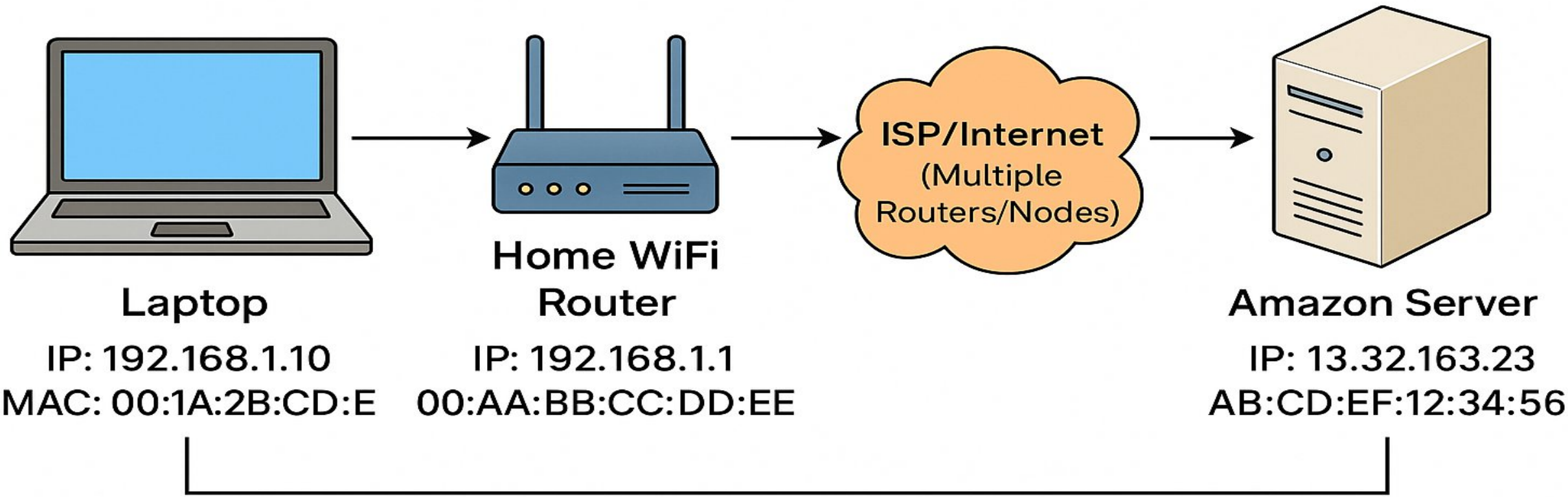
- A Network Address is a logical or physical address that uniquely identifies a host or a machine in a telecommunication network.
- A network may also not be unique and can contain some structural and hierarchical information of the node in the network.
- Internet protocol (IP) address, media access control (MAC) address and telephone numbers are some basic examples of network addresses. It can be of numeric type or symbolic or both in some cases.



Addressing

- It is the prime responsibility of the network layer to assign unique addresses to different nodes in a network. As mentioned earlier they can be physical or logical but primarily they are logical addresses i.e. software-based addresses.
- The most widely used network address is an IP address. It uniquely identifies a node in an IP network. An IP address is a 32-bit long numeric address represented in a form of dot-decimal notation where each byte is written in a decimal form separated by a period.

Addressing in Computer Networks



Zomoto/Swiggy analogy

1. Logical Addressing = Delivery Address (IP Address)Just like your home address tells the delivery guy where to take the food
An IP address tells the network where to send the data.
Example:Your Swiggy delivery address = #42, MG Road, Bangalore
Your computer's IP address = 192.168.1.10

2. Physical Addressing = Door Nameplate (MAC Address)The delivery agent might reach the building (via IP address),But to hand over the order, they look for your name on the door (like a MAC address).MAC Address Example: 00:1A:2B:3C:4D:5EUsed only within the local building (LAN) to find the exact flat.

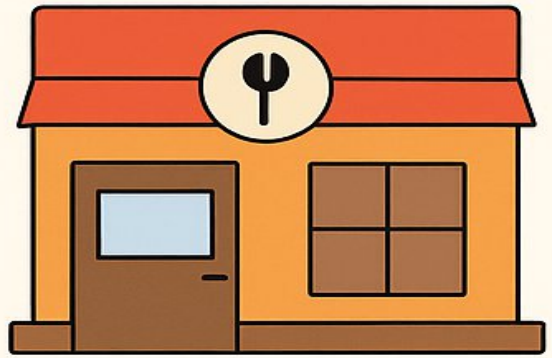
Addressing in Computer Networks

Places order

zomato

Delivers order

#42 MG Road, Hyderabad



Logical Address

= Delivery Address
(IP Address)

Restaurant

Door Nameplate
(MAC Address)

PHYSICAL LAYER

- In transmission media is the way the systems are connected to route data signals in a network.
- The telecommunication links are classified into two categories:
- Guided media (wired)
- Unguided media (wireless).
- Both guided and unguided are used for short distance (LANs, MANs) as well as long distance (WANs) communication

Physical Layer: Transmission Media

Guided Media

Letter sent via a postal van on a road

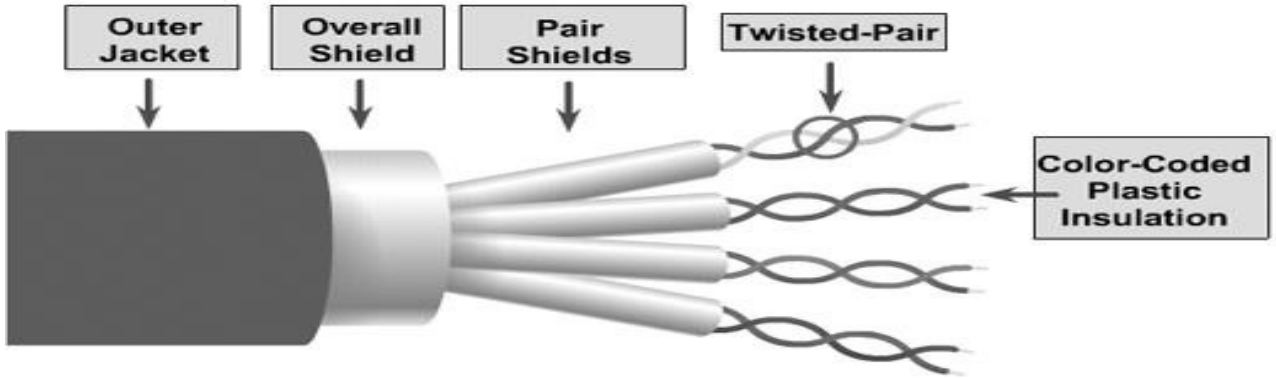
Unguided Media

Letter dropped from a helicopter flying over the city

Guided transmission media

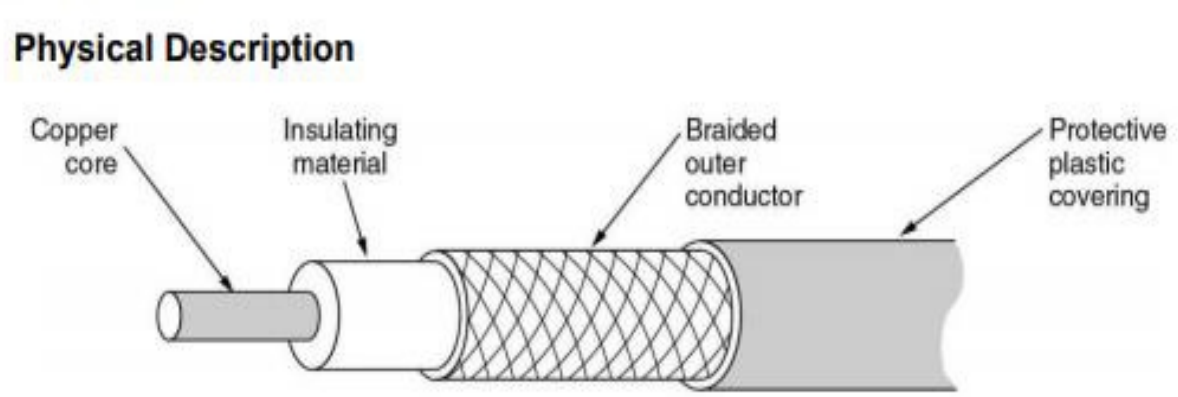
- Guided transmission media consists of physical connection between source and destination through a wire or a cable.
- There are three basic types of guided media which are as follows −
- Twisted pair cable
- Co-axial cable
- Fiber-optic cable

Twisted Pair Copper



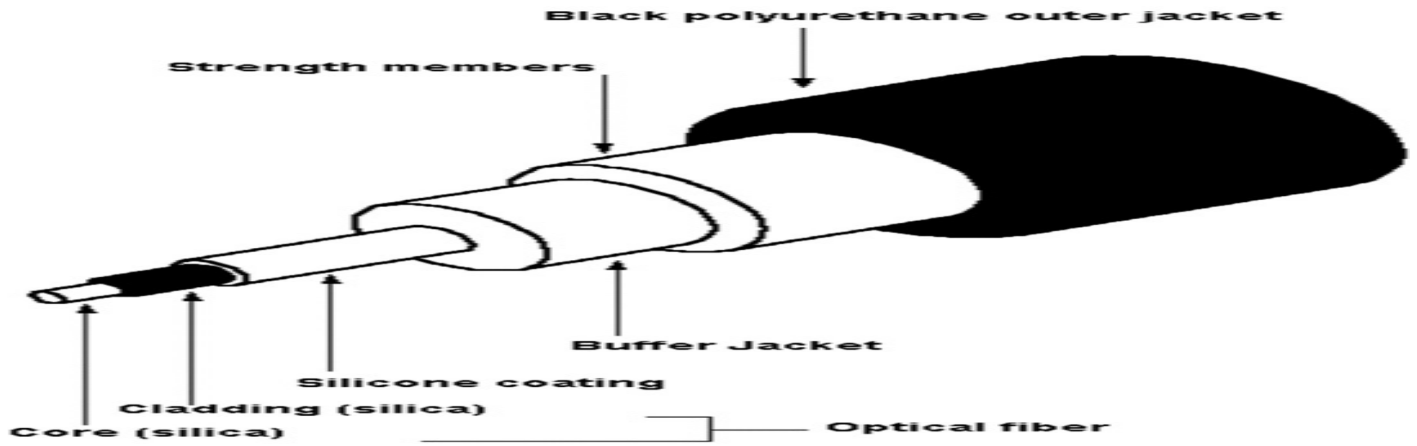
- **Step 1** − It is the most used media across the world. All the local telephone exchanges are made of twisted pair copper. These telephone lines are reused as last mile DSL access links to access the internet from home.
- **Step 2** − Twisted pair copper wires are also used in Ethernet LAN cables within homes and offices.
- **Step 3** − It supports low to High Data Rates which is in the order of Gigabytes.
- **Step 4** − These wires are effective up to a maximum distance of a few kilometres/miles, because the signal strength is lost significantly beyond the distance.
- **Step 5** − Generally, they come in two variants as follows −
- UTP (unshielded twisted pair)
- STP (shielded twisted pair)
- For every variant, there are multiple sub-variants, based on the thickness of the material (like UTP-3, UTP-5, UTP-7 etc.)

Copper Co-axial Cables



- **Step 1 −** Co-axial copper cables consist of inner copper conductor and an outer copper shield, which are separated by a di-electric insulating material, helpful in preventing signal losses.
- **Step 2 −**: Copper co-axial cables used in cable TV networks and as trunk lines between telecommunication equipment's.
- **Step 3 −** It serves as an internet access line from the home and supports medium to high data rates.

Fiber Optic Cables



- **Step 1** − In fiber optic cable the information is transmitted by propagation of optical signals (light) through fiber optic cables and not through the electrical/electromagnetic signals. Because of this, the fiber optics communication supports longer distances as there is no electrical interference.
- **Step 2** −: The fiber optic cables are made of very thin strands of glass (silica). It supports high data rates.
- **Step 3** − It is used for accessing the internet from home through FTTH (Fiber-To-The-Home) lines.
- Examples − OC-48, OC-192, FTTC, HFC.

Unguided transmission media

- In Unguided transmission media there is no physical connection between source and destination, instead they use air itself. These connections are not bound to a channel to follow.
- Unguided transmission media uses two basic types of primary technologies which are as follows −
- Microwaves
- **Step 1** − Microwaves travel in straight lines and therefore the narrow focus concentrates all the energy into a beam.
- **Step 2** − In microwaves periodic repeaters are necessary for long distances and for transmitting and receiving antennas are aligned accurately.
- Example − Bluetooth technology.

Satellite

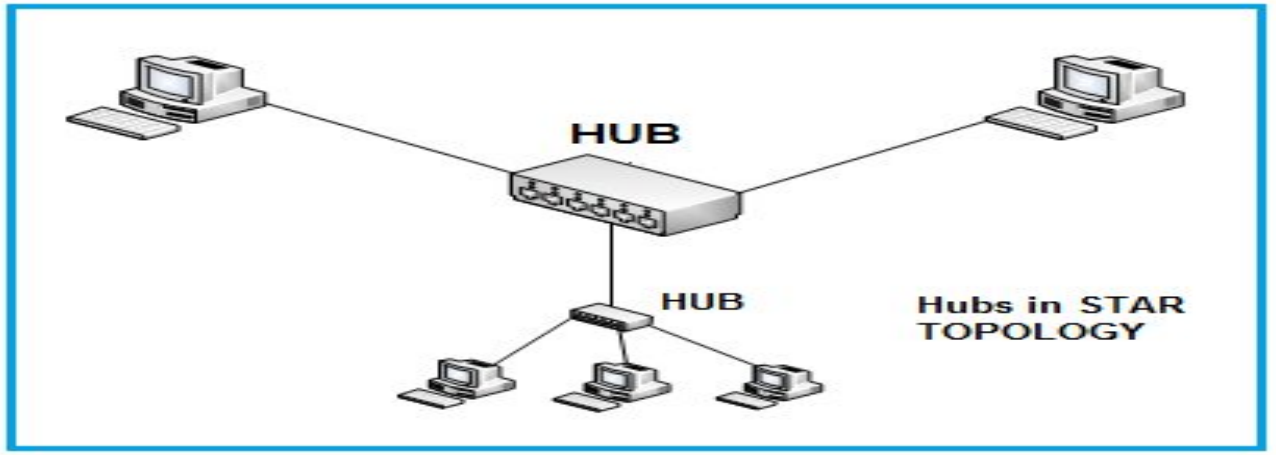
- **Step 1** − Use microwave radio to protect from the atmosphere and act as a microwave relay station.
- **Step 2** − They are situated in space 22,000 miles above the equator, and it appears stationary from the earth as it rotates with specific speed.
- **Step 3** − They can amplify and relay microwave signals from one transmitter on the ground to another.

Differences

- The major differences between guided and unguided transmission media are as follows

Guided media	Unguided media
The signal requires a physical path for transmission.	The signal is broadcasted through air or sometimes water
It is called wired communication or bounded transmission media.	It is called wireless communication or unbounded transmission media.
It provides direction to signal for travelling. Twisted pair cable, coaxial cable and fibre optic cable are its types.	It does not provide any direction. Radio waves, microwave and infrared are its types.

Network Devices (Hub, Repeater, Bridge, Switch, Router, Gateways)

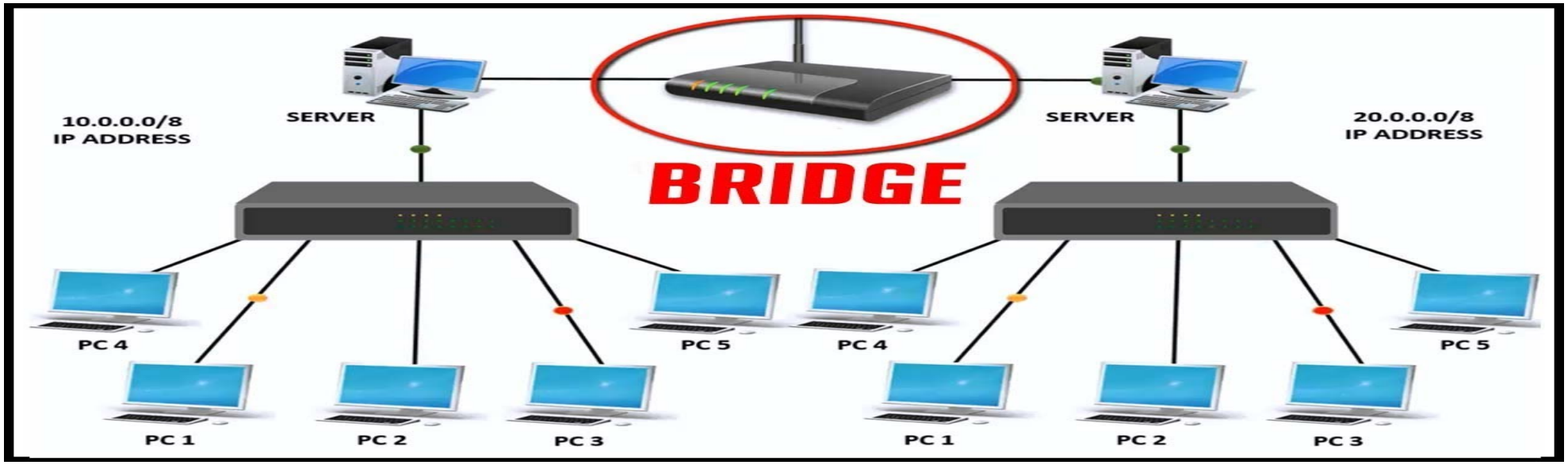


- Hub
- Hubs work in the physical layer of the OSI model. A hub is a device for connecting multiple Ethernet devices and making them act as a single network segment. It has multiple inputs and output ports in which a signal introduced at the input of any port appears at the output of every port except the original incoming port.
- A hub can be used with both digital and analog data. Hubs do not perform packet filtering or addressing function, they send the data packets to all the connected devices.

Switch

- Switches may operate at one or more layers of the OSI model. They may operate in the data link layer and network layer; a device that operates simultaneously at more than one of these layers is known as a *multilayer switch*.
- A Switch can check the errors before forwarding the data, which makes it more efficient and improves its performance. A switch is the better version of a hub. It is a multi-port bridge device.

Bridge



- A bridge operates at the data link layer of the OSI model.
- It can read only the outmost hardware address of the packet but cannot read the IP address.
- It reads the outmost section of the data packet to tell where the message is going.
- It reduces the traffic on other network segments. It does not send all the packets. So, a bridge can be programmed to reject packets from a particular network.

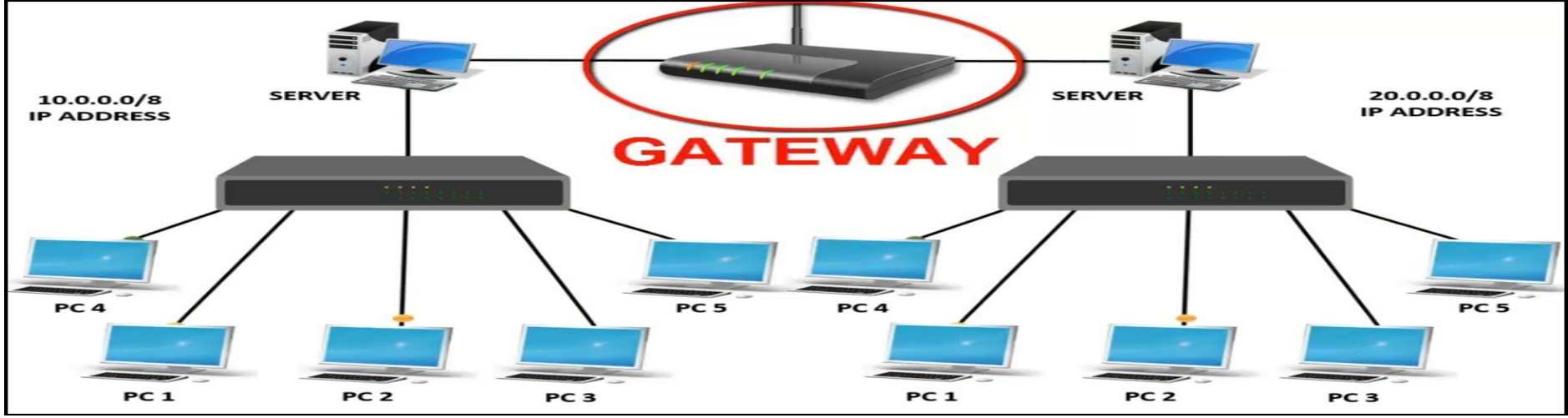
Repeater

- A repeater operates at the physical layer of the OSI model.
- A Repeater connects two segments of a network cable.
- Sometimes it regenerates the signals to proper amplitudes and sends them to the other segment.
- If the signal becomes weak, it can copy the signal bit by bit and regenerate it at the original strength.
- It is a 2-port device.

Router

- Routers are small physical devices that operate at the network layer to join multiple networks together.
- A router is a device like a switch that routes data packets based on their IP addresses.
- Routers normally connect LANs and WANs and have a dynamically updating routing table based on which they make decisions on routing the data packets.
- A Router divides the broadcast domains of hosts connected through it.

Gateway



- A gateway is an internetworking capable of joining together two networks that use different base protocols.
- A network gateway can be implemented completely in software, hardware, or a combination of both, depending on the types of protocols they support.
- A network gateway can operate at any level of the OSI model. A broadband router typically serves as the network gateway, although ordinary computers can also be configured to perform equivalent functions.
- A gateway is a router or proxy server that routes between networks.
- A gateway belongs to the same subnet to which the PC belongs.