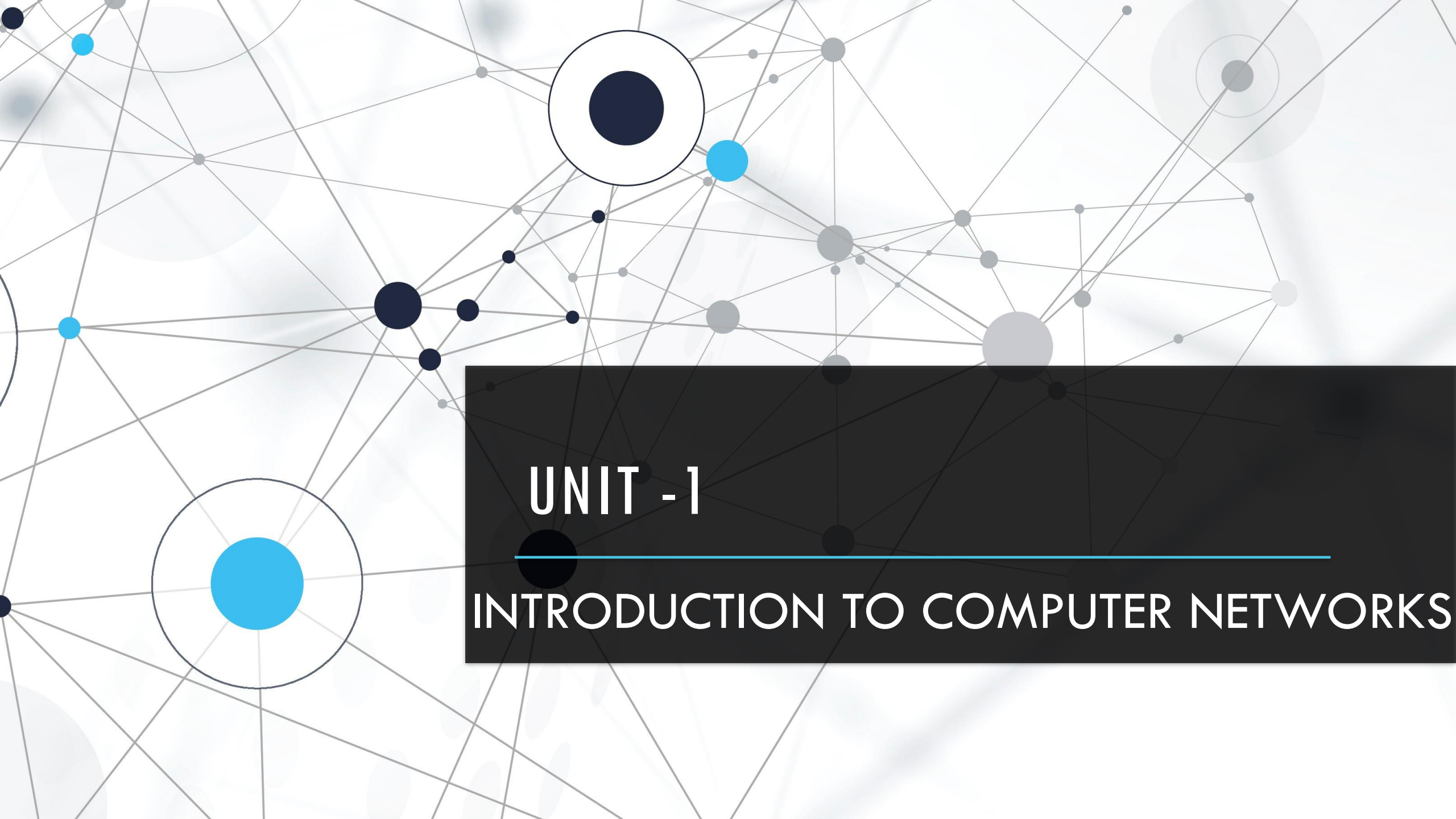


UNIT -1

INTRODUCTION TO COMPUTER NETWORKS

CONTENTS

WHAT IS COMPUTER NETWORK?

> A network is a **set of devices** (often referred to as **nodes**) connected **by communication links.**

> A node can be a computer, printer, or any other device capable of **sending and/or receiving** data generated by other nodes on the network.

> These devices in a network are connected using **wired or wireless** transmission media such as cable or air.

USE OF COMPUTER NETWORK

> 1. **Resource Sharing:** Resource sharing means you can share one Hardware and Software among multiple users.

>2. **Information Sharing:** We can share Information over the network, and it provides Search capabilities such as WWW.

>3. **Communication:** Communication includes email, calls, message broadcast, electronic funds transfer system etc.

> 4. **Entertainment Industry:** In Entertainment industry also uses computer networks widely. Some of the Entertainment industries are Video on demand, Multiperson real-time simulation games, movie/TV programs, etc.

> 5. **Access to Remote Databases:** Computer networks allow us to access the Remote Database of the various applications by the endusers. Some applications are Reservation for Hotels, Airplane Booking, Home Banking, etc.

>6. **Home applications:** Common uses of computer network are as home applications. For example, access to remote instruction, electronic commerce and entertainment. Another way is managing bank accounts, paying bills electronically.

>7. **Business applications:** The result of business application here is resource sharing. Most of the companies are doing business electronically with other companies and with other clients worldwide with the help of a computer network.

> 8. **Mobile(portable) users:** The rapidly growing sectors in computer applications are mobile devices like notebook computers and PDAs. It is widely used in new-age technology like smartwatches, wearable devices, etc.

>9. **Social media:** It helps people to share and receive any information related to political, ethical and social issues.

TYPES OF COMPUTER NETWORK

> Computer Networks can be categorized by their size as well as their purpose, mode, authentication, etc.

> The size of a network can be expressed by the geographic area.

> Some of the different **networks based on size/scale** are:

PAN (PERSONAL AREA NETWORK)

> Personal area networks appropriate to **personal or separate workspace** under the range of **10 meters.**

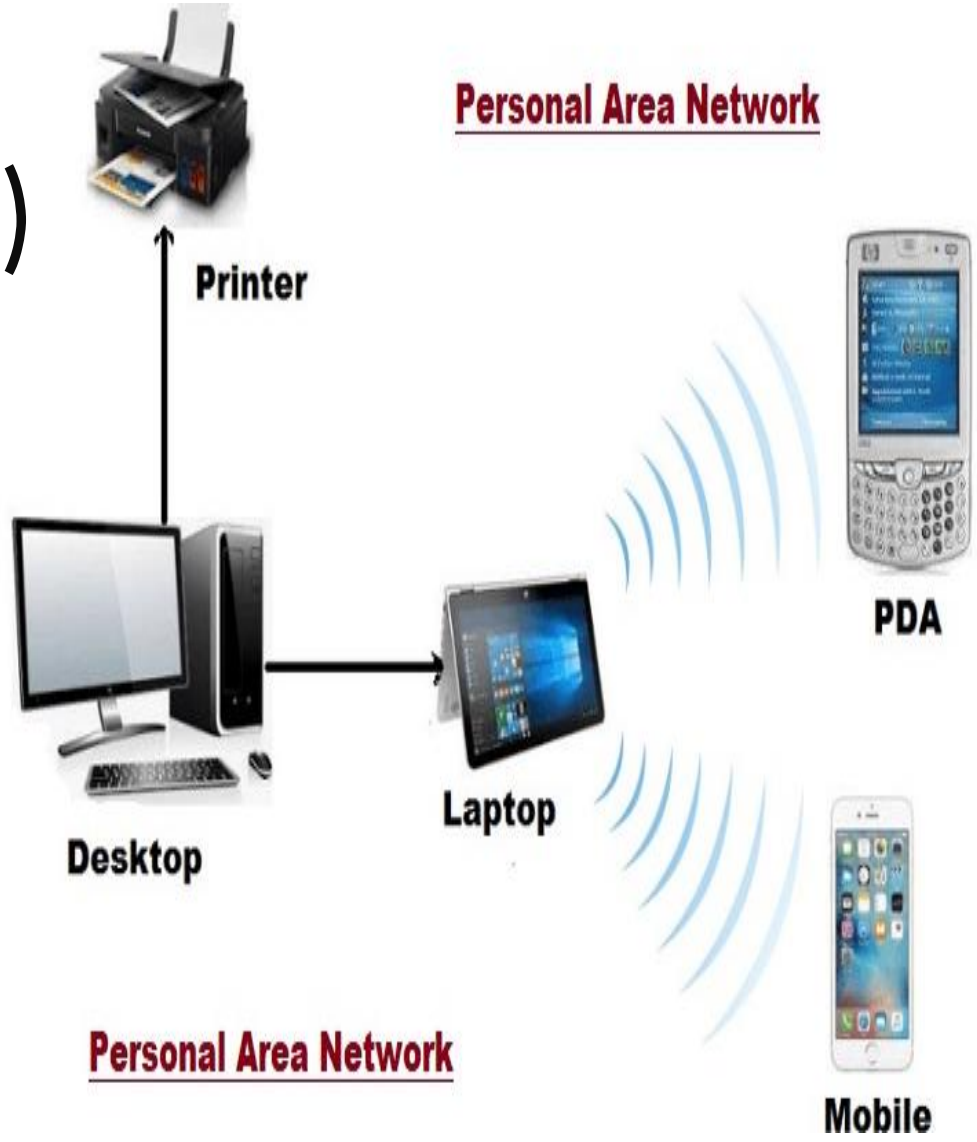
> These networks are mostly used to connect **tablets, smartphones and laptops.**

> A **small network centered** around an individual person, typically within a range of a few meters.

> **Examples:** Bluetooth, Infrared, USB connections.

> **Advantages:** Easy to set up, low cost, portable, doesn't require frequent maintenance

> **Disadvantages :** Low network coverage area, limited data rates, devices may not be compatible



LAN (LOCAL AREA NETWORK)

> LAN is a **small high-speed network**. In LAN **few numbers of systems** are interconnected with networking device to create network.

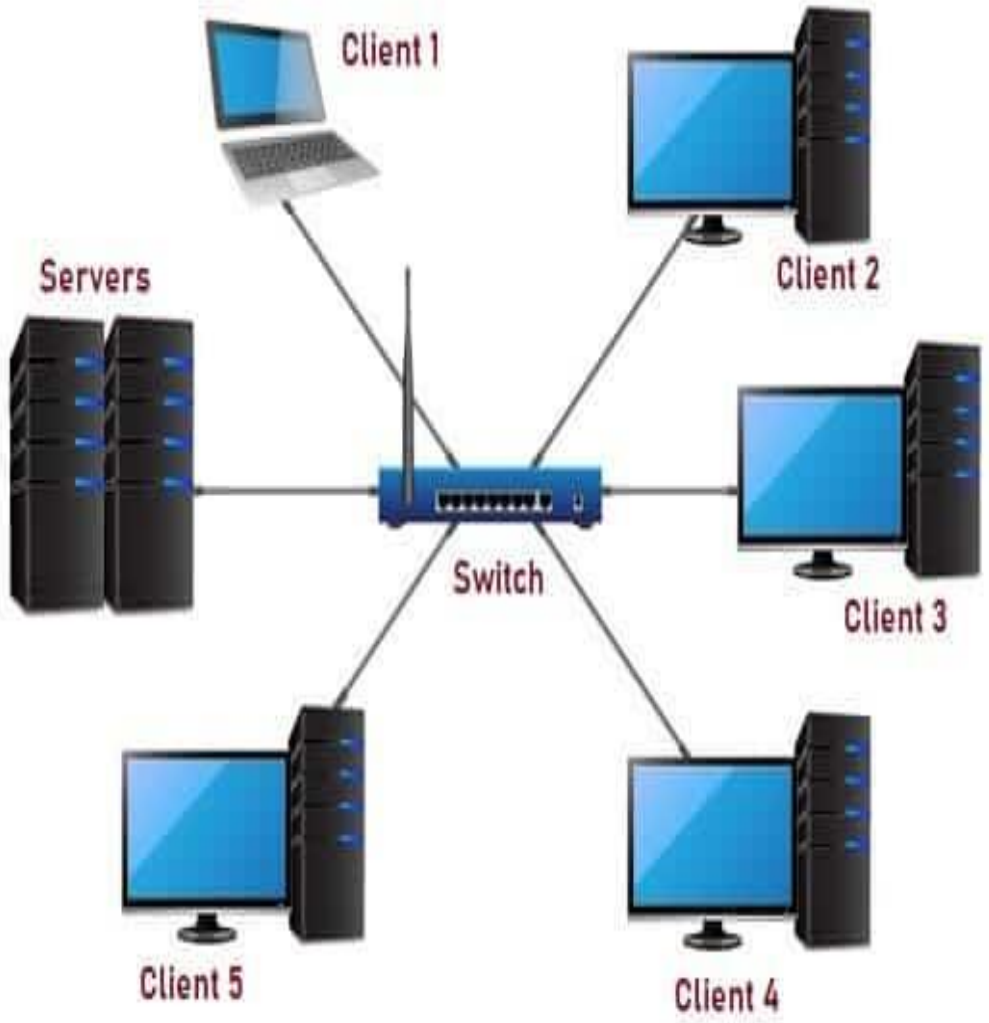
> The network that **spans a relatively small area** that is, in the single **building or campus** is known as LAN.

> **Sharing resources** such as files, printers, and internet connections among a group of computers in a **few hundred meters.**

>**Examples: Ethernet-based** networks in homes or small businesses.

> **Advantages:** Resource Sharing, High Speed, Cost-Effective, Centralized Management, Flexibility.

> **Disadvantages :** Limited Coverage, Maintenance Problems, Security Risks.



MAN (METROPOLITAN AREA NETWORK)

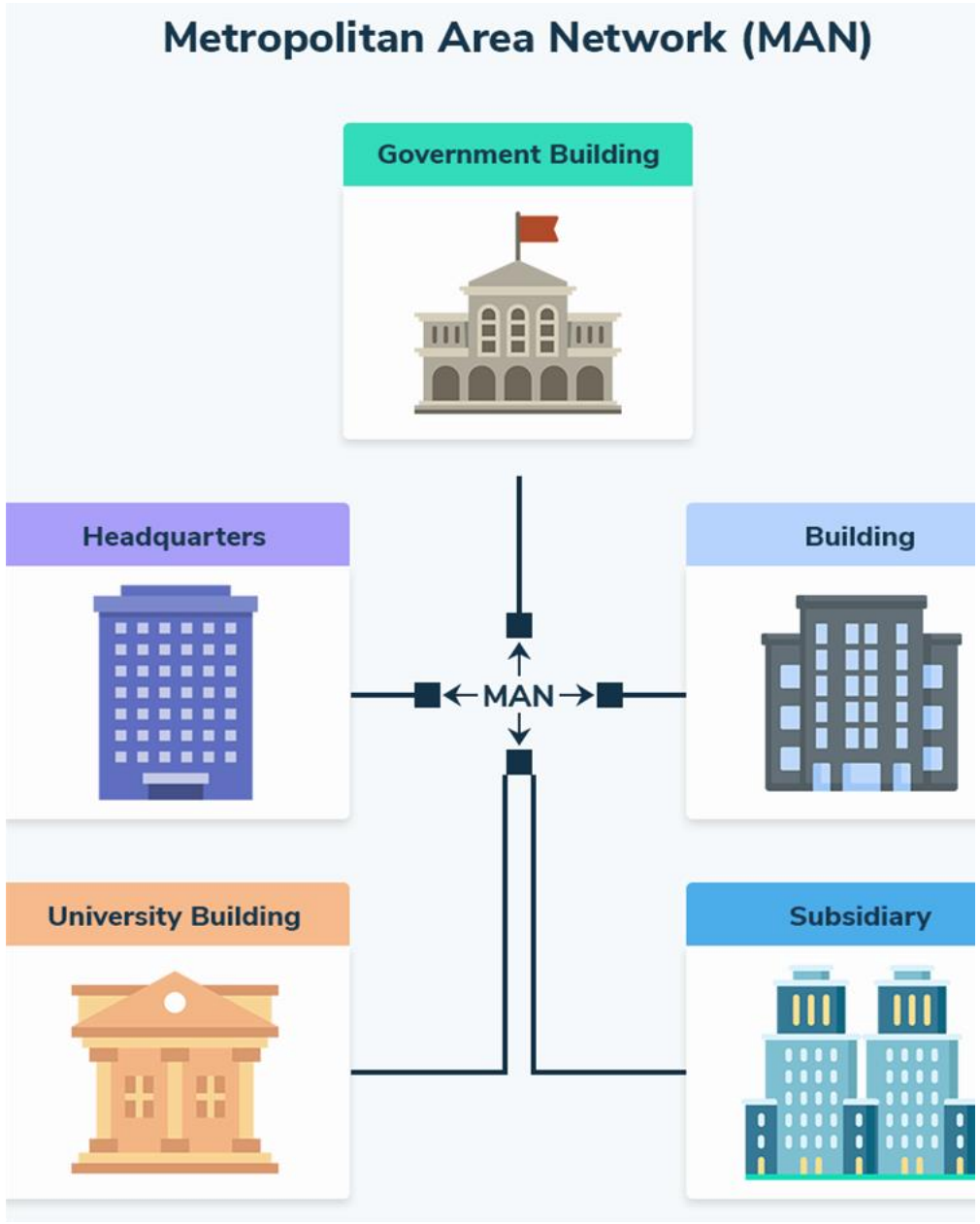
> Metropolitan area networks are used to connect the devices over an **entire city under the range of up to 50 km.**

> It may be a single network or a network in which **more than one local area network** can share their resources

>**Examples:** These networks are used in the **telephone** company network and **cable TV network.**

> **Advantages:** Covers a larger area than LAN, provides high-speed data transfer, easy to manage, efficient communication across multiple locations.

> **Disadvantages :** Limited Coverage compared to WAN, requires advanced technology and infrastructure so can be bit expensive to setup and maintenance.



WAN (WIDE AREA NETWORK)

> WAN is **collection of network (or LAN).**

> Wide Area Networks are used in the wide geological range over a **country and continent over 50 kilometers,** up to global scale.

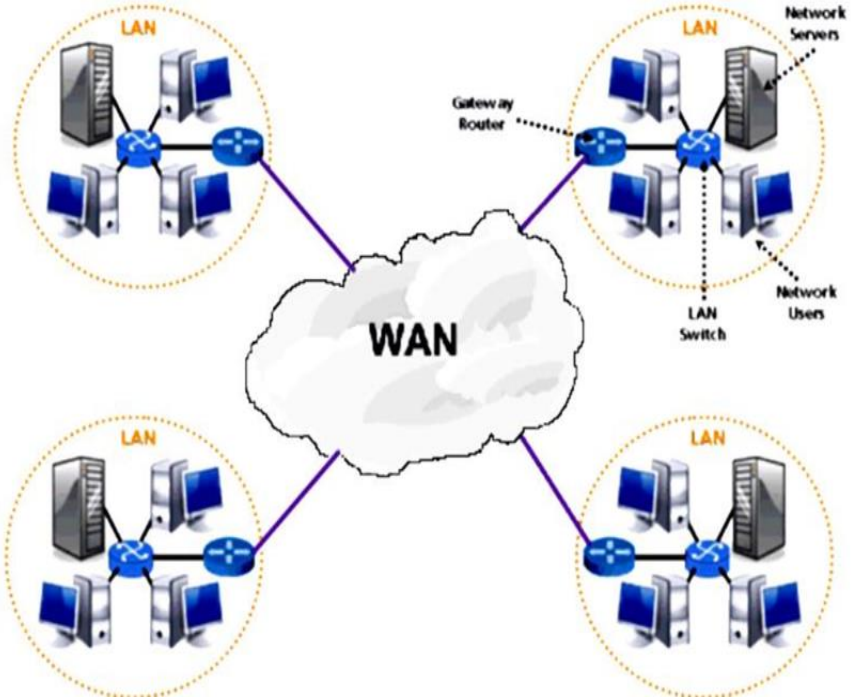
> It contains a **collection of machines** intended for running user (i.e., application) programs. These machines are called as **hosts.**

> **Usage:** Used for **long-distance communication** and data transfer between different regions or countries.

> **Examples:** The **Internet,** corporate networks connecting branch offices in different cities or countries. The **cellular telephone network** is another example of a WAN that uses wireless technology.

>**Advantages:** Allows Resource Sharing, Centralized Data Management, Scalibility, Supports real-time communication.

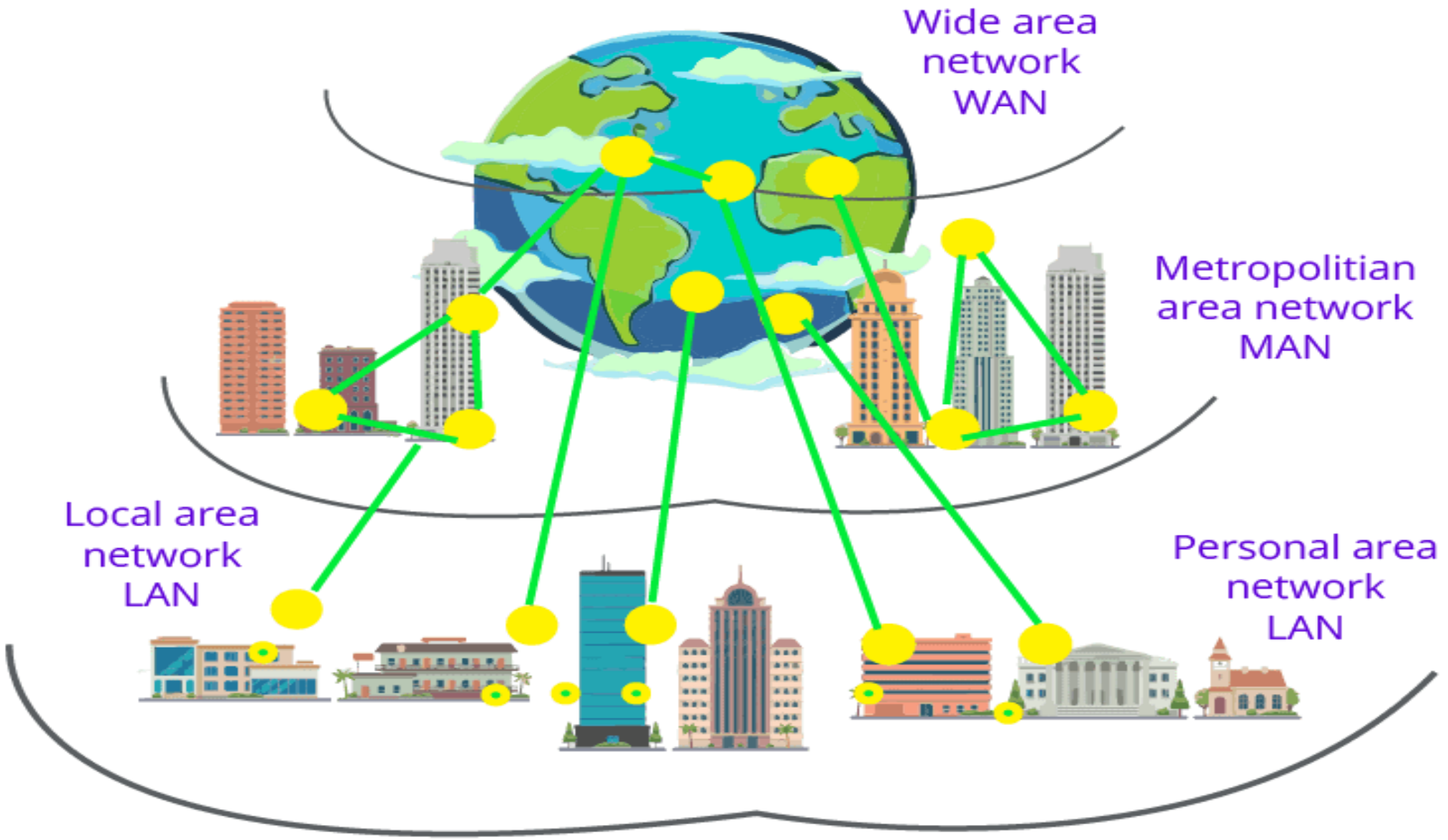
> **Disadvantages :** Expensive due to complex setup, Lower Speed, Security Issues.



TYPES OF COMPUTER NETWORK - SUMMARY

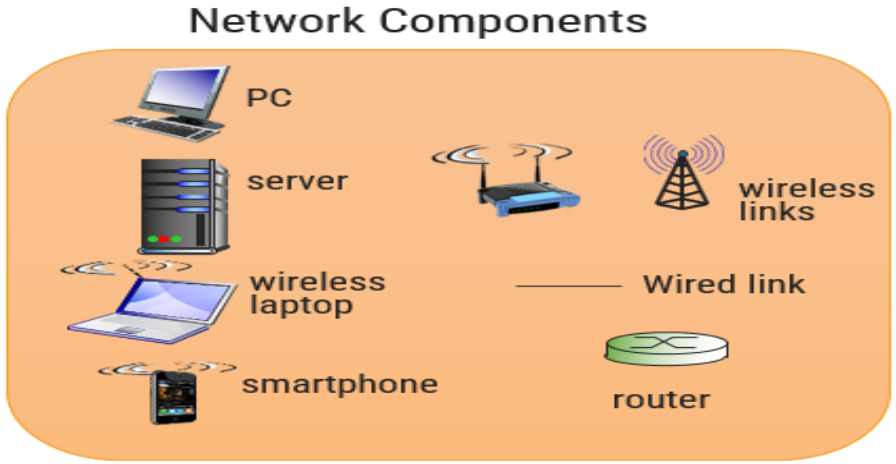
Comparison	LAN	MAN	WAN
Full Name	Local Area Network	Metropolitan Area Network	Wide Area Network
Meaning	A network that connects a group of computers in a small geographical area	It covers relatively large region such as cities, towns	It spans large locality & connects countries together. e.g. Internet
Ownership of Network	Private	Private or Public	Private or Public (VPN)
Design and Maintenance	Easy	Difficult	Difficult
Propagation Delay	Short	Moderate	Long
Speed	High	Moderate	Low
Equipment Used	NIC, Switch, Hub	Modem, Router	Microwave, Radio Transmitter & Receiver
Range(Approximately)	1 to 10 km	10 to 100 km	Beyond 100 km
Used for	College, School, Hospital	Small towns, City	State, Country, Continent

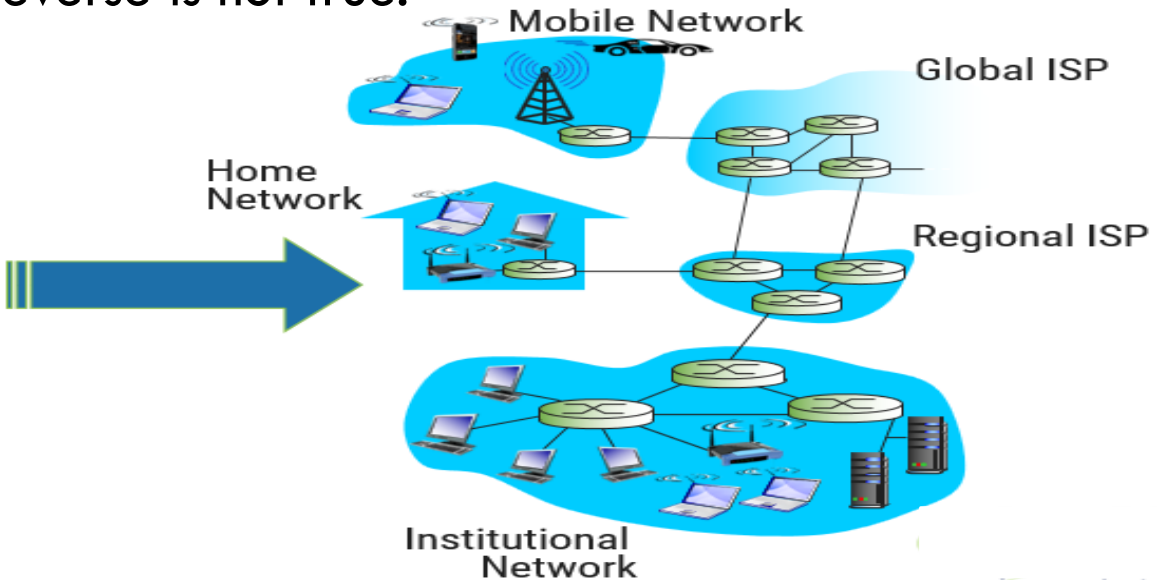
TYPES OF COMPUTER NETWORK - SUMMARY



INTERNET

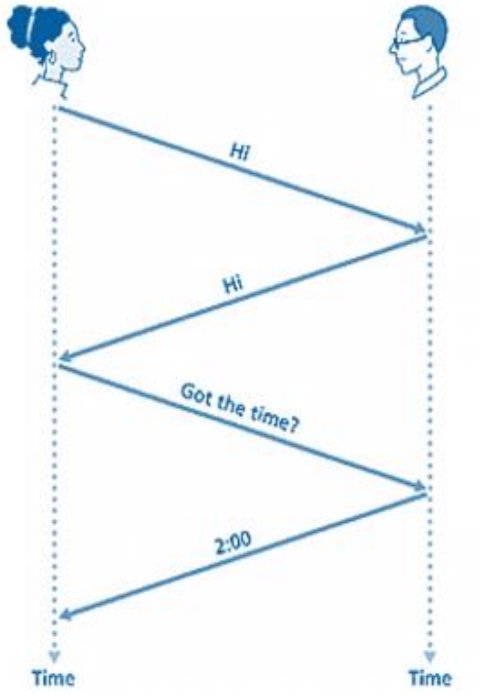
- **A collection of interconnected networks is called an internetwork or internet.**
- The **Internet uses ISP networks** to connect enterprise networks, home networks, and many other networks.
- The internet is type of world-wide computer network.
- The lowercase **internet means multiple networks connected together,** using a common protocol suite. The uppercase **Internet refers to the collection of hosts** around the world that can communicate with each other using TCP/IP. While the Internet is an internet. the reverse is not true.





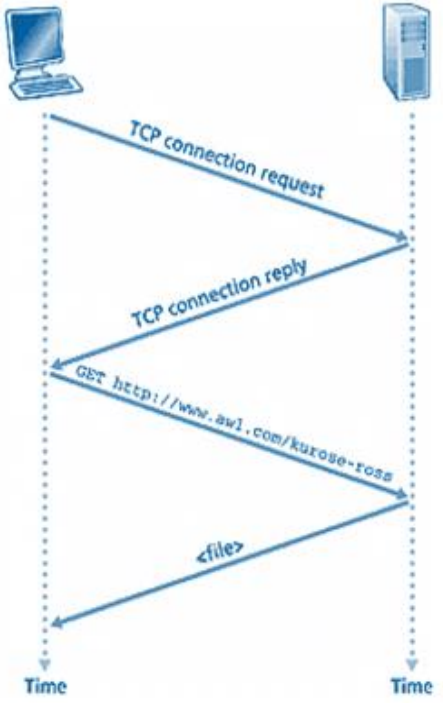
PROTOCOL

- Human Protocol(Language)
  - "what's the time?"
  - "I have a question"
  - Introduction Talk



Protocol is define format, order of message that sent and received among network entities, and actions taken on message transmission and reception.

- Network Protocol
  - Set of rules
  - Machines rather than humans.
  - All communication activity in Internet governed by protocols.



NETWORK DEVICES

REPEATER

A repeater is a two-port network device that regenerates the signal over a network before it becomes weak or gets damaged.

BRIDGE

A bridge is a device that joins any two networks or host segments together.

MODEM

Modems are devices that transform digital signals into the form of analog signals that are of various frequencies

NETWORK HUB

A network hub is a multiport repeater that connects multiple wires from different branches.

NETWORK SWITCH

Switches play a more important role than hubs. A switch is a multi-port device that enhances network efficiency.

GATEWAY

As the name suggests, the gateway is a passage that interlinks two networks together.

ACCESS POINT

An AP or Access Point is a wireless appliance that operates on the OSI model's second layer. It can be used in two ways.

NIC (NETWORK INTERFACE CARD)

> NIC is a hardware component used to connect a computer with another computer onto a network o It can support a transfer rate of 10,100 to 1000 Mb/s.

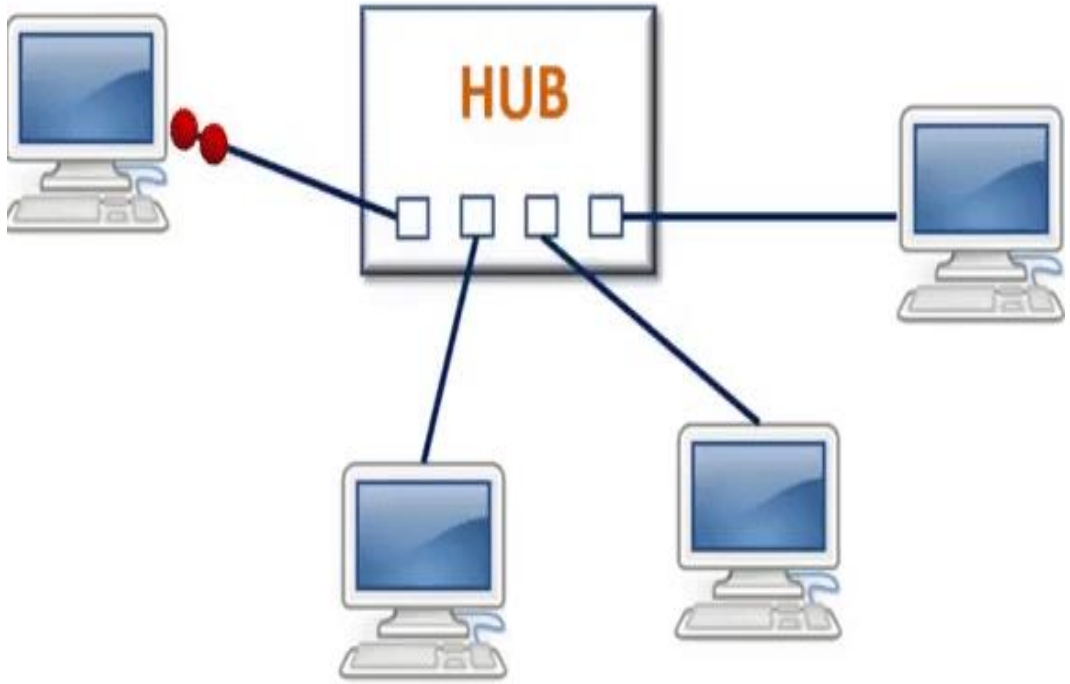
> The MAC address or physical address is encoded on the network card chip which is assigned by the IEEE to identify a network card uniquely. The MAC address is stored in the PROM (Programmable read-only memory).

> Types of NIC: 1. Wired 2. Wireless

> Wired NIC: The Wired NIC is present inside the motherboard. Cables and connectors are used with wired NIC to transfer data.

>Wireless NIC: The wireless NIC contains the antenna to obtain the connection over the wireless network. For example, laptop computer contains the wireless NIC

HUB



> It is uses to connect systems or nodes or networks in LAN.

> It has direct connection to a node (point to point connection).

> It prevents collision between packet transmission from one node to other.

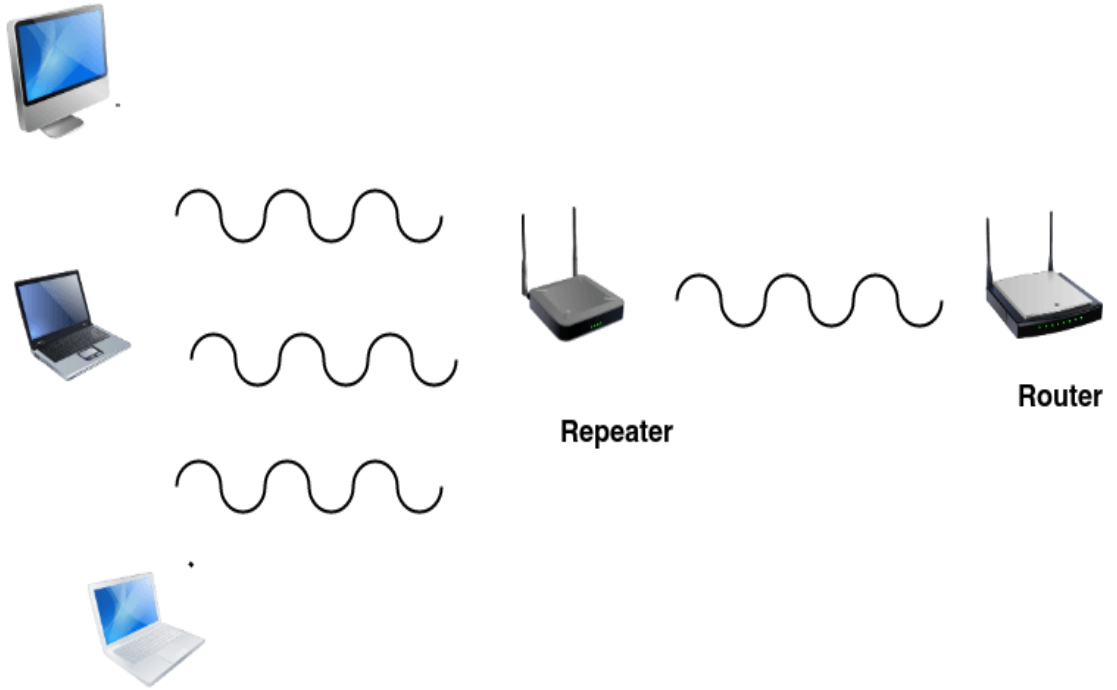
> A hub takes data from input port & retransmits input data on output port.

> A Hub is a physical layer hardware device that divides the network connection among multiple devices.

>When computer requests for some information from a network, it first sends the request to the Hub through cable.

>Hub will broadcast this request to the entire network. All the devices will check whether the request belongs to them or not. If not, the request will be dropped. It more simply called **concentrators**.

REPEATER



> A repeater is a device which regenerates or amplifies the data or signal so that it can be travel to the other segment of cable.

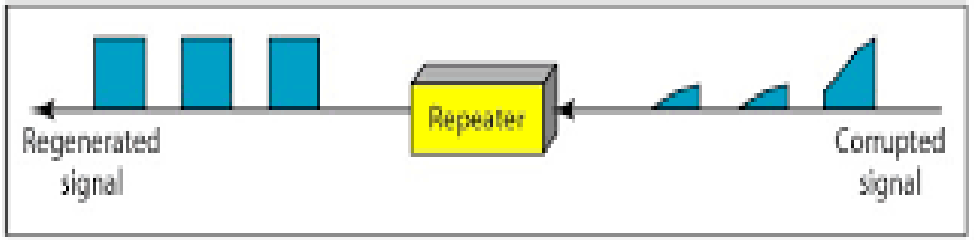
> It is used to extend the distance of a particular network.

> It boost the signal and then send it to next node.

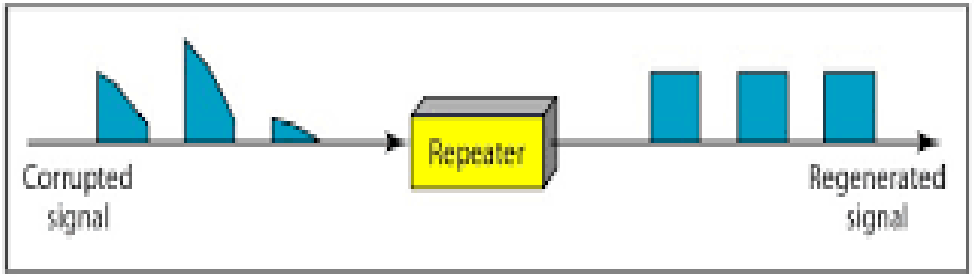
> It is used to connect two networks that uses same type of media or technology and protocol.

> It does not filter or translate any data.

> It works in physical layer.

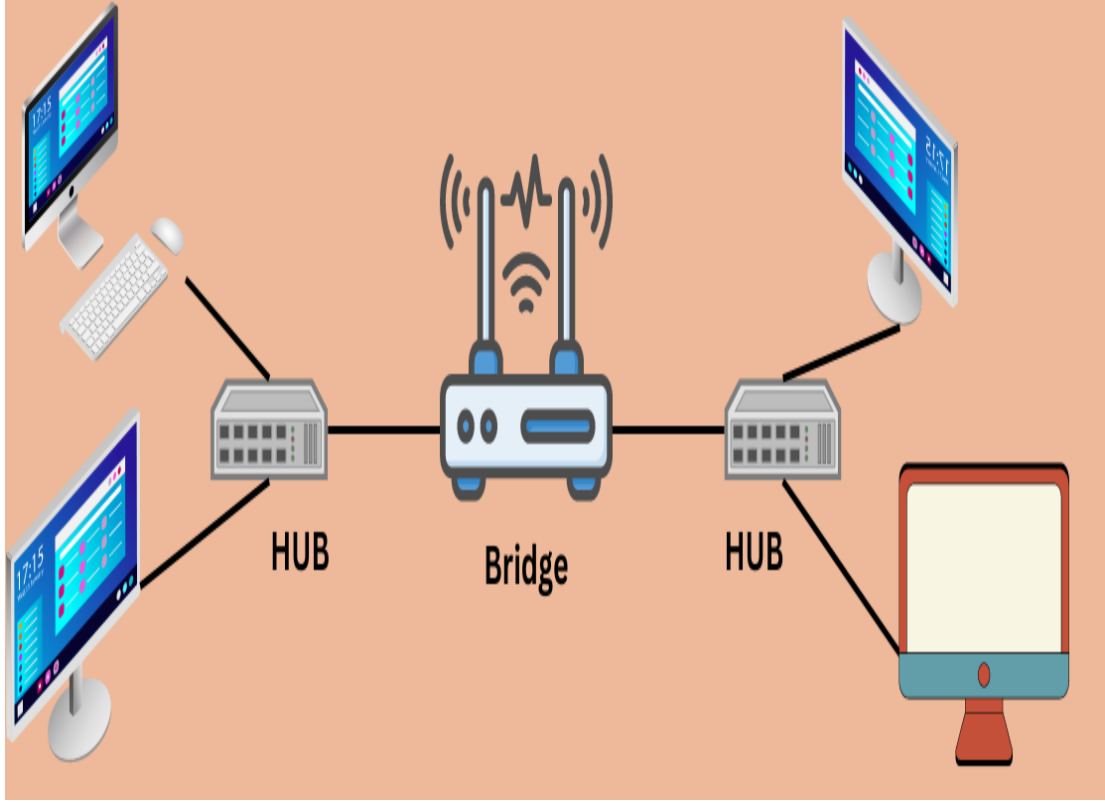


a. Right-to-left transmission.



b. Left-to-right transmission.

BRIDGE



> It is used to connect two networks.

>It divides the collision domain based on number of ports or interface present in a bridge.

> It uses the packet switches that forward and filter the frames using LAN destination address.

> Bridge examines the destination address of frame and forwards it to the interface or port which leads to the destination.

> It uses the routing table for routing frame from one node to other using MAC address.

>It works in Data Link Layer.

> It is used to connect two networks.

>It divides the collision domain based on number of ports or interface present in a bridge.

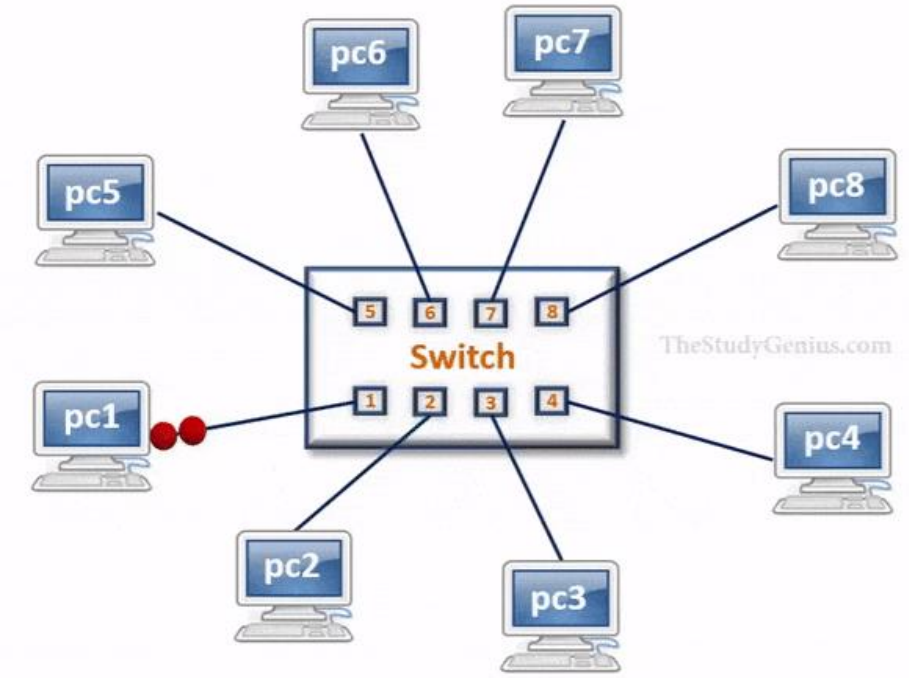
> It uses the packet switches that forward and filter the frames using LAN destination address.

> Bridge examines the destination address of frame and forwards it to the interface or port which leads to the destination.

> It uses the routing table for routing frame from one node to other using MAC address.

>It works in Data Link Layer.

SWITCH



> It is similar to bridge. It has more number of interfaces as compared to b

> It allows direct communication between the nodes.

>It works in Data Link Layer.

> It uses MAC address for data transmission and communication.

> A switch is a hardware device that connects multiple devices on a computer network.

> A Switch contains more advanced features than Hub.

>The Switch contains the updated table that decides where the data is transmitted or not.

> Switch delivers the message to the correct destination based on the physical address present in the incoming message.

> A Switch does not broadcast the message to the entire network like the Hub.

> It determines the device to whom the message is to be transmitted.

> Therefore, we can say that switch provides a direct connection between the source and destination. It increases the speed of the network.

ROUTER

> It is used to **connect different types of network** (types- architecture/ Protocol).

> It work **similar to bridge** but it **uses IP address** for routing data. Router can't be used for connecting Systems.

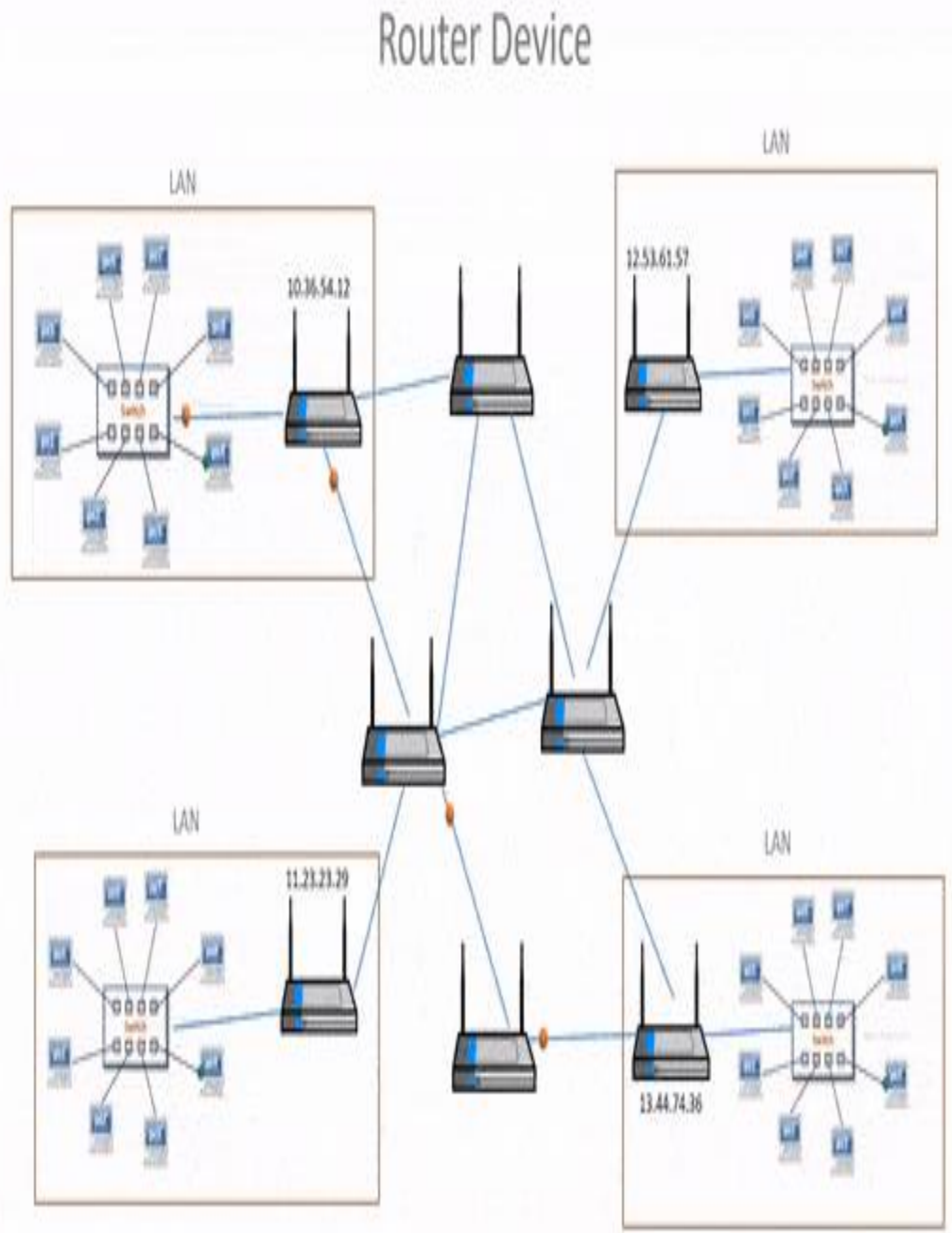
> It works in **Network Layer** of OSI Reference Model.

> A router is a hardware device which is used to **connect a LAN with an internet connection**.

>It is used to **receive, analyze and forward the incoming packets** to another network.

>It determines **the best path** from the available paths for the transmission of the packet.

> Router enhances the overall performance of the network.



GATEWAY(1)

> Gateways make **communication possible between systems that use different communication protocols,** data formatting structures, languages and architectures.

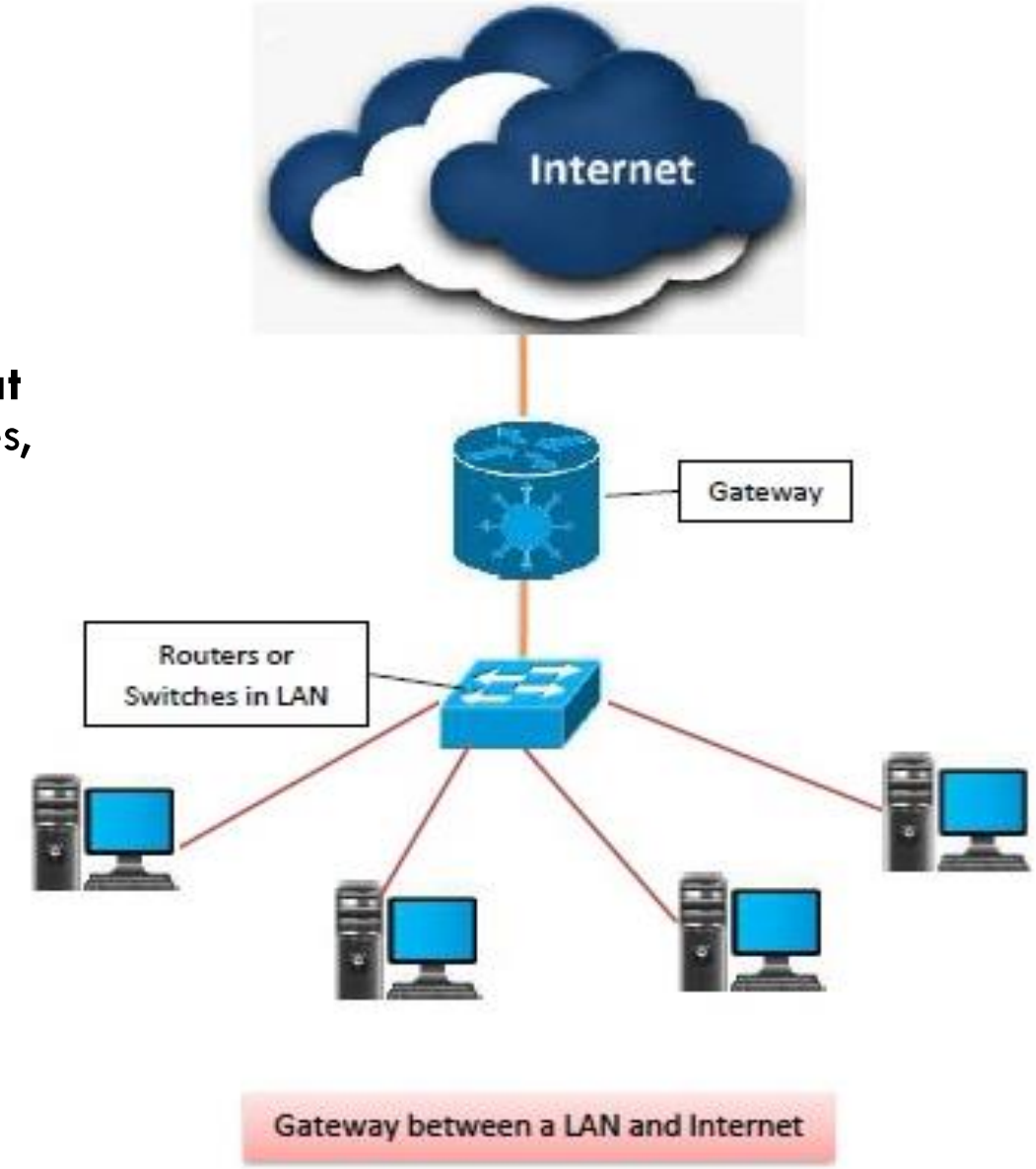
> Gateways **repackage data** going from one system to another.

>Gateways are usually **dedicated servers** on a network and are task-specific.

> Gateways **serve as an entry and exit point** for a network as all data must pass through or communicate with the gateway prior to being routed.

> Its primary function is to **translate data between networks** that use different protocols or technologies.

> Gateways are also known as **protocol converters** because they help to convert protocol supported by traffic of the different networks into that are supported by this network. Because of that, it makes smooth communication between two different networks.

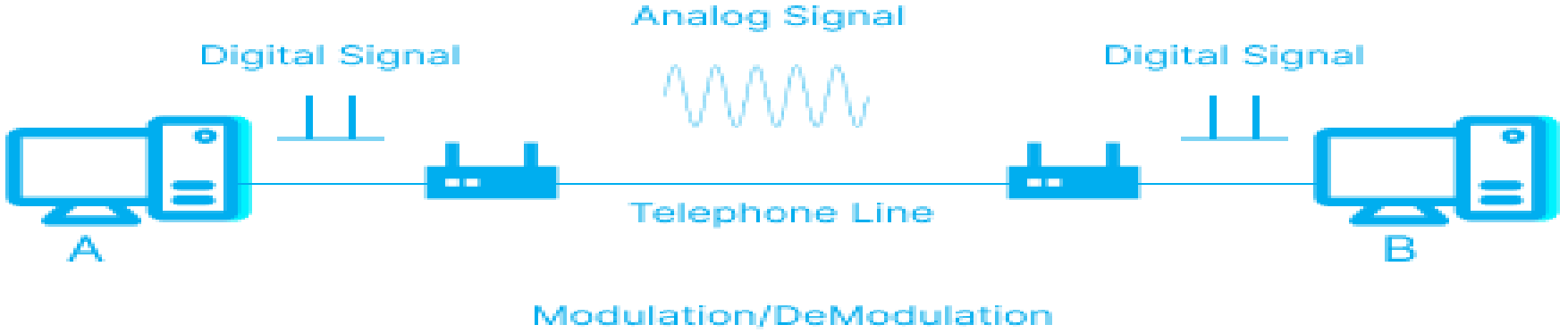


Gateway between a LAN and Internet

GATEWAY(2)

- Gateway has a simple working methodology of five steps:
  - Step 1: It **gets data** from the network
  - Step 2: It **intercepts** and **analyzes** the received data.
  - Step 3: It **routes the data** to the destination address.
  - Step 4: It **converts the received data** to make that compatible with the receiver network.
  - Step 5: It **sends the final data** inside the network.
- Actually what happens on the gateway after receiving a data packet is that they **check header information** that is present in the data packet.
- After that, it **validates the destination IP address** and searches for any error. If it gets no error then it makes that data packet compatible for the new network by converting protocols or other stuff.

MODEM



>A modem is a **hardware device** that allows the **computer to connect to the internet** over the existing **telephone line.**

> A modem is not integrated with the motherboard rather than it is **installed on the PCI slot found on the motherboard.**

>It stands for **Modulator/Demodulator.** It **converts the digital data into an analog signal** over the telephone lines.

> **<u>Modulation</u>** is a process of adding meaningful information to a carrier wave so that it can be transmitted over long distances.

>Based on the differences in speed and transmission rate, a modem can be classified in the following categories:

- > Standard PC modem or Dial-up modem
- > Cellular Modem
- > Cable modem

NETWORK SOFTWARE

> Network Software is mainly focused on reducing design issues like **managing, improving, or deploying a network.** It helps network administrators to **manage a network and prevents unauthorized access** and various cyber-attacks, as by using network software one can restrict access to the network.

> The two major software used in computer networks are the **Operating system and the Protocol suite.**

>>The function of Operating system is to support network. One can use OS to make system a server.

>>**Protocol suite consists of layers** and each layer is working according to different protocols. Here, protocol is a set of rules upon which communication devices agree to communicate successfully.

> Network software is intended for network administrators so that they can set up and install OS & protocol suites (OSI and TCP/IP models) in a network to secure the network.

> Nowadays software and hardware are integrated into some network devices such as routers and switches. Due to this network software structure is highly structured in today's time. So, the main five techniques are used to understand the network software structuring. They are as follows:

1. Protocol Hierarchies
2. Design Issues for the layers
3. Connection-oriented and Connectionless
4. Service primitives
5. Relationship of Services to protocol

PROTOCOL HIERARCHIES

> A protocol hierarchy in computer networks refers to the **organization and arrangement of networking protocols in a layered structure.**

> This layered approach helps in achieving interoperability, modularity, and ease of implementation and maintenance within complex network systems.

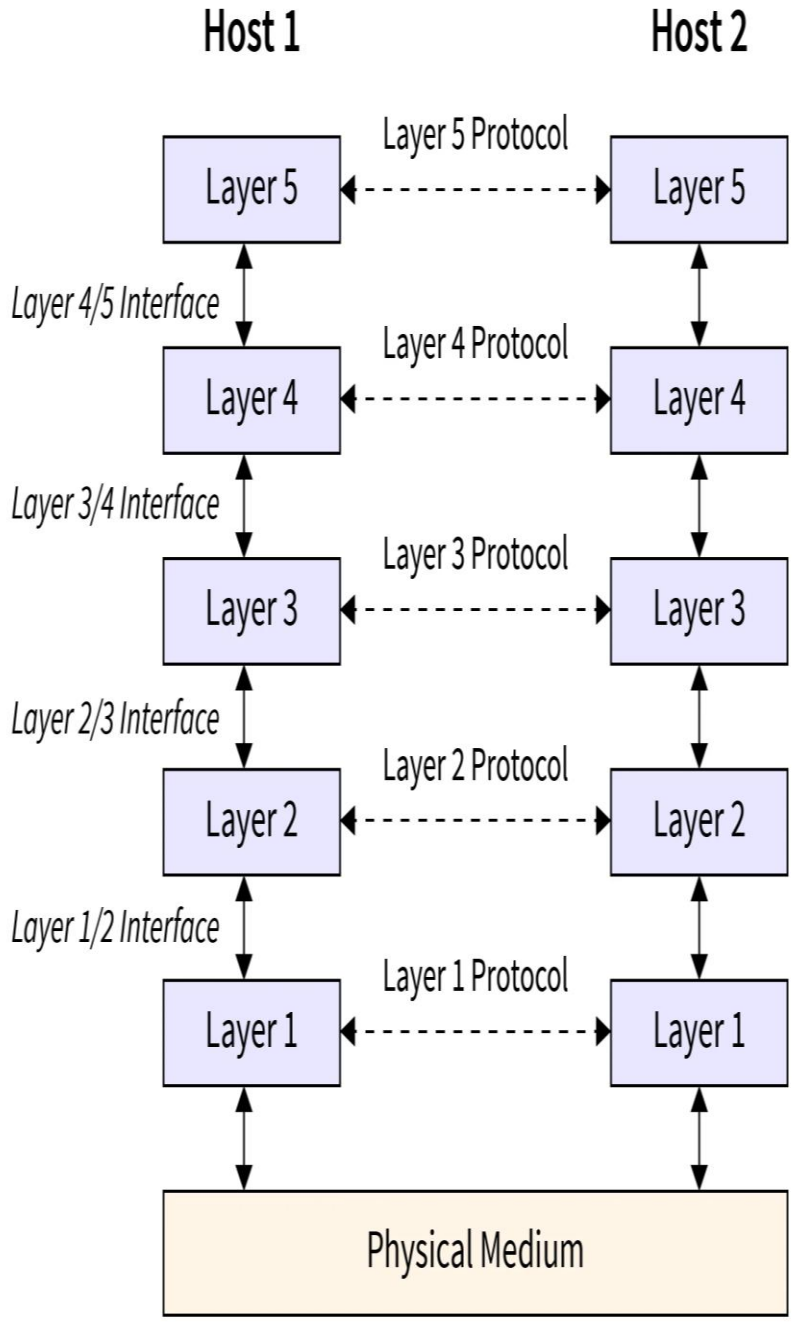
> Basically, a **protocol is a set of rules and agreement** between the communicating parties on how communication is to proceed.

> The **entities comprising the corresponding layers** on different machines are called **peers.**

> Between each pair of **adjacent layers is an interface.** The interface defines which primitive operations and services the lower layer makes available to the upper one.

> A **set of layers and protocols** is called a **network architecture**

>**TCP/IP model and OSI reference model** are examples of protocol hierarchies



DESIGN ISSUES

> When one layer is exchanging its information with another layer there may be **chance of error** such as **change of original message, broken link, or low data rate,** etc. to occur. Therefore, most of the design issues are known and **resolved by this technology**. Let's look at some design issues.

> **Error detection:** Between transmission of the message there may be a chance that the **message will get corrupted**. Therefore, to detect errors in the received information, an error detection technique is used.

> **Error correction:** Error detection techniques only detect errors, but Error correction techniques are used to **correct corrupted information**.

> **Routing:** There are several paths available between the sender and the receiver. Suppose User-A wants to send a message to User-B. And there are multiple paths available between User-A and User-B. If User-A sends his message through **one path which is broken, then User-A can send the same message through another path. This is called routing.**

>**Addressing:** This technique is used to **uniquely identify devices** on the network.

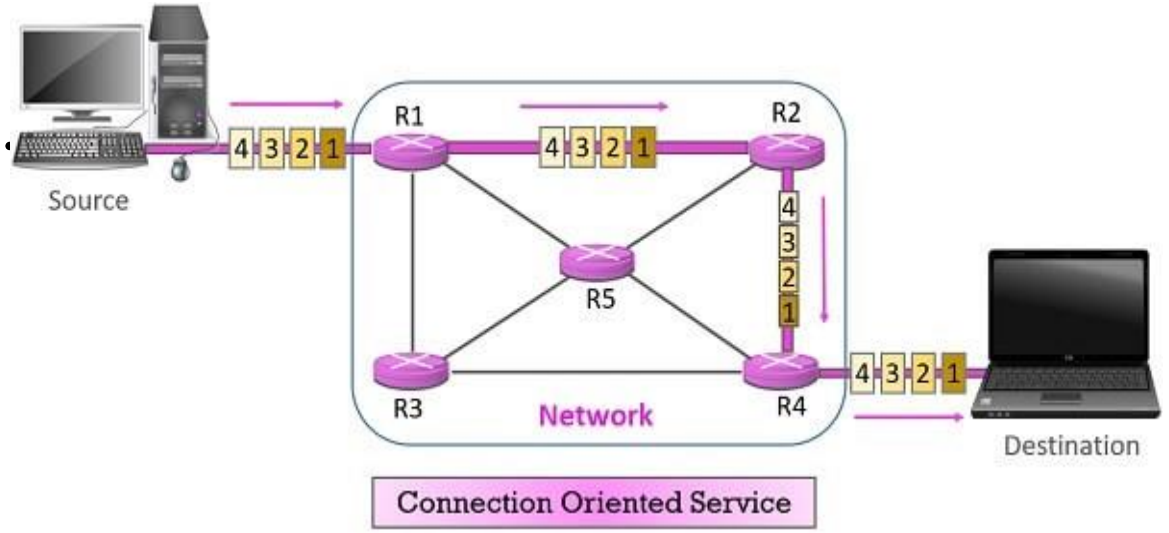
CONNECTION-ORIENTED AND CONNECTIONLESS SERVICES

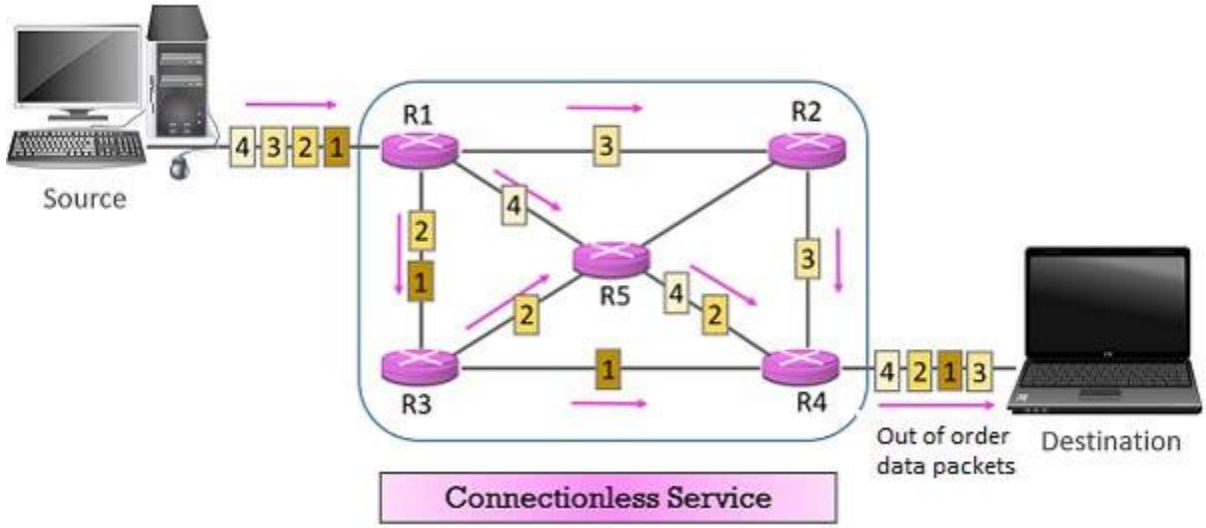
> Layers of network software use connection-oriented &connectionless services for communication.

> **Connection-oriented:** the connection between communication devices is established before the communication takes place Connection-Oriented services are designed on basis of the **Telephone System.**

> **Connectionless:** Connectionless service **does not require a pre-established connection** between communication devices. So, it ensures **unreliable transfer.**

> Connectionless service is modeled **after the postal system.** The source divides message into small acceptable packets known as a **datagram.**





SERVICE PRIMITIVES & RELATIONSHIP

Primitive	Meaning
LISTEN	Block waiting for an incoming connection
CONNECT	Establish a connection with a waiting peer
ACCEPT	Accept an incoming connection from a peer
RECEIVE	Block waiting for an incoming message
SEND	Send a message to the peer
DISCONNECT	Terminate a connection

Figure 1-17. Six service primitives that provide a simple connection-orient service.

> **Service primitives:** Service comprises a set of primitives and here **primitive means operation.** The primitives or operations are available to the user's processes to access the service.

> These primitives generally tell the service to **perform some action on the action taken by the user entity.** Here the purpose of the service is to define the special operations which are to be performed at a particular layer.

> **Relationship of Services to Protocols**: As we have seen in Service Primitives, the service defines the operations for the layers, but it says nothing about how these operations are performed to the layers.

> Whereas a protocol is a set of rules, so the **entities use the protocol to implement the service definitions.**

OSI REFERENCE MODEL

> The **OSI (Open Systems Interconnection**) model is a **conceptual framework** for **understanding** and **standardizing** how different networking protocols and technologies communicate with each other in a network.

> Developed by the **ISO (International Organization for Standardization**) in **1984,** it breaks down the complex process of network communication into **seven distinct layers,** with each layer serving a specific function.

>**Application Layer:** The main functionality of AL is to provide the **user interface.**

> **Presentation Layer: Translate** the sender's data into a computer-readable format & send it to the receiver by performing **encryption and compression** on the data.

> **Session Layer:** Basically, it provides **services to the presentation layer** to **manage** data exchange and dialog control.

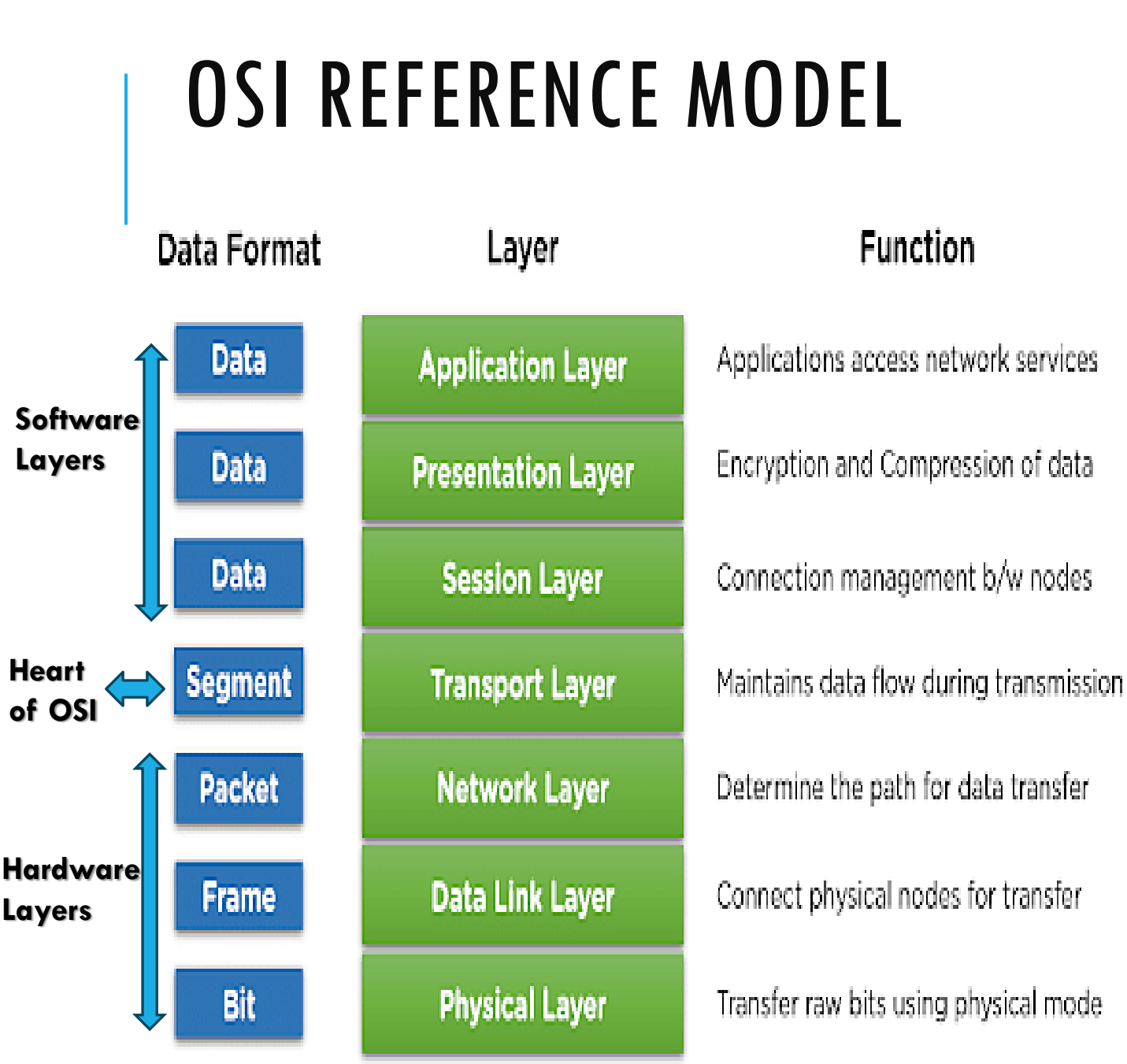
> **Transport Layer:** It is responsible for the **process-to-process delivery.**

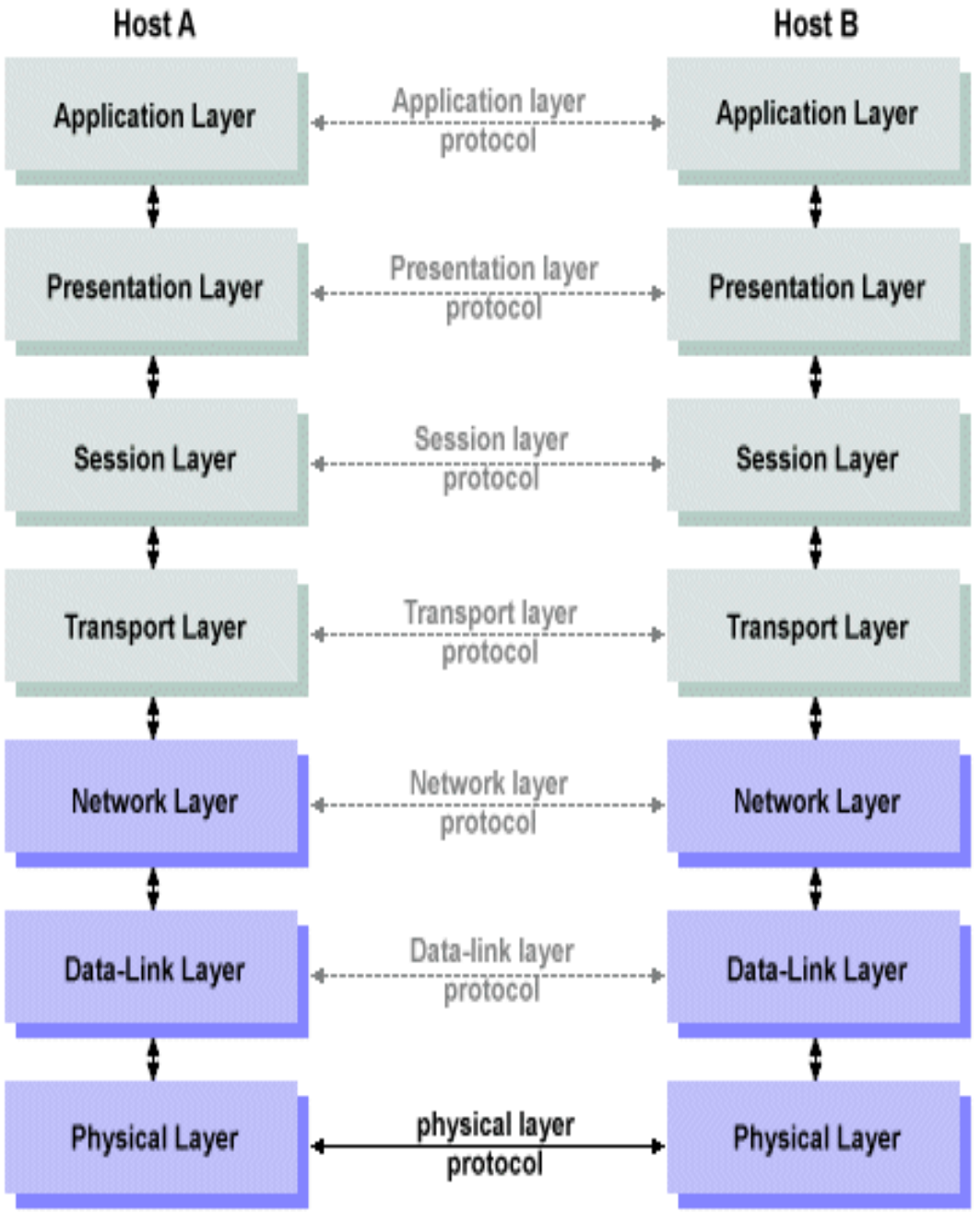
> **Network Layer:** It is responsible **for host-to-host delivery.**

> **Data Link Layer:** It **converts packets** received from the network layer **into frames** and **sends** them to the physical layer.

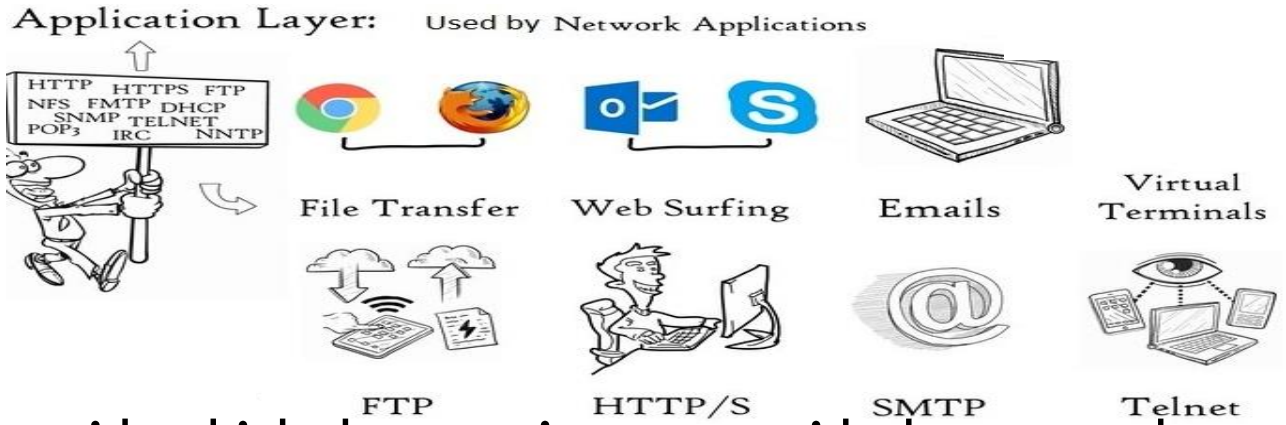
> **Physical Layer:** It **converts the frames** received from DLL **into bits** and sends them to the receiver physical layer through **media**.

OSI REFERENCE MODEL





APPLICATION LAYER



> The application layer provides **the user interface** with which the user interacts with the network and accesses the services or resources he wants to access.

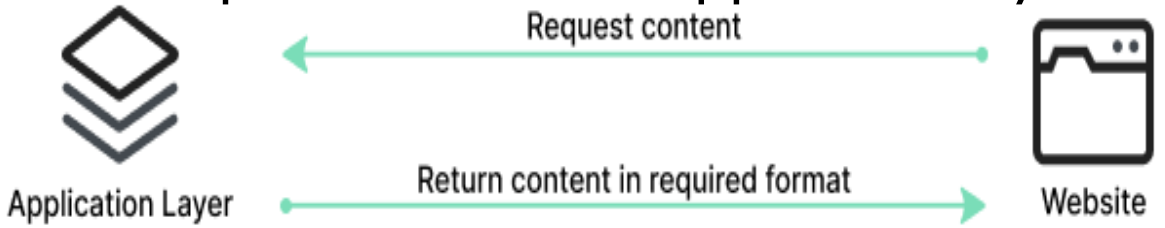
> It consists of protocols that focus on process-to-process communication across an **IP network** and provides a firm communication interface and end-user services.

> Some services provided by this layer includes: **E-Mail, transferring files, distributing the results to user, directory services, network resources, etc.**

> Remote access, email services, shared databases, NVT (Network Virtual Transmission), DNS (Domain Name System) are services of the application layer.

> **SSH, TELNET, HTTP/HTTPS, POP, IMAP, SMTP, FTP, etc.** are protocols used in application layer.

> **Example:** When you browse a **website using HTTP/HTTPS, or send an email using SMTP,** you're interacting with the Application Layer.



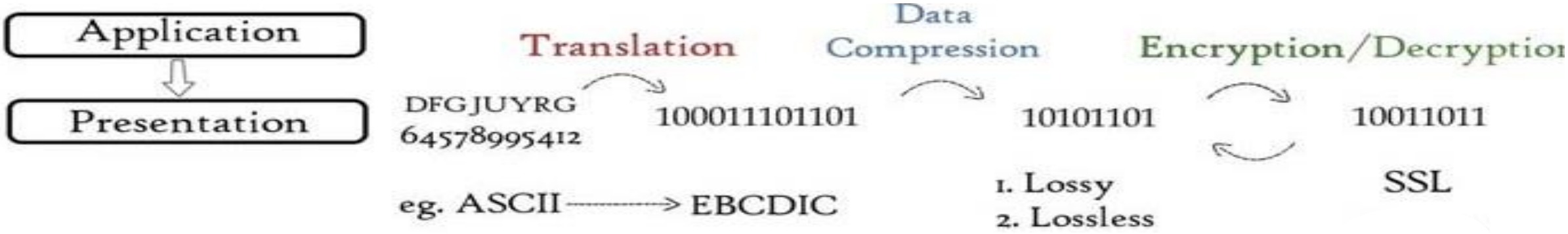
PRESENTATION LAYER

> **Data translation, data encryption, and data compression** are the responsibilities of the presentation layer. It also takes care of the syntax and semantics of the data exchanged between the two devices.

> **Translation**: Using translation, the message is **translated from human-readable format to computer-readable format.** In short, the **data is converted into a stream of bits** because the computer understands the only binary language.

> **Encryption**: Once the data translation is complete, the **data will be encrypted** to protect it from unauthorized access.

> **Data Compression**: After the data encryption is completed, the **data compression algorithm** will be used to compress the data. Because compressed data is transmitted faster than the original data.



SESSION LAYER

>The Session Layer **establishes, maintains,** and **terminates** connections, ensuring that data exchanges occur efficiently and in an organized manner.

> A session is a continuous **exchange of information** between two applications and can involve **multiple data transfers.**

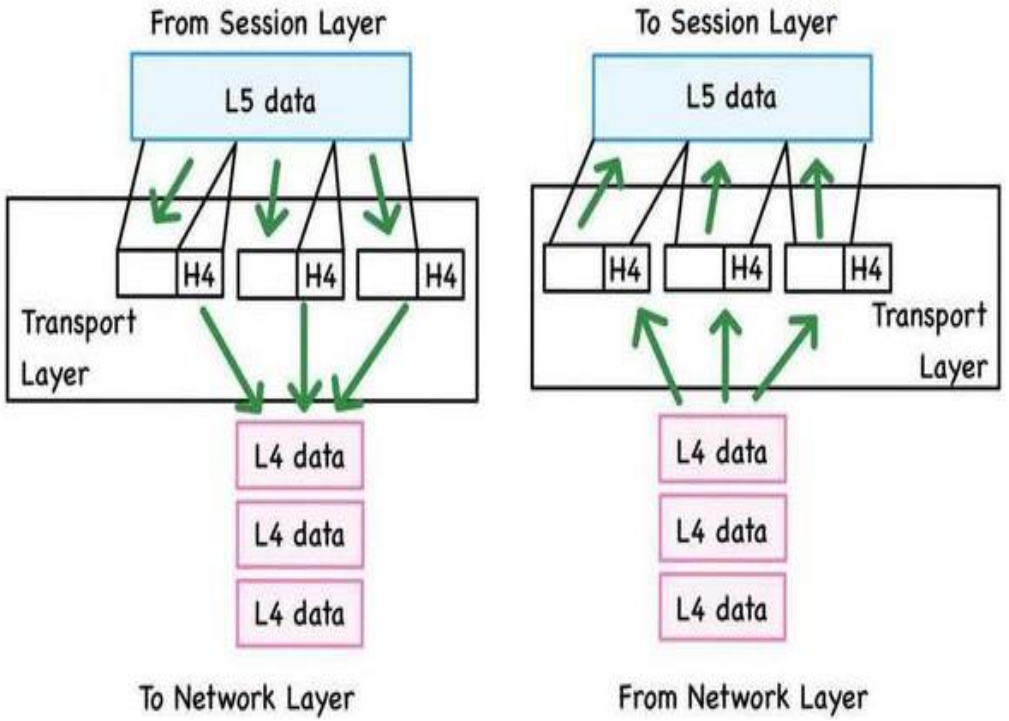
> The session layer ensures that the **session stays open long enough** to transfer all the data being exchanged, and then promptly closes the session in order to **avoid wasting resources.**

> An essential concept in this layer is **synchronization,** in which **checkpoints** during the session ensure a coordinated data flow that is free of unplanned breaks or data loss.

> Another concept is Dialog Controller: The session layer allows two systems to **start communication** with each other in **half-duplex or full duplex.**

>Common Session Layer Protocols : **Remote procedure call protocol (RPC), Point-to-Point Tunneling Protocol (PPTP), Session Control Protocol (SCP), Session Description Protocol (SDP)**

TRANSPORT LAYER



> It is responsible for the **end-to-end delivery** of the complete message. The transport layer also provides the **acknowledgment** of the successful data transmission and **re-transmits the data if an error is found.**

>**Service-point Addressing:** The transport layer adds **header that contains the address** known as **service-point address or port address.**

> **Segmentation:** This includes taking data from the session layer and **breaking it up into chunks called segments** before sending it to layer 3. The transport layer on the receiving device is responsible for **reassembling the segments** into data the session layer can consume.

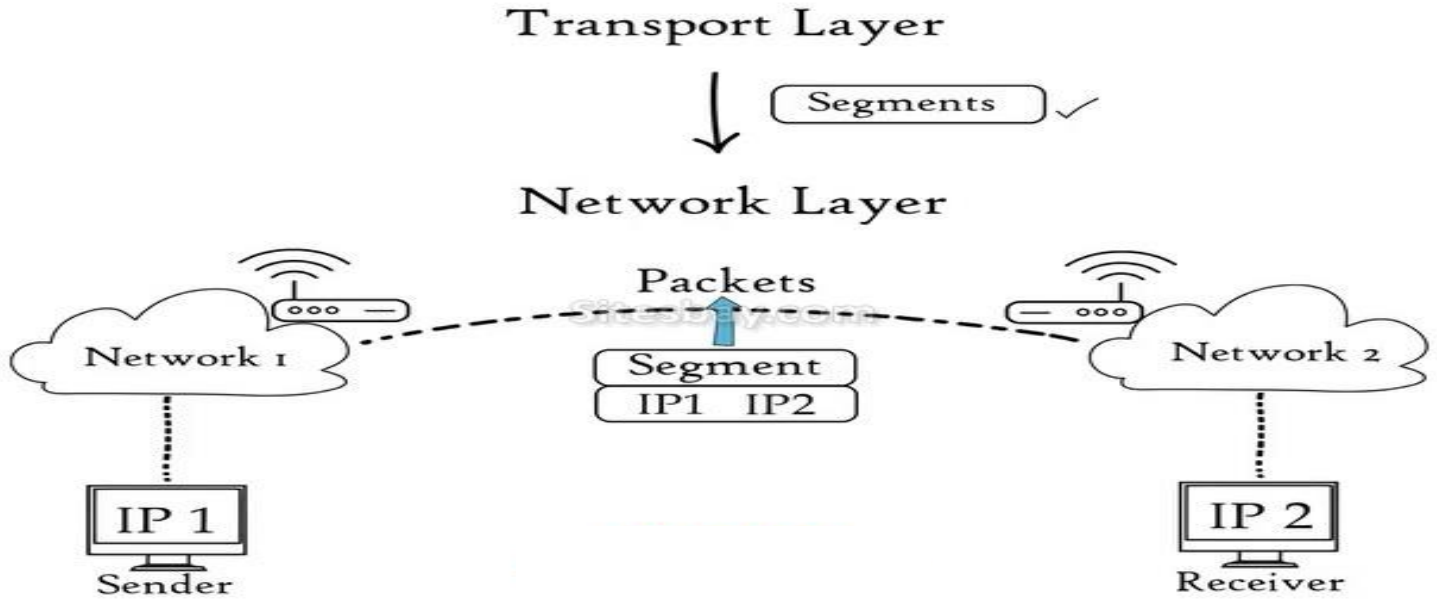
>**Connection Control:** Transport layer provides **two services Connection-oriented service and connectionless service.**

> **Flow control:** The transport layer also responsible for **flow control** but it is performed **end-to-end** rather than across a single link.

> **Error control:** The sender transport layer ensures that **message reach at the destination without any error.**

> Protocols at this layer include **Transmission Control Protocol (TCP) and User Datagram Protocol (UDP).**

NETWORK LAYER



> The network layer is responsible for **facilitating data transfer between two different networks.** If two devices communicating are on same network, then network layer is unnecessary.

> The network layer **breaks up segments from the transport layer into smaller units, called packets,** on the sender's device, and **reassembling these packets on the receiving device.**

> **Internetworking**: It provides a **logical connection between different devices.**

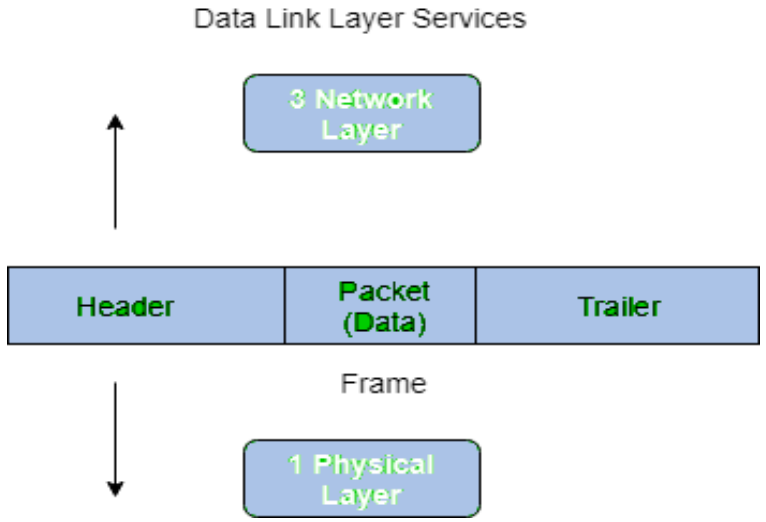
> **Addressing**: A Network layer **adds the source and destination address** to the header of the frame. Addressing is used to **identify the device** on the internet.

> **Routing**: It **determines the best optimal path** out of multiple paths from source to the destination.

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

> Key protocols include **Internet Protocol (IP)**, **Internet Control Message Protocol (ICMP)** for diagnostic and error-reporting purposes, and **Routing Information Protocol (RIP)** manage routing of data across networks.

DATALINK LAYER



>It **defines the format** of the data on the network.

>The data link layer is responsible for the **node-to-node delivery** of the message.

> The main function of this layer is to make sure **data transfer** is **error-free from one node to another,** over the physical layer.

> When a packet arrives in a network, it is the responsibility of the DLL to transmit it to the Host using its **MAC address.**

>Packet in the Data Link layer is referred to as **Frame.**

>**Switches and Bridges** are common Data Link Layer devices.

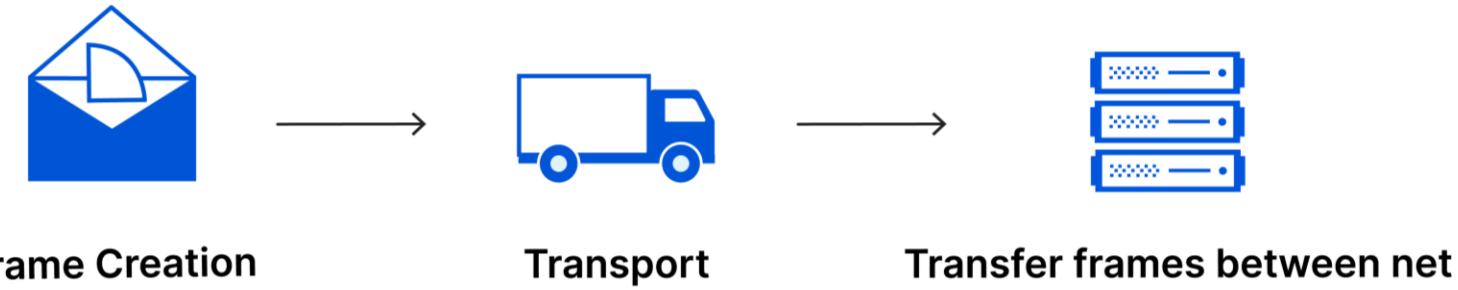
> It contains two sub-layers:

1. **Logical Link Control Layer**
   > It is responsible for **transferring the packets** to the Network layer of the receiver that is receiving.
   > It **identifies the address** of the network layer protocol from the header.
   > It also **provides flow control.**
2. **Media Access Control Layer**

> A Media access control layer is a **link between the Logical Link Control layer and the network's physical layer.**

> It is used for **transferring the packets** over the network.

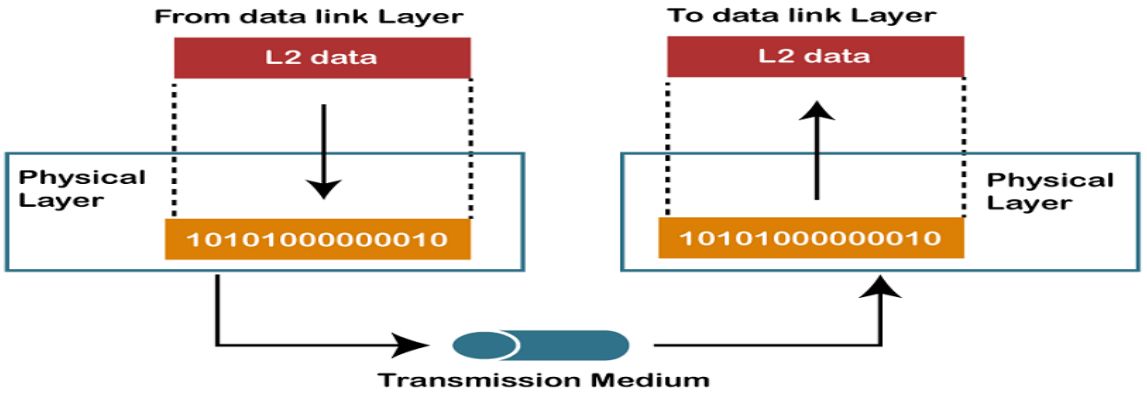
DATALINK LAYER



>Functions of the Data Link Layer

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

PHYSICAL LAYER



> The **data units** on this layer are called **bits.**

>This layer defines the **mechanical and electrical definition** of **the network medium (cable) and network hardware.**

> This includes how **data is impressed onto the cable and retrieved from it.**

> The physical layer is responsible for **passing bits onto and receiving them** from the connecting medium.

> This layer gives the data-link layer (layer 2) its ability to transport a stream of serial data bits between two communicating systems; it **conveys the bits that moves along the cable.**

>The main network device found the Physical layer is a **repeater.**

> On this layer, **the raw bits are transmitted physically over copper cables, fiber optics, and wireless signals.**

> Example: The **Ethernet cable** that connects your device to the internet or the fiber optic cables used by ISPs operate at the physical layer.

TCP/IP PROTOCOL

> The TCP/IP protocol model is the **foundation of the internet.**

> **"TCP"** stands for **Transmission Control Protocol,** while **"IP"** stands for **Internet Protocol.** Together, they form a standardized way for different devices to connect and share information over a network.

>It provides a **framework for communication over the internet,** allowing computers to send and receive information from each other regardless of geographical location.

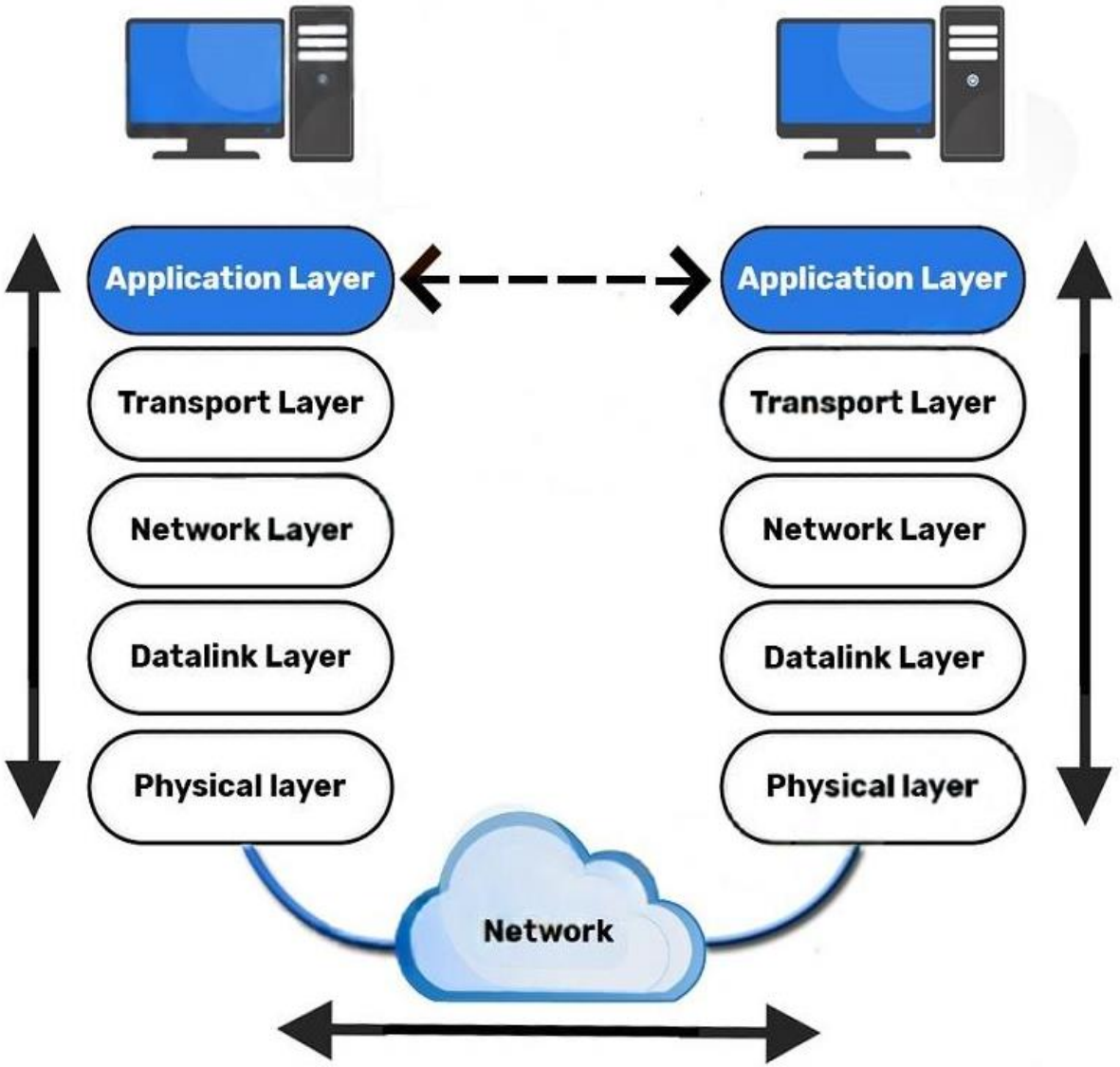
> Example: Imagine sending a package. **TCP makes sure your package is complete and undamaged, while IP finds the correct address and sends it to the right place.**

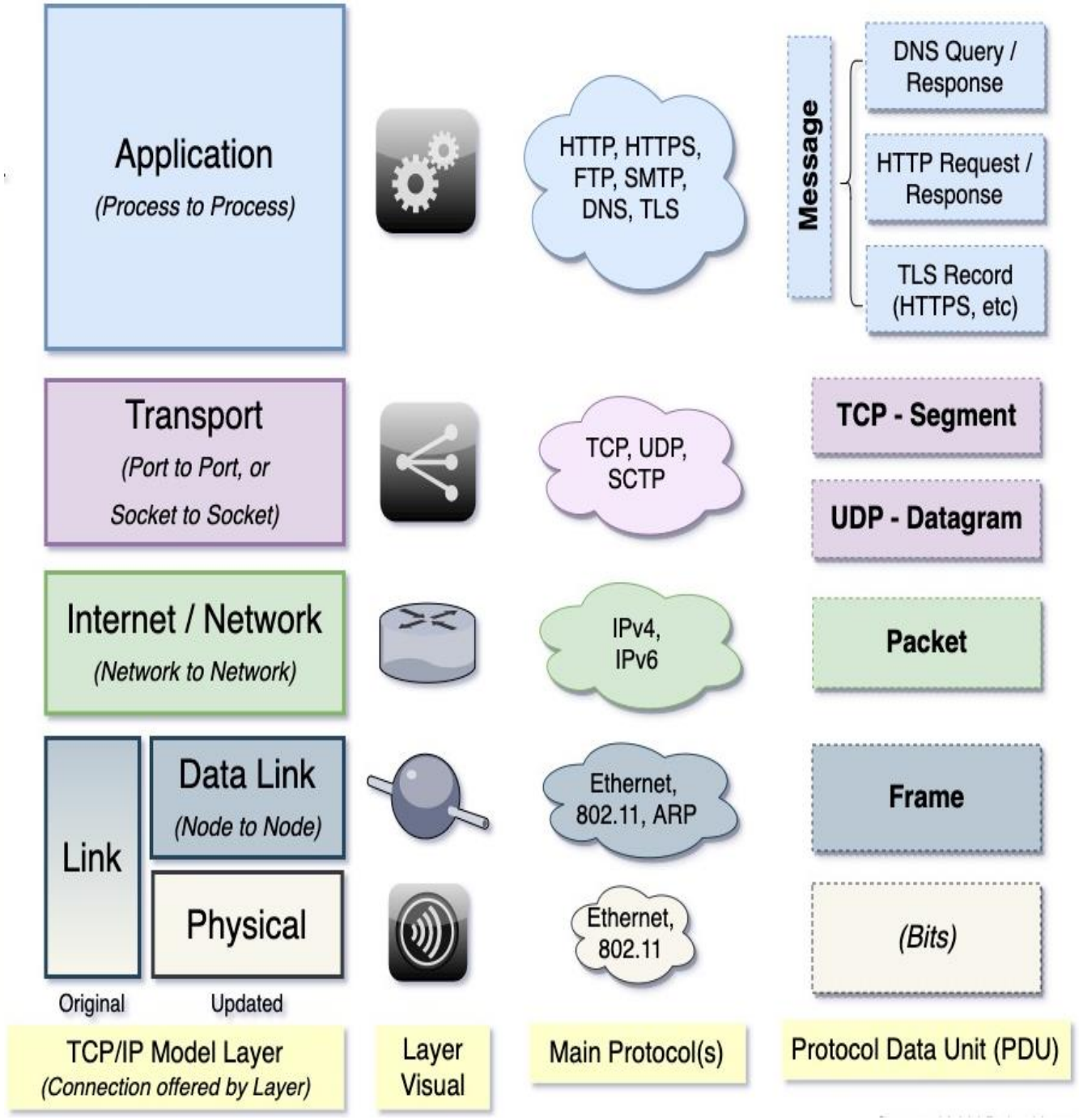
>Each layer has its **own set of protocols** that allow for data transmission and packet switching between different nodes on a network.

> There are **Five Layers** in TCP/IP Protocol Model:

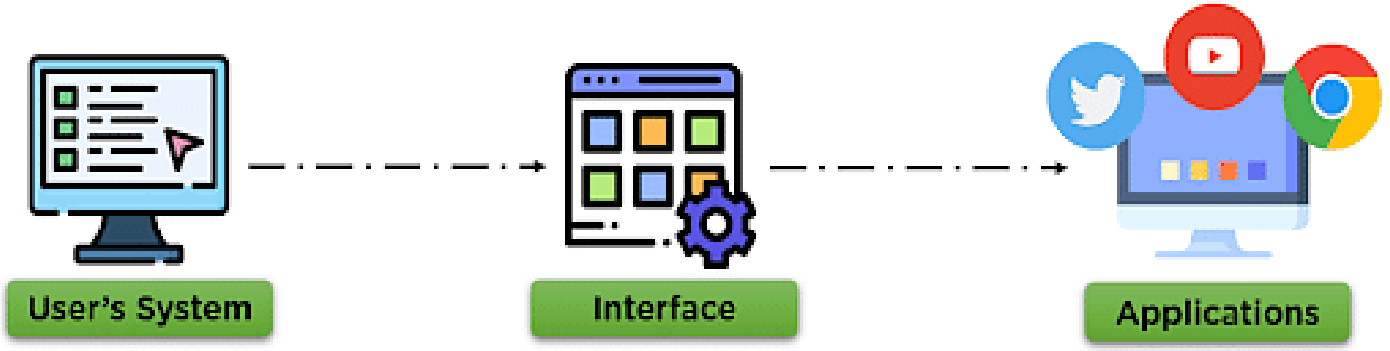
1. Application Layer
2. Transport Layer
3. Network Layer
4. Data Link Layer
5. Physical Layer

TCP/IP PROTOCOL





APPLICATION LAYER



> The Application layer **directly interacts with end-user software.**

> This is the **topmost layer** which indicates the **applications** and **programs** that utilize the TCP/IP model for communicating with the user through applications and various tasks performed by the layer, including **data representation for the applications executed by the user and forwards it to the transport layer.**

> The application layer maintains a **smooth connection between the application and user** for data exchange and offers various features as **remote handling of the system, e-mail services,** etc.

> Some of the protocols used in this layer are:

- HTTP: Hypertext transfer protocol is used for accessing the information available on the internet.
- SMTP: Simple mail transfer protocol, assigned the task of handling e-mail-related steps and issues.
- FTP: This is the standard protocol that oversees the transfer of files over the network channel.

> It's where **network applications** can access network services.

TRANSPORT LAYER

> Here's where **TCP comes into play**. This layer ensures that the **data is transmitted reliably.**

> **It breaks the data into packets** and makes sure they get to their destination in the **correct order.**

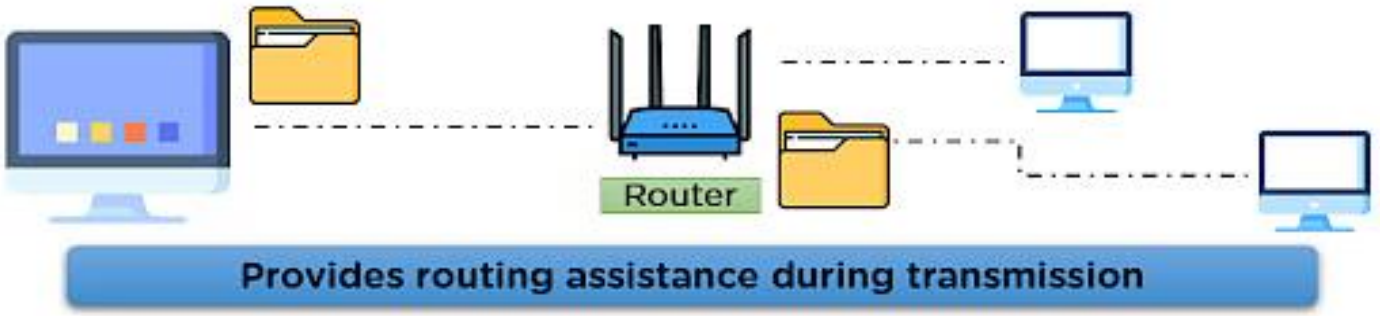
> TCP handles communications between hosts and provides **flow control, multiplexing and reliability.** The transport protocols include TCP and User Datagram Protocol (UDP), which is sometimes used instead of TCP for special purposes.

> This layer is responsible for **establishing the connection between sender and receiver** device.

>The protocols used in this layer are:

- **TCP**: Transmission Control Protocol is responsible for the proper transmission of segments over the communication channel. It also establishes a network connection between the source and destination system.
- **UDP**: User Datagram Protocol is responsible for identifying errors, and other tasks during the transmission of information. UDP maintains various fields for data transmission such as:
- **Source Port Address**: This port is responsible for designing the application that makes up the message to be transmitted.
- **Destination Port Address**: This port receives the message sent from the sender side.
- **Total Length**: The total number of bytes of the user datagram.
- **Checksum:** Used for error detection of the message at the destination side.

NETWORK LAYER



> This is where **IP does its job**. It **routes the data packets** across the network, making sure they get to **the right address.**

> The network layer deals with how **to combine multiple links into networks,** and networks of networks, into internetworks so that we can send packets between distant computers. This includes the task of **finding the path along which to send the packets.**

> The **internet layer, also called the network layer,** deals with packets and connects independent networks to transport the packets across network boundaries.

>This layer performs many important functions in the TCP/IP model, some of which are:

1. It is responsible for **specifying the path** that the data packets will use for transmission.
2. **providing <u>IP addresses</u>** to system for identification matters over network channel.

> Some of the protocols applied in this layer are:

- IP: This protocol assigns your device with a **unique address;** the IP address is also responsible for routing the data over the communication channel.
- ARP: This protocol refers to the **Address Resolution Protocol** that is responsible for finding the physical address using the IP address.

DATA LINK LAYER

> The **network link layer, also known as the network interface layer** or data link layer, consists of protocols that operate only on a link -- the network component that interconnects nodes or hosts in the network.

> The protocols include **Ethernet for local area networks and Address Resolution Protocol.**

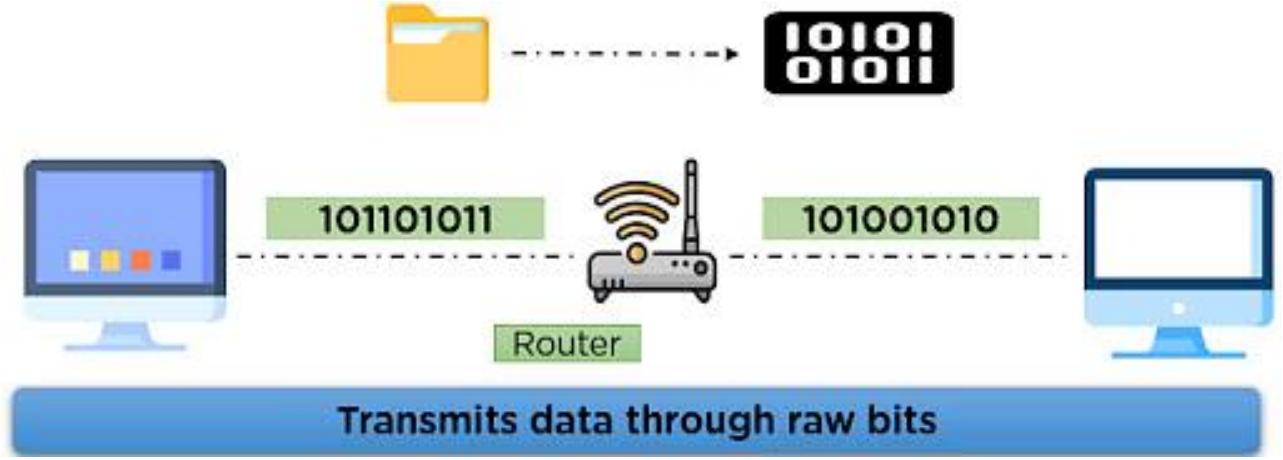
> The datalink layer defines **how data should be sent,** handles the physical act of sending and receiving data, and is responsible for transmitting data between applications or devices on a network.

> This includes defining how data should be signaled by hardware and other transmission devices on a network, such as a computer's device driver, an **Ethernet cable, a network interface card (NIC), or a wireless network.**

>Here are the most commonly used data link layer protocols:

- **PPP (Point-to-Point Protocol)** enables communication between two points. It's used for internet connections over dial-up modems or DSL.
- **Wi-Fi** is a wireless version of Ethernet that connects devices without cables within a local area network.

PHYSICAL LAYER



> The lowest layer, this is responsible for the **physical transmission of data**. It's how **data moves over cables, fiber optics, or wireless signals.**

>This includes the **cables, connectors, and other hardware** used in networking. In addition, some standard protocols like **Ethernet and Wi-Fi** are also part of this layer.

> The Physical layer **ensures that data packets are correctly** transmitted over a physical medium, such as a cable. It also handles data transmission **synchronization**, ensuring that packets are sent and received in the correct order.

> Without the Physical layer, it would **be impossible for two systems to communicate with each other** since there would be no way for them to transmit data between them physically.

> The Physical layer is an **essential part of the TCP/IP model** and is critical for successful communication.