SYLLABUS:

UNIT – I INTRODUCTION OF COMPUTER NETWORKS

1. **Network Hardware:**
   - **1.1.** Personal Area Networks
   - **1.2.** Local Area Networks
   - **1.3.** Metropolitan Area Networks
   - **1.4.** Wide Area Networks
   - **1.5.** Internetworks

2. **Network Software:**
   - **2.1.** Protocol Hierarchies
   - **2.2.** Design issues for the Layers
   - **2.3.** Connection-Oriented v/s Connectionless Services
   - **2.4.** Service Primitives

3. **Reference Models:**
   - **3.1.** Open System Interconnections (OSI)
   - **3.2.** Transmission Control Protocol / Internet Protocol
   - **3.3.** Comparison of OSI and TCP/IP.

4. **Example Networks**:
   - **4.1.** ARPANET
   - **4.2.** Internet.

5. **Physical Layer:**
   - **5.1.** Guided Transmission media
     - 5.1.1.Twisted Pairs.
     - 5.1.2.Coaxial Cable.
     - 5.1.3.Fiber Optics.
     - 5.1.4.Wireless transmission.
   - **5.2.** Wireless Networks – Packet Radio Network

6. **Wireless LAN:**
   - **6.1.** IEEE 802.11b,
   - **6.2.** Wireless Application Protocols (WAP) & WML and
   - **6.3.** Virtual Private Network
   - **6.4.** VPN
   - **6.5.** Technology.

1. NETWORK HARDWARE:

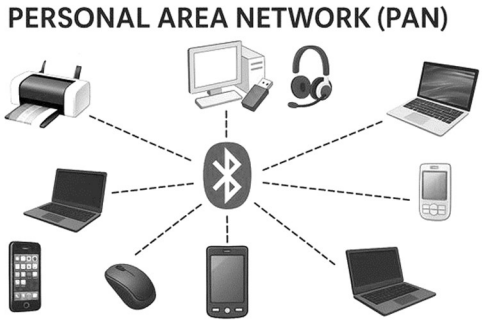
Computer Network is the interconnection between multiple devices. Computer Network allows to send and receive data and information between different connected devices. Different devices in a network are connected through links.

- There are two types of transmission technology that are in widespread use: broadcast links and point-to-point links.
- Point-to-point links connect individual pairs of machines.
- To go from the source to the destination on a network made up of point-to-point links, short messages, called packets in certain contexts, may have to first visit one or more intermediate machines.
- Often multiple routes, of different lengths, are possible, so finding good ones is important in point-to-point networks. Point-to-point transmission with exactly one sender and exactly one receiver is sometimes called unicasting.
- Broadcast systems usually also allow the possibility of addressing a packet to all destinations by using a special code in the address field. When a packet with this code is transmitted, it is received and processed by every machine on the network. This mode of operation is called broadcasting.
-
- Some broadcast systems also support transmission to a subset of the machines, which known as multicasting.
- Data flow is the way in which the data is communicated between nodes. The ways of data flow is
  - **Simplex**: Data flows only in one direction. Ex: Satellite – Television, TV Remote – TV.
  - **Half Duplex**: Data flows in both directions but not at the same time. Ex: Walkie-Talkie
  - **Duplex/Full Duplex**: Data flows in both the direction. Data can flow in both directions at same time. Ex: Mobile communication.
- Networks basically are categorized as (also mentioned is the range)
  1) Personal Area Network(PAN)
  2) Local Area Network(LAN)
  3) Metropolitan Area Network(MAN)
  4) Wide Area Network(WAN)
  5) Internetworking

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

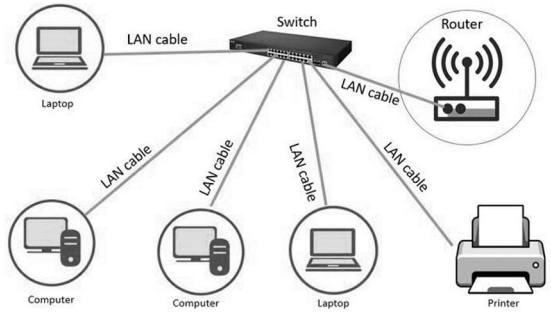
1.1. Personal Area Networks (PAN):

- Connects electronic devices of the user within a small range of few centimeters to few meters
- PAN keeps the data more private
- One of the most common example of PAN is the Bluetooth connection between a mobile and the sound speaker
- PAN can either a wired or wireless connected
- Example for wired connection is USB connected laptop with mobile
- Wireless connection includes Bluetooth, wi-fi, zigbee etc.,
- Data Transfer speed is very low



1.2. Local Area Network (LAN):

- LAN is a group of connected devices in very small area viz. school, office, home
- It ranges over 10m to few 100s of meters
- Real world example is a computer connected to keyboard, mouse and printer at home/office/campus
- Data Transfer speed is up to 10Mbps.
- LANs are of 2 types. Wired LAN and Wireless LAN
- Wired LAN is one where the devices are connected through a cable. Ex: computer Laboratory
- Wireless LAN is one where the devices are connected without cable. Ex: Laptop/Mobile connected to a sound-bar at home



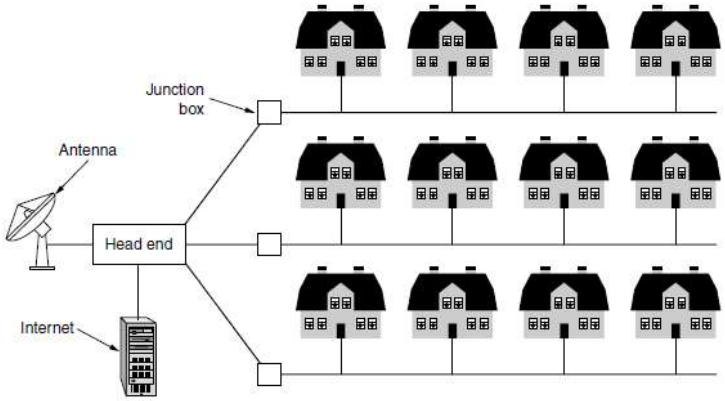
Local Area Network

1.3. Metropolitan Area Network (MAN):

- A **MAN** (**Metropolitan Area Network**) covers a city.
- The best-known examples of MANs are the cable television networks available in many cities
- MAN is network that connects the devices across a city
- MAN stands between LAN and WAN
- MAN is used to connect multiple LAN networks, in doing so the network become wide enough to be called as Metropolitan Area Network
- MAN covers a distance of over 10kms

1.4. Wide Area Network (WAN):

- Wide Area Network is computer network that covers a larger geographical area. viz, country, continent
- WAN stands above LAN and MAN
- WAN is a network that connect an office at Delhi with an office at Cochin
- Slower but expensive than LANs



Comparision:

Criteria	MAN	LAN	WAN	PAN
Definition	A network that covers a city or large campus.	A network within a limited area like a home, school, or office.	A network that spans large geographical areas, connecting multiple LANs.	A very small network around an individual. typically, within a few meters.
Coverage Area	Medium (up to 50 km)	Small (up to a few kilometers)	Very large (country or worldwide)	Very small (up to 10 meters)
Ownership	Often owned by cities or large organizations	Typically owned by a single organization	Public or private (e.g., ISPs)	Individual-owned
Speed	Moderate to high	High (up to 10 Gbps or more)	Lower than LAN (due to distance and complexity)	Varies, usually low (Bluetooth, etc.)
Example	City-wide Wi-Fi or cable TV network	Office network, school network	The internet, company networks across cities	Bluetooth connection, smartphone to smartwatch
Technology Used	Fiber optics, wireless, microwave links	Ethernet, Wi-Fi	Fiber optics, satellite, MPLS, VPN	Bluetooth, USB, Infrared
Usage	Connecting government offices, universities	File sharing, printers, internal communication	Global communication, business networks	Syncing personal devices

2. NETWORK SOFTWARE:

2.1. Protocols:

- A set of rules and standards that define how data is transmitted, received, and interpreted between devices on a network.
- Protocols ensure that different devices, possibly made by different manufacturers, can communicate with each other effectively and understand the exchanged data.
- Protocols define
    - How the communication is established and terminated?
    - What is the data format?
    - Error handling
    - Data flow control
- Examples:
    - HTTP – Hyper Text Transfer Protocol
    - Wi-Fi – Wireless-fidelity
    - POP – Post Office Protocol
    - SMTP - Simple Mail Transfer Protocol

2.2. Protocol Hierarchy:

- Protocol Hierarchy refers to the way network protocols are organized in layers, where each layer has specific functions and interacts with the layers above and below it
- This layered approach helps in managing complex communication systems by breaking them into smaller, manageable parts.
- This layered approach provides a systematic way to design, implement, and manage network communication, making it easier to understand and maintain complex systems
- Well know example for protocol hierarchy is Open System Interconnects(OSI) model consisting of 7 layers
- Protocol hierarchy allows each layer to focus on a specific part of the communication process.

2.3. Design Issues:

Design issues in computer networks refer to the challenges and decisions that need to be addressed when creating or improving a network to ensure it works efficiently, reliably, and securely.

2.3.1. **Reliability**:

- Minimal Downtime of network
- Network must be dependable
- During transmission if one link fails, the data is to be transmitted through another link.
- Network should have the mechanism like error correction and detection.

2.3.2. **Security**:

- Network should include data encryption to protect from unauthorized access.
- Network should have user authentication

2.3.3. Scalability:

- A network can be scalable(grow) according to the usage. ie., it can add more devices and more users.
- In doing so, the performance of the network should not be downgraded significantly

2.3.4. Quality of Service(QoS):

- Network should have mechanism to prioritize and manage network traffic based on bandwidth, latency and reliability.

2.3.5. Tunneling:

- Designing tunneling protocols to encapsulate packets from one network within another network's packets, enabling communication across heterogeneous networks.

2.3.6. Multicasting and Broadcasting:

- Network should support an efficient data distribution to multiple recipients using multicast and broadcast addressing.

2.3.7. Subnetting:

- Dividing larger networks into smaller subnets to enhance manageability, improve performance, and optimize address utilization.

2.4.

3. REFERENCE MODELS:

With reference to the layers in networking, there are two types of reference models.

1. **OSI** - Open Systems Interconnections
2. **TCP/IP** – Transmission Control Protocol / Internet Protocol

Note:

- Protocols associated with the OSI model are not used anymore, but the ***model is still valid***.
- The model associated with the TCP/IP model is not used anymore, but the ***Protocols are still valid***

Therefore, we need to learn both models.

A 4-layered reference model is shown below for reference

- ✓ Layers are arranged as a stack, where the data flows from a layer to a layer below during transmission, and layer above during receiving the data
  Host 1 be a transmitter and Host 2 be a Transmitter
- ✓ Layer-n on Host1 cannot send data directly to the same layer-n on Host2. The data should pass through the layers below and reach the lowest layer in Host1. The data then passes through the physical media, and finally reach the lowest layer of HOST2. The data then travels through the layers above and finally reaches layer-n of HOST2
- ✓ Each layer connected with each other by in interface
- ✓ Interface between layer n and n+1 is designated as **layer n/(n+1) interface** as refereed in the block diagram
- ✓ Layer n on each network should follow the same protocol.

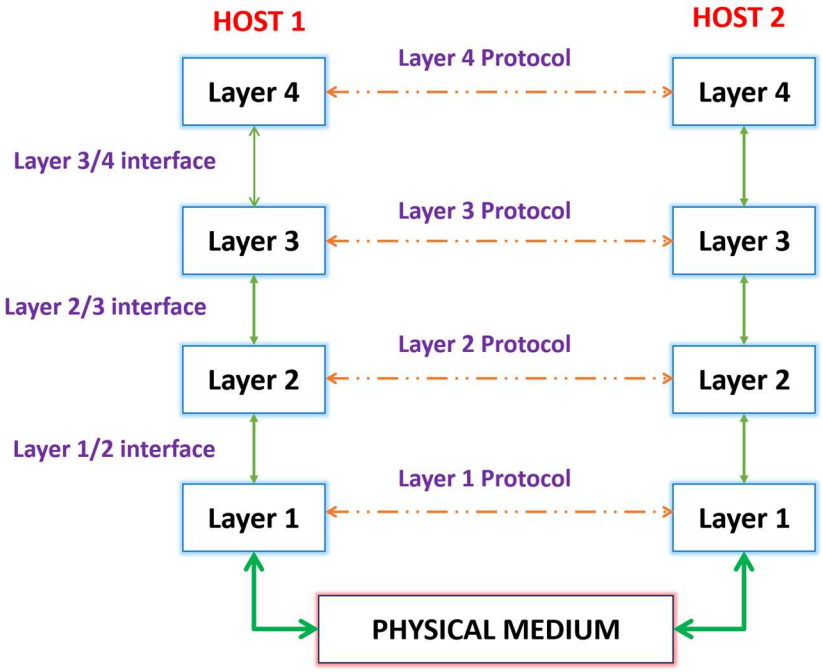
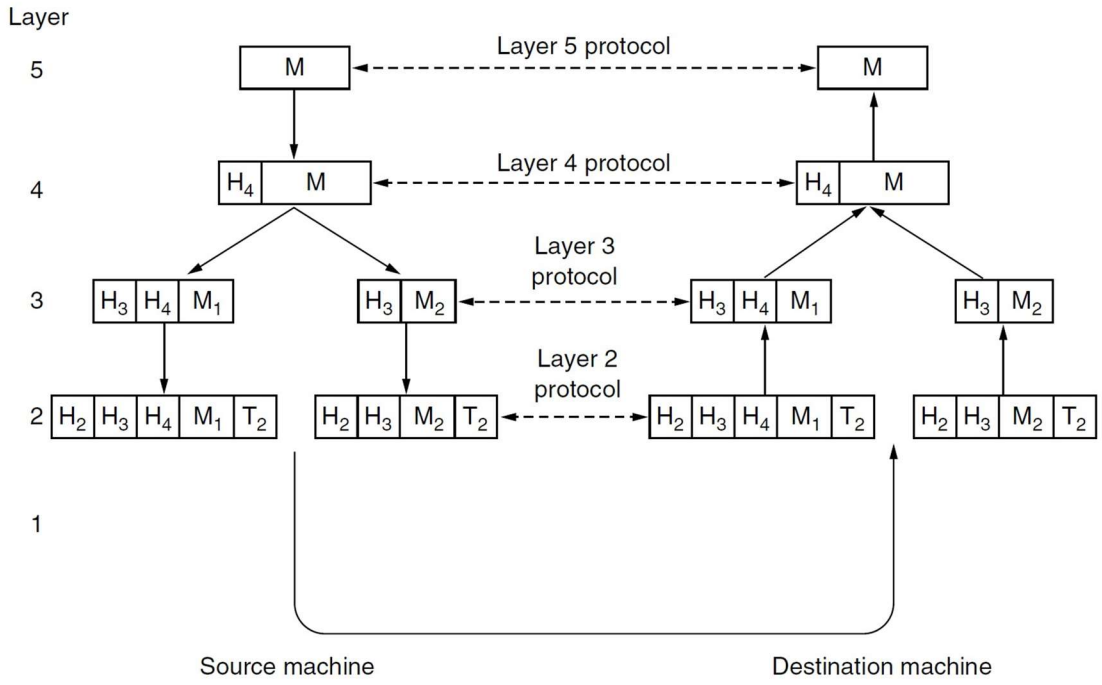


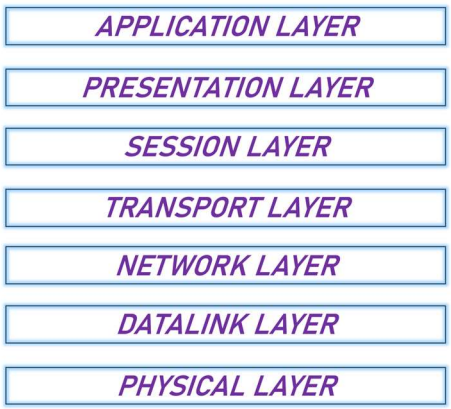
Fig: A 4-Layer Network Model

The figure below explains how the message/data is being transmitted when it passes through different layers. The data transmitted at Layer 5 travels down through the layer below and gets transformed. As the message/data passes through each layer, some layer information is added to the message/data.



3.1. OSI Reference Model

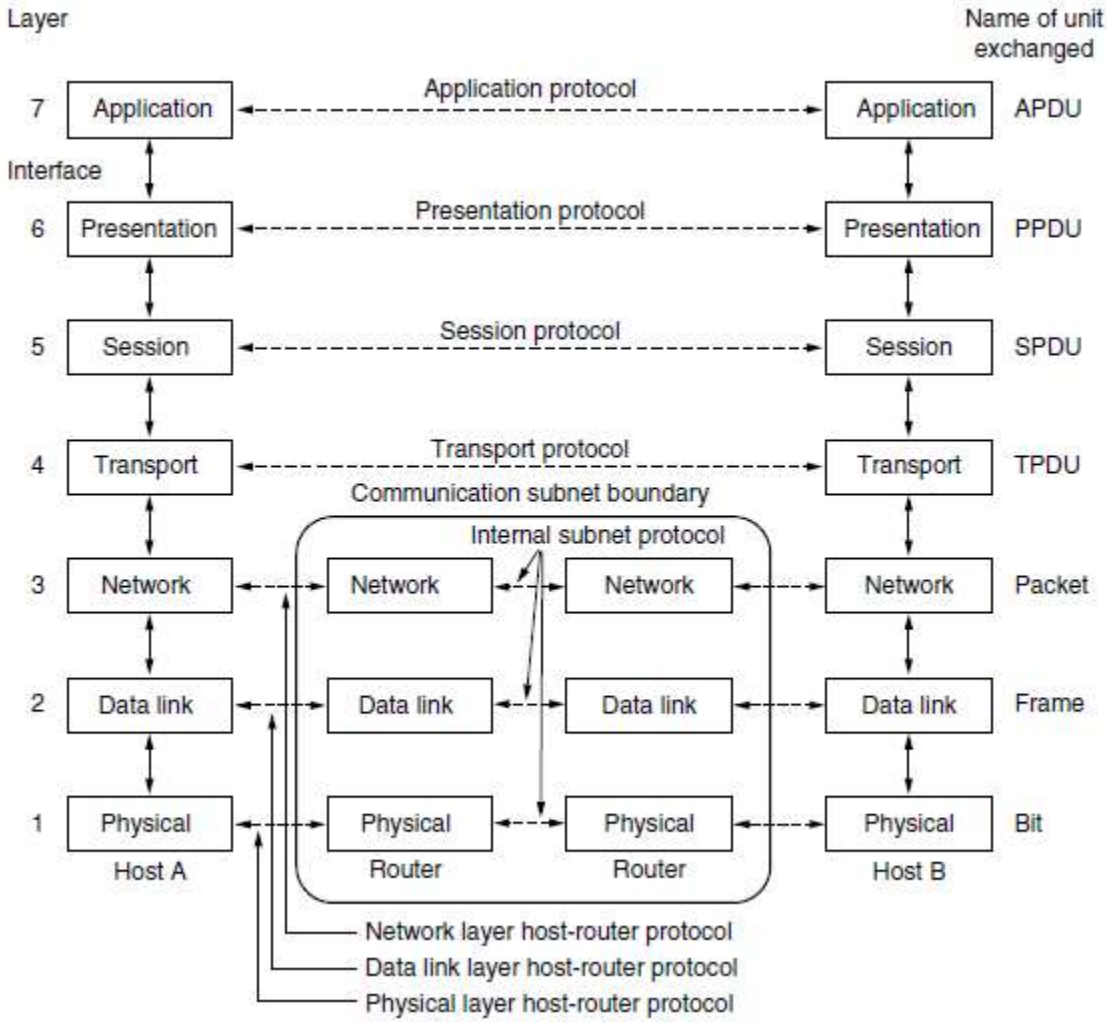
- The model is based on ISO (International Standards Organization)
- This model connects the systems that are open for communication, and hence the name Open Systems Interconnections.
- The OSI model has **7** layers, namely
    1) Application Layer
    2) Presentation Layer
    3) Session Layer
    4) Transport Layer
    5) Network Layer
    6) Datalink Layer
    7) Physical Layer
- At source, the data flows in a top-down approach
- At Destination, the data flows in a bottom-up approach
- Why 7 layers?
    1) Each layer should perform a well-defined function
    2) A layer is created wherever a different abstraction is needed
    3) Each layer is designed according to the international standards
    4) No. of Layers should be large enough such that a large number of functions are not accommodated in the same layer.
    5) Also, the architecture should not be wide
- The OSI layer ordering is shown below.
    1) Application is the top layer and physical layer is the bottom layer
    2) Physical layer is the one which send the data to the physical media



The figure below shows, the data transmitted form one node to the another through a set of intermediate nodes.

At the end nodes the data will pass through all the layers.
But at the intermediate nodes, only network layer, data link layer and the physical layer are active.

The group of intermediate nodes through which the data passes is called as subnets.



3.1.1. Application Layer:

- The Application Layer serves as the interface between the end-user applications and the underlying network services.
- It enables the users to get connected with the network and use its resources
- Services provided by the Application Layer
  - File Transfer
  - Access Management etc.,
- Protocols include
  - HTTP (Hyper Text Transfer Protocol) for World Wide Web
  - DNS (Domain Name System) for domain name
  - SMTP (Simple Mail Transfer Protocol) for emailing
  - Etc.,

Example:

- ✓ WhatsApp Messaging application,
- ✓ Mozilla Firefox for browsing,
- ✓ Internet Explorer for browsing
- ✓ Winamp for audio/video

3.1.2. Presentation Layer:

- This layer is concerned with syntax and semantics of the information exchanged between the devices
- Presentation layer is responsible for translating data between the application layer and the network format.
- Services provided are:
  - data formatting
  - data compressor.
  - data encryption/decryption. i.e, it takes data from application layer, manipulates the data as per the accepted format
  - facilitates the interoperability between different systems
- Protocols include
  - AFP (Apple Filling Protocols)
  - SSL (Secure Socket Layer)
  - Etc.,

3.1.3. Session Layer:

- Session layer allows users on different machines to establish session between them.
- Provides services like
  - Dialog Control – keeps track of whose is turn to transmit
  - Token management – preventing the users to from attempting the same operation
  - Synchronization – use of checkpoint to understand where they left off in case of crash in transmission.
- It establishes, maintains, and terminates connections, ensuring that data exchanges occur efficiently and in an organized manner
- Protocols include
  - RTCP (Real-Time Transport Control Protocol)
  - PPTP (point-to-point tunneling Protocol)
  - PAP (Password Authentication Protocol)

3.1.4. Transport Layer:

- At transmitter side, the transport layer receives data from layer above, performs segmentation.
- Data in this layer is referred as Segments.
- The transport layer is a true end-to-end layer; it carries data all the way from the source to the destination
- The basic function of the transport layer is to accept data from above it, split it up into smaller units if need be, pass these to the network layer, and ensure that the pieces all arrive correctly at the other end
- Transport layer also provides the acknowledgement for a successful transmission and re-transmits the data if errors are found
- Protocols include
  - TCP – Transmission Control Protocol
  - UDP – User Datagram Protocol

3.1.5. Network Layer:

- The data in this layer is referred as Packets
- It takes care of packet routing i.e., selection of shortest path to transmit the data.
- The senders the receives IP addresses are placed in the header by network layer
- Network layer is implemented by network devices like routers and switches.

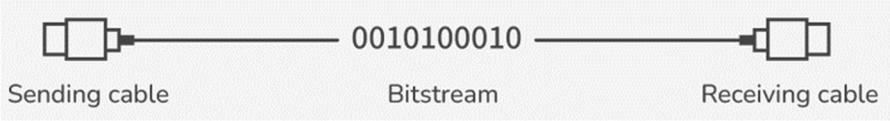
3.1.6. Data Link Layer:

- The Data Link Layer is responsible for node-to-node data transfer
- error detection and correction
- It ensures that data is transmitted to the correct device on a local network segment
- This layer manages MAC (Media Access Control) addresses and is divided into two sublayers: Logical
- Link Control (LLC) and Media Access Control (MAC).

- The packet received from the network layer is further divided into frames depending on the frame size of the Network Interface Card(NIC)
- Protocols include
    - Ethernet –which defines the rules for data transmission over local area networks (LANs),
    - Point-to-Point Protocol (PPP) for direct connections between two network nodes.

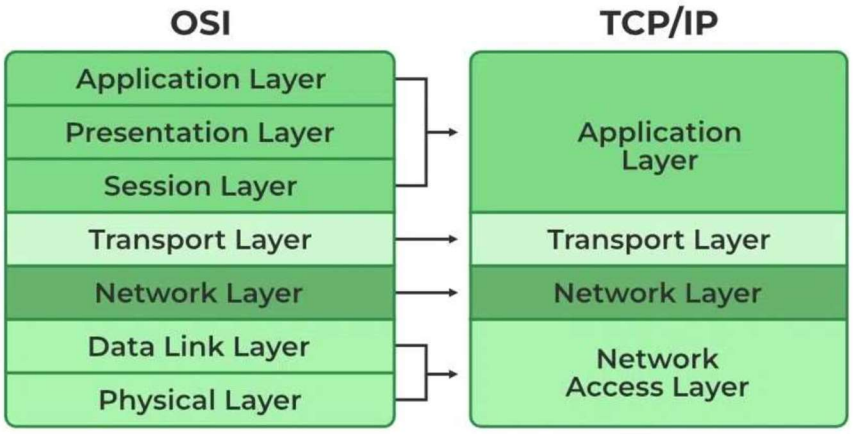
3.1.7. Physical Layer:

- The lowest layer of the OSI reference model is Physical Layer
- The Physical Layer is responsible for the physical connection between devices.
- It defines the hardware elements involved in the network, including cables, switches, and other physical components.
- Physical layer contains information in the form of Bits
- This layer is responsible for transmitting individual bits from node to the other.
- Facilitated functions like:
    - Bit synchronization
    - Bit rate control
    - Transmission mode like simplex, hald-duplex and duplex



3.2. TCP/IP Reference Model

- TCP/IP is a 4 layered network
  - Application Layer
  - Transport Layer
  - Network Layer
  - Network Access Layer



Application Layer:

- The application layer is formed by combining the functionalities of the Application Layer, Session Layer, and Presentation Layer from the OSI reference model.
- The application layer is at the top of the transport layer.
- Over the years, many protocols have been added to the application layer, including
  - HTTP
  - STMP
  - RTP
  - DNS

- Enables communication between software applications across networks.
- Handles data formatting, encryption, and session management.

Transport Layer:

It is designed to allow peer entities on the source and destination hosts to carry on a conversation, just as in the OSI transport layer. Two End-to-end transport protocols have been defined here

Transmission Control Protocol: that allows a byte stream originating on one machine to be delivered without error on any other machine in the internet. It segments the incoming byte stream into discrete messages and passes each one on to the internet layer. At the destination, the receiving TCP process reassembles the received messages into the output stream. TCP also handles flow control to make sure a fast sender cannot swamp a slow receiver with more messages than it can handle.

User Datagram Protocol: is an unreliable, connectionless protocol for applications that do not want TCP's sequencing or flow control and wish to provide their own. It is also widely used for one-shot, client-server-type request-reply queries and applications in which prompt delivery is more important than accurate delivery, such as transmitting
speech or video.

Internet Layer:

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

Network Access Layer:

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

3.3. Comparison of OSI and TCP/IP

Parameter	***Open Systems Interconnection (OSI)***	***Transmission Control Protocol/Internet Protocol (TCP/IP)***
Layer	7 layers	4 layers
	1) Application 2) Presentation 3) Session	1) Application, Presentation and Session layer of OSI are part of Application Layer in TCP/IP
	4) Transport	2) Transport
	5) Network	3) Network layer form TCP/IP is renamed as Internet Layer
	6) Data Link Layer 7) Physical	4) Data Link Layer and Physical Layer from OSI is part of Network Access Layer in TCP/IP
Standardization	Protocol-independent model	Protocol-specific model
Layer Functions	Independent Layer	Functions are combined into broader layers
Flexibility	More flexible in design	More rigid, designed around the protocols
Developed by	ISO (International Organization for Standardization)	DARPA (U.S. Department of Defense)
Protocols	Do not specify protocols	Specifies Standard Protocols