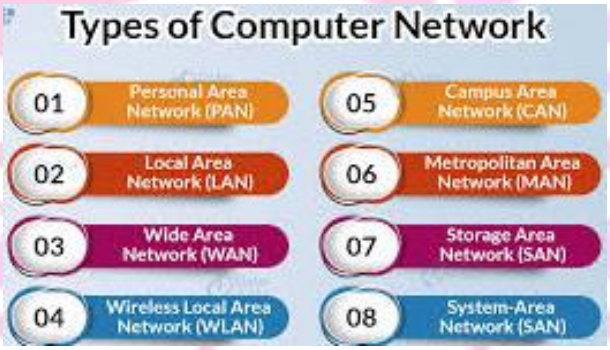
History of Computer Networks

- Early machines like ENIAC were standalone systems for calculations, no networking concept.
- First network ARPANET in 1969.
- TCP/IP created by Vinton Cerf and Robert Kahn which is foundation of modern Internet.
- Domain Name System (DNS) is introduced in 1983, replacing numeric IPs with domain names (e.g., www.google.com).
- World Wide Web (WWW) is invented by Tim Berners-Lee in 1991; enabled hypertext document sharing.

Computer Network

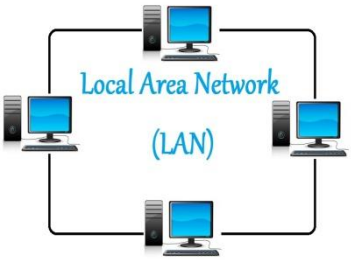
- A computer network is a collection of interconnected devices (such as computers, servers, and peripherals) that communicate and share resources (e.g., data, applications, and hardware) using wired or wireless communication channels.
- Networks range from small (LAN) to global (Internet), supporting collaboration and connectivity.

Types of Computer Network



1. Local Area Network (LAN)

- A LAN is a network that connects computers and devices within a limited geographical area such as a home, office, or campus.
- It ranges within 1 meter to a 5 kilometers.
- It usually owned, operated, and managed by a single organization or individual.
- Ethernet (IEEE 802.3), Wi-Fi (IEEE 802.11) is used as technology.

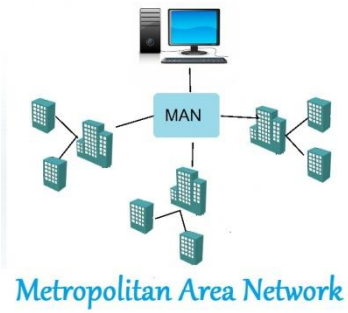


Advantages:
High speed and low latency.
Cost-effective as it uses inexpensive equipment like switches and routers.
Easy to maintain and troubleshoot.

Disadvantages:
Limited range.
Security risks if not properly managed.

2. Metropolitan Area Network (MAN)

- A MAN is a network that spans a city or a large campus, providing connectivity larger than LAN but smaller than WAN.
- It covers a city or metropolitan area 5-50 km.
- Often owned by municipal organizations or telecom companies.
- Fiber Distributed Data Interface (FDDI), Metro Ethernet, and WiMAX.



Advantages:

- Cost-effective for connecting multiple LANs within a city.
- Provides robust disaster recovery capabilities due to redundant paths.

Disadvantages:

- Higher installation and maintenance costs than LAN.
- Requires technical expertise for setup and management.

3. Wide Area Network (WAN)

- A WAN is a network that spans large geographical areas, such as cities, countries, or even continents.
- It is usually owned by multiple organizations or service providers.
- It can span thousands of kilometres across cities, countries, or continents.
- Examples: Internet.

Advantages:

- Covers vast distances.
- Supports large-scale communication and data sharing.
- Enables connectivity across diverse locations.

Disadvantages:

- High cost of setup and maintenance.
- Lower reliability and higher latency compared to LANs.

4. Personal Area Network (PAN)

- A PAN is a network designed for personal use, connecting devices within a very small range (up to 10 meters).
- It is typically owned and managed by a single user.
- Bluetooth, Infrared (IrDA), Zigbee, and USB is used.

Advantages:

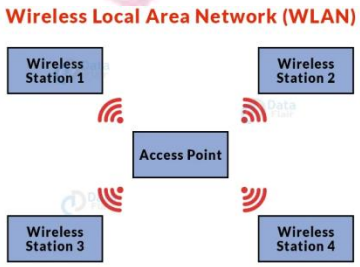
- Convenient and easy to set up.
- Low cost due to limited range and simple devices.
- Promotes mobility and portability.

Disadvantages:

- Limited range and speed.
- Potential security risks from unauthorized access.

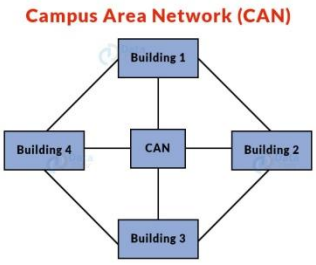
5. Wireless Local Area Network (WLAN)

- WLAN is a form of computer network that functions similarly to a local area network but uses wireless network technologies such as Wi-Fi.
- This network, unlike LAN, lets devices connect wirelessly rather than through physical wires.
- Example: Wi-Fi.



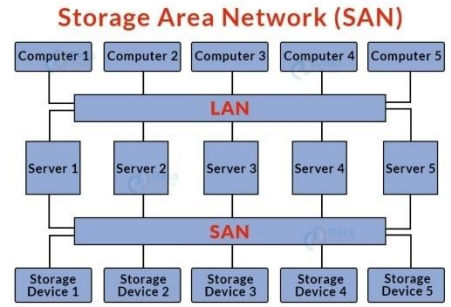
6. Campus Area Network (CAN)

- A CAN network is larger than a LAN but smaller than a MAN network.
- This is a sort of computer network that is commonly seen in locations such as a school or college.
- This network has a limited geographical coverage, since it is dispersed among various buildings on campus.
- Example: Networks that cover schools, colleges, buildings, etc.



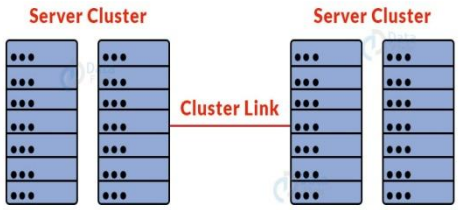
7. Storage Area Network (SAN)

- A storage area network (SAN) is a high-speed computer network that links groups of storage devices to several servers.
- This network is not reliant on LAN or WAN. A SAN, on the other hand, transfers storage resources from the network to its own high-powered network.
- A SAN allows you to access block-level data storage.
- Example: Servers that access a network of disks.



8. System area network

- A system area network (SAN) is a sort of computer network that connects a group of high-performance machines.
- It is a network with a high bandwidth and a focus on connections.
- A SAN is a sort of LAN that can handle enormous volumes of data in big requests.
- This network is ideal for processing applications that need a high level of network performance.
- Example: Microsoft SQL Server 2005 using virtual interface adapter.



Internet

- The Internet is a global network of interconnected devices and networks that communicate using standardized protocols (TCP/IP).
- It allows users to access and share information, communicate, and utilize services globally.
- Global Connectivity: Connects billions of devices worldwide.
- Scalability: Accommodates new devices and technologies seamlessly.
- Interoperability: Supports diverse hardware, software, and networks using standardized protocols.
- Decentralization: No single entity controls the entire Internet.
- Accessibility: Available to users via ISPs (Internet Service Providers) and public access points.

1. Intranet

- An intranet is a private network accessible only to authorized users within an organization.
- It is designed to facilitate internal communication, collaboration, and resource sharing.
- Restricted access; only employees or members of the organization can use it.
- Secure, as it operates within the organization's internal firewall.
- Often includes tools like internal email, shared file storage, employee directories, and company portals.

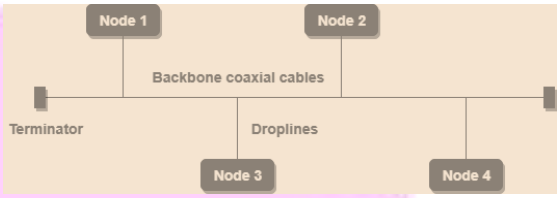
2. Extranet

- An extranet is an extension of an intranet that allows external stakeholders (e.g., clients, vendors, partners) limited access to specific organizational resources.
- Combines internal and external communication.
- Access is granted to specific users outside the organization via secure authentication.
- Often used for collaboration with third parties, sharing project data, or providing services.

Network Topologies

1. Bus Topology

- A single central cable (backbone) connects all network devices.
- Data travels in both directions along the backbone.
- Terminators are used at both ends of the backbone to prevent signal bounce.
- it is used to build small networks.



Advantages:

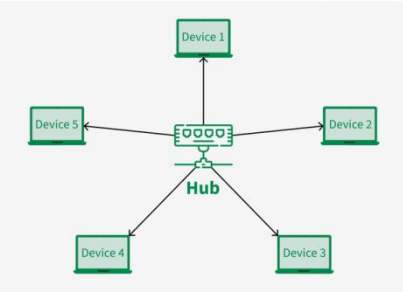
- Simple and inexpensive to implement.
- Requires less cable compared to other topologies.

Disadvantages:

- Limited scalability; performance degrades as devices increase.
- Single point of failure: Backbone failure disrupts the entire network.
- If the network traffic is heavy, it increases collisions in the network. To avoid this, various protocols are used in the MAC layer known as Pure Aloha, Slotted Aloha, CSMA/CD, etc.

2. Star Topology

- All devices are connected to a central device, such as a hub or switch through a cable.
- Data passes through the central device.
- Each device requires a separate connection to the central hub.
- The hub serves as the central node, and it can be either:
- Passive: Non-intelligent, primarily broadcasting signals.
- Active: Intelligent, with built-in repeaters for signal amplification.
- Connections typically use coaxial cables or RJ-45 Ethernet cables, and protocols like CSMA/CD (Carrier Sense Multiple Access with Collision Detection) are commonly employed.



Advantages:

- Requires only N cables to connect N devices, simplifying installation.
- Each device connects to the hub using one port, minimizing complexity.
- A failure in one link affects only that link, not the entire network.
- New devices can be added to the network without disrupting existing connections.
- All data passes through the hub, enabling easier monitoring and control.

Disadvantages:

- If the hub fails, the entire network becomes inoperable.
- Network performance is heavily reliant on the hub's capacity and efficiency.
- All data passes through the hub, which can cause congestion during high traffic.

3. Ring Topology

- In a Ring Topology, each device is connected to exactly two neighboring devices, forming a circular network.
- Data Flow typically unidirectional but can be made bidirectional using Dual Ring Topology (two connections per node).
- Data passes through multiple nodes before reaching its destination, So repeaters used to prevent data loss in large networks
- Uses a token-passing protocol to avoid data collision.
- A token (a special data frame) circulates in the network, granting permission to transmit data.
- Token Ring Protocol is commonly used for managing data transmission.

Advantages:

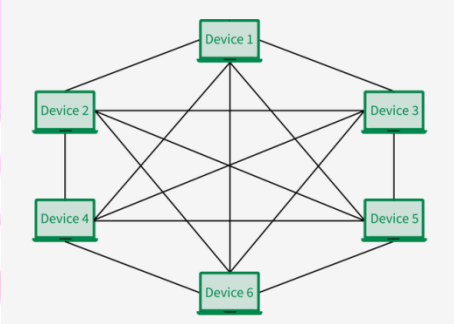
- Equal access to the network for all devices.
- Efficient for small networks with predictable traffic.

Disadvantages:

- A failure in one node or connection can disrupt the entire network.
- Slower data transmission in large networks due to multiple hops.

4. Mesh Topology

- Every device is connected to every other device, either fully or partially.
- The nodes are connected to each other completely via a dedicated link during which information travels from nodes to nodes.
- If a mesh network has N nodes, then there are N(N-1)/2 links.
- Full Mesh: Every node is directly connected to every other node.
- Partial Mesh: Some nodes are connected to all others, while others are only connected to a few.



Advantages:

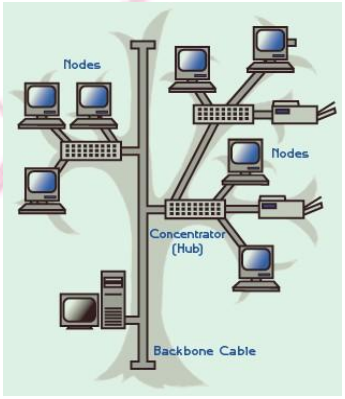
- Network remains functional even if one device fails.
- No traffic issues due to dedicated point-to-point links.
- Offers high privacy, security, and reliable data transmission.
- Adding devices does not disrupt the network.

Disadvantages

- High cost compared to other topologies.
- Complex installation and configuration.
- High power consumption as all nodes remain active.
- Increased maintenance and utility costs.

5. Tree Topology

- A hierarchical topology where devices are connected in the shape of a tree.
- It combines characteristics of star and bus topologies.
- Central nodes act as roots, and branches connect other nodes.
- Data flows through parent-child relationships.



Advantages:

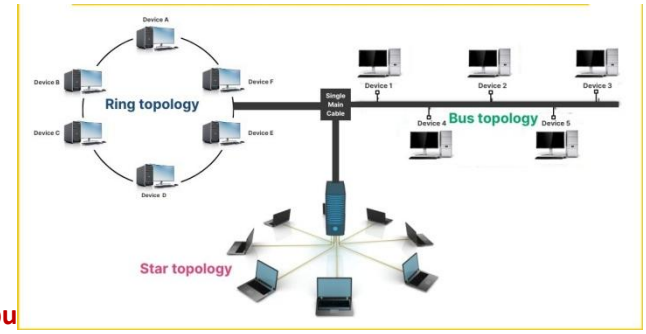
- Scalable and suitable for hierarchical organizations as the leaf nodes can add one or more nodes.
- Fault isolation is easier.

Disadvantages:

- Requires a lot of cable.
- A fault in the backbone can disrupt communication.
- Due to the presence of a large number of nodes, the network performance of tree topology becomes a bit slow.

6. Hybrid Topology

- Combines two or more different topologies into a single network.
- We can mix star, bus, ring, etc., depending on requirements.



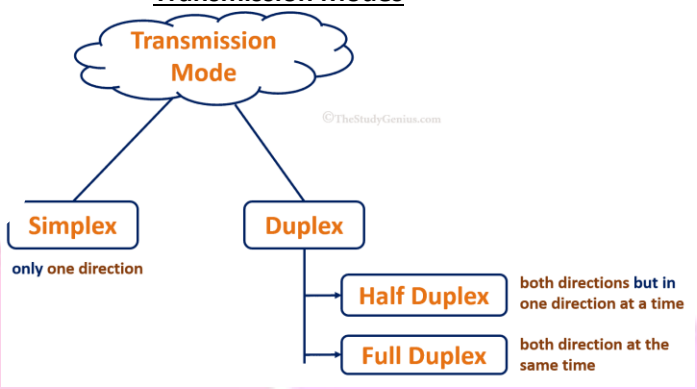
Advantages:

- Highly flexible and scalable.
- Optimized for specific use cases.

Disadvantages:

- Complex to design and maintain.
- Expensive

Transmission Modes

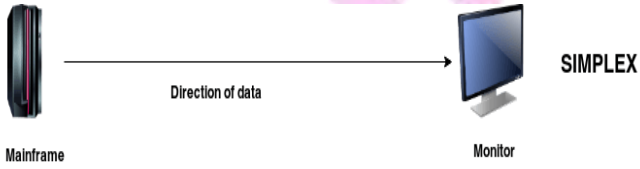


1. Simplex Mode

- Data flows in only one direction. There is no provision for reverse communication.
- Unidirectional communication: Information flows from the sender to the receiver only.
- No feedback: The sender does not receive any acknowledgment or data from the receiver.
- Low complexity: Since no reverse communication is needed, hardware and protocols are simpler.

Example:

- Television broadcasting
- Keyboard to computer



Advantages:

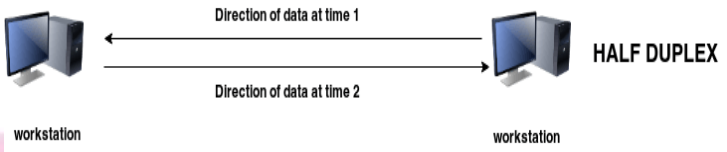
- Simple and cost-effective.
- Efficient for applications where only one-way communication is needed.

Disadvantages:

- Lack of interaction or feedback.
- Not suitable for two-way communication systems.

2. Half-Duplex Mode

- Data flows in both directions, but only one direction at a time. Communication is alternated between sender and receiver.
- Bidirectional communication: Devices can send and receive data but not simultaneously.
- Control mechanism: Requires coordination to determine which device can send or receive at any given time.
- Moderate complexity: More complex than simplex due to the need for direction control.



Example:

- Walkie-talkies: A person can speak (send) or listen (receive) at a time, but not both simultaneously.
- Shared ethernet networks: In traditional shared Ethernet, data flows in one direction at a time.

Advantages:

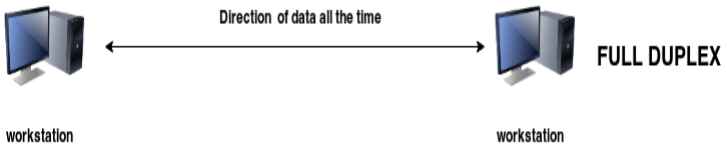
- Allows two-way communication.
- More cost-effective than full-duplex systems.

Disadvantages:

- Slower communication as devices take turns.
- Inefficient for systems requiring simultaneous data flow.

3. Full-Duplex Mode

- Data flows in both directions simultaneously. Both sender and receiver can transmit data at the same time.
- Simultaneous communication: Both devices actively send and receive data.
- Higher bandwidth utilization: Requires channels capable of handling simultaneous flows.
- High complexity: Requires advanced hardware and protocols.



Example:

Telephone conversations: Both participants can speak and listen simultaneously.

Modern networks: Full-duplex Ethernet allows devices to send and receive data at the same time.

Advantages:

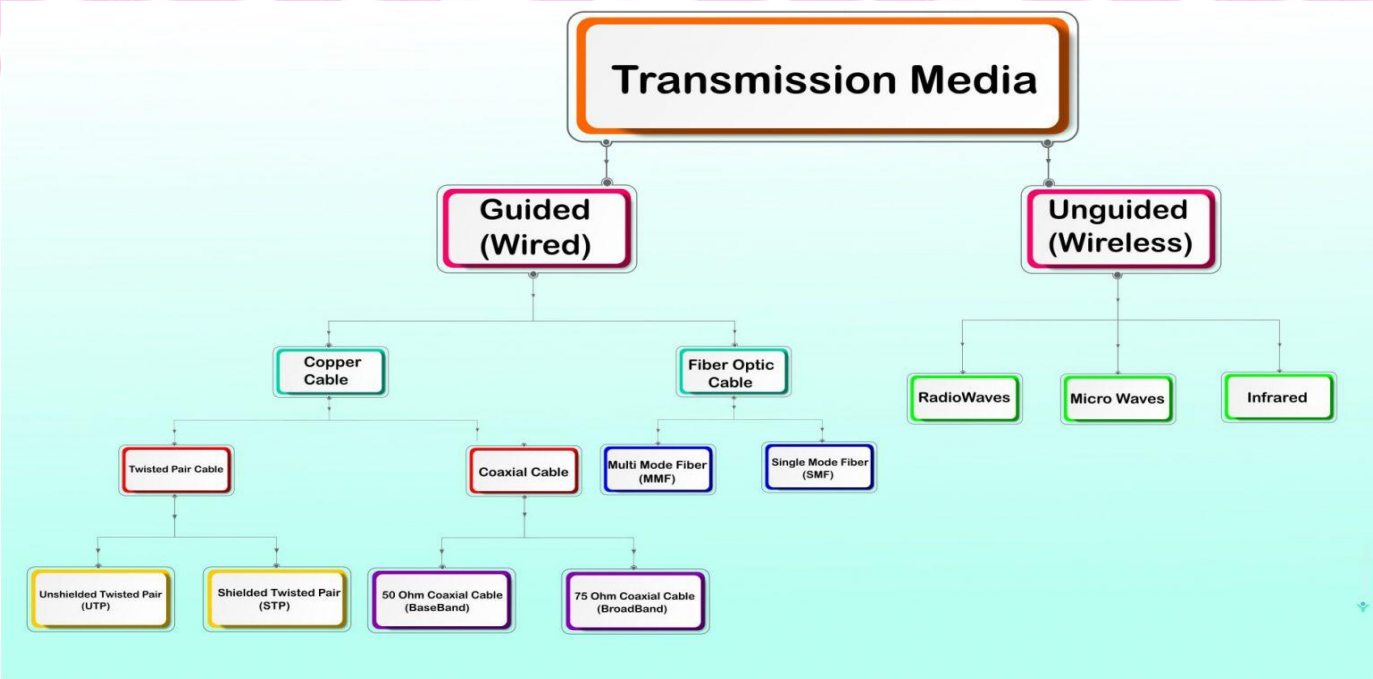
- Fast and efficient communication.
- Ideal for real-time applications like voice and video calls.

Disadvantages:

- Higher cost due to complex hardware and software requirements.
- Requires well-managed infrastructure to avoid interference.

Transmission Media

Transmission media refer to the physical pathways or channels used for transmitting data from one device to another. It plays a critical role in determining the speed, reliability, and efficiency of data communication.

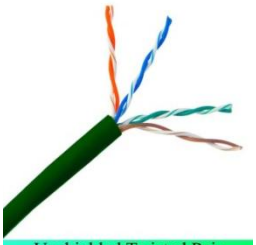


Types of Transmission media

1. **Guided (Wired)**
   - **a)** Twisted Pair Cable
   - **b)** Coaxial Cable
   - **c)** Fiber Optic Cable
2. **Unguided (Wireless) media**
   - **a)** Radio Waves
   - **b)** Microwaves
   - **c)** Infrared (IR)

1. Guided (Wired)

a) Twisted Pair



- A Twisted Pair Cable is a type of communication cable made of two insulated copper wires twisted together.
- It is widely used for data and voice transmission in networks.
- Twisting the wires helps reduce interference and crosstalk from external sources.

Types of Twisted pair

1. **Unshielded Twisted Pair (UTP):**
   - No additional shielding; cost-effective and commonly used in Ethernet networks.
   - Example: Cat5, Cat6 cables.
2. **Shielded Twisted Pair (STP):**
   - Additional metallic shielding around the twisted wires for extra protection.
   - Better resistance to interference but more expensive than UTP.

Data Transmission:

- Supports analog and digital transmission.
- Commonly used for telephone lines and network cables.

Advantages

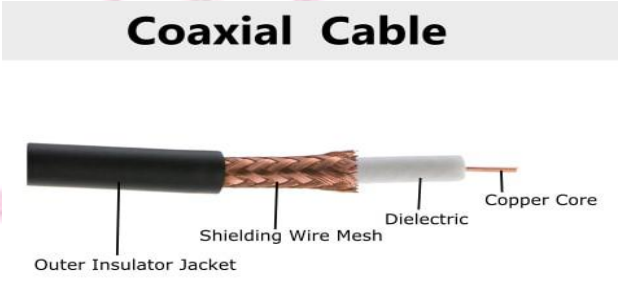
- Cost-Effective: Cheaper than other guided media like coaxial and fiber optic cables.
- Flexible and Easy to Install: Lightweight and simple to handle.
- Widely Available: Easily found and used in most network setups.

Disadvantages

- Limited Bandwidth: Cannot support very high data rates.
- Short Distance: Suitable for short-range communication only.
- Prone to Interference: Susceptible to electromagnetic interference (more in UTP).

b) Coaxial Cable

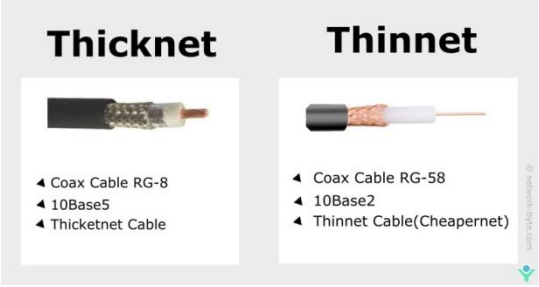
- A coaxial cable (coax cable) is a high-frequency transmission cable with low signal loss.
- It has a single solid copper core surrounded by insulation, a metallic shield, and an outer cover.
- This design prevents electromagnetic interference and helps transmit radio frequency (RF) signals as transverse electromagnetic waves.
- It is commonly used in cable TV, broadband, and CCTV systems.



The coaxial cable transmits information in two modes:

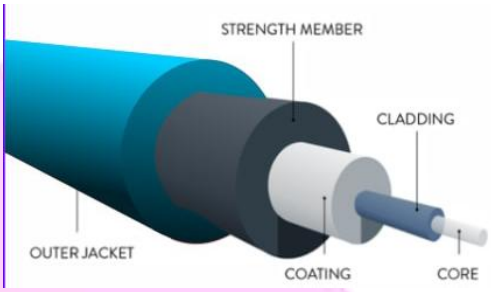
a) **Baseband mode**
b) **Broadband mode**.

There are two types coaxial cables based on Impedance: 75 Ohm Coaxial Cable and 50 Ohm coaxial Cable



c) FIBER OPTIC CABLE

- The world of telecommunications is rapidly moving from copper wire networks to fiber optics due to higher capacity bandwidth in fiber Optic cable.
- Fiber optics are now in widespread use, and form the backbone of most telecommunications networks.
- Fiber-optic cabling contains long thin strands of pure glass or plastic fiber.
- Fiber optic cable is composed of two layers of glass: The core, which carries the actual light signal, and the cladding, which is a layer of glass surrounding the core. The cladding has a lower refractive index than the core. This causes Total Internal Reflection within the core.



Advantages:
Extremely high bandwidth, immune to electromagnetic interference, supports long-distance communication.

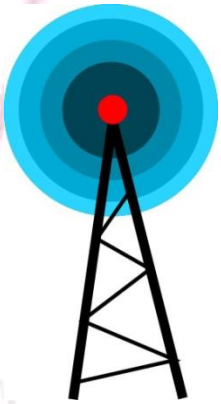
Disadvantages:
Expensive, complex installation, and maintenance.

2. Unguided Media (Wireless Media)

- Unguided Transmission is also known as Unbounded Transmission where Data signal are not bonded to cable media.
- In Unguided media signal are transmitted as electromagnetic signal through air.
- Unguided signals can travel from the source to the destination in several ways: Gound propagation, Sky propagation and Line-of-sight propagation.

This transmission uses different kinds of waves:

a) Radiowaves
b) Microwaves
c) Infrared waves



a) Radio Wave

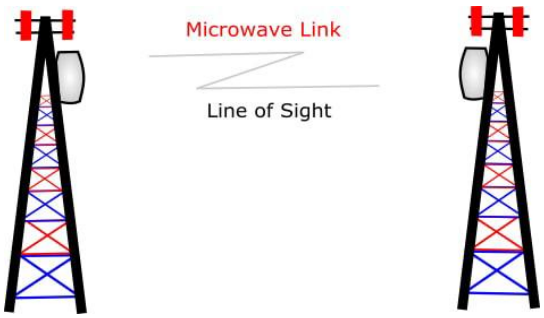
- Radio waves are electromagnetic waves with wavelengths ranging from 1 mm to 100 km (frequencies between 3 kHz to 300 GHz).
- They are omnidirectional, meaning they travel in all directions from the source.
- Generated by radio transmitters and received by radio receivers, both use antennas to transmit and capture signals.
- Radio waves are used in mobile communication, AM/FM radio, and television broadcasting.

b) Microwaves

- Microwaves are high-frequency radio waves (300 MHz to 300 GHz) used for line-of-sight communication, where sending and receiving antennas must be properly aligned.
- They have small wavelengths, allowing signals to focus into narrow beams, ideal for point-to-point communication.
- Microwaves cannot penetrate walls and are unidirectional, making them useful for unicast communication (one-to-one).

Applications:

- Satellite communication
- Radar and navigation
- Wireless LANs and cellular networks
- Remote sensing



c) Infrared

- Infrared signals have frequencies between 300 GHz to 400 THz and are used for short-range communication in closed areas with line-of-sight propagation.
- Their high frequency prevents interference between systems but limits their use outdoors due to interference from sunlight.

Applications:

- TV remotes
- Wireless speakers
- Automatic doors
- Infrared thermometers

Analog vs Digital Signals

Feature	Analog Signals	Digital Signals
Nature	Continuous	Discrete
Representation	Smooth waveform	Square waves (binary)
Noise Resistance	Low	High
Signal Quality	Degrades over distance	Maintains quality over distance
Encoding Methods	AM, FM, PM	NRZ, Manchester, ASK, FSK, PSK
Applications	Radio, TV	Internet, digital phones
Cost	Lower	Higher

Network Devices

Network devices are hardware components that connect and manage communication between different devices in a network.
They facilitate data transfer, ensure security, and manage network traffic.

1. Hub

- A basic device that connects multiple devices in a network and broadcasts data to all connected devices.
- It works on Physical Layer.
- It does not filter data and Broadcasts incoming data to all connected devices.
- Data collisions occur frequently as all devices share the same communication channel.

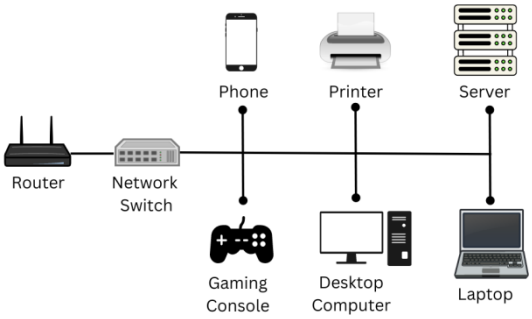
Applications: Small networks with minimal traffic.

Types of Hubs:

1. **Passive Hub:** Only connects devices without amplification.
2. **Active Hub:** Amplifies and regenerates signals.
3. **Intelligent Hub:** Includes additional monitoring features.

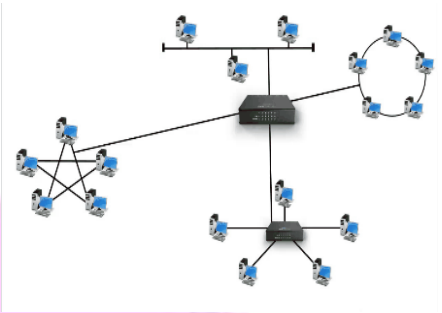
2. Switch

- A device that connects multiple devices and forwards data based on MAC addresses.
- It works on Data Link Layer.
- Filters and forwards data to the intended recipient.
- Reduces network collisions.
- Applications: Used in LANs for efficient communication.



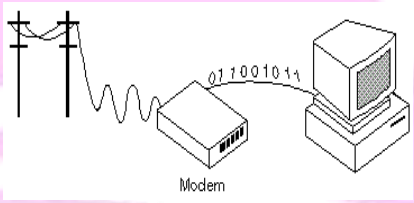
3. Router

- A device that connects different networks and forwards data based on IP addresses.
- It works on Network Layer device.
- It directs data packets to the correct destination.
- A router forwards the packet based on the information available in the routing table.
- It supports wired and wireless communication.
- Applications: Connecting home or office networks to the internet.



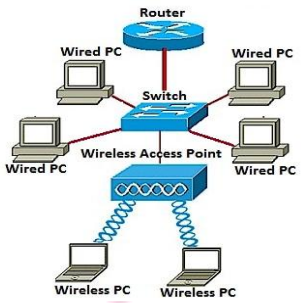
4. Modem

- A device that converts digital signals to analog for transmission over telephone lines and vice versa.
- It operates at the Physical Layer.
- It facilitates internet access over traditional lines.
- It supports DSL, cable, and fiber connections.
- Applications: Home and office internet connectivity.



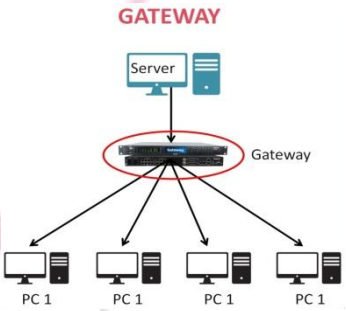
5. Access Point (AP)

- An access point (AP) is a device that connects wireless devices, like smartphones and laptops, to a wired network.
- It creates a Wi-Fi network, allowing devices to communicate with the internet or other devices.
- Access points are used to extend network coverage or provide Wi-Fi in areas without it, commonly found in homes, offices, and public places.



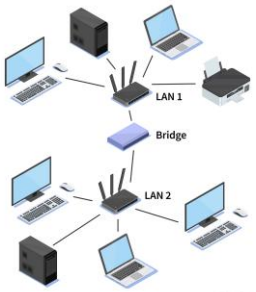
6. Gateway

- A device that connects two different networks using different protocols.
- Gateways are also called protocol converters and can operate at any network layer.
- It take data from one system, interpret it, and transfer it to another system.
- Acts as an entry/exit point for networks.
- Applications: Connecting corporate networks to the internet.



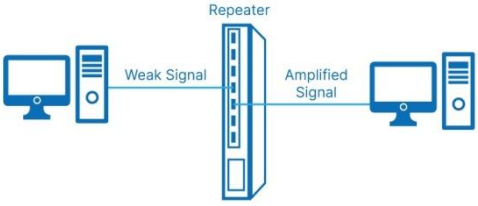
7. Bridge

- A device that connects two or more LANs, forwarding data based on MAC addresses.
- It operates on Data Link Layer.
- Filters and forwards traffic between LAN segments.
- Reduces traffic and improves performance.
- Applications: Dividing large networks into smaller segments.



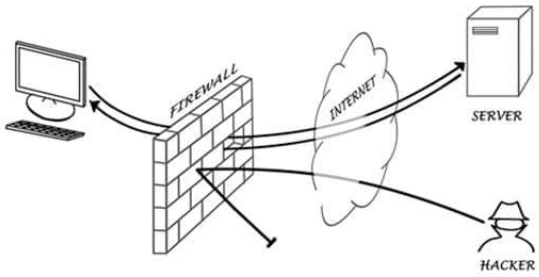
8. Repeater

- A repeater operates at the physical layer and amplifies or regenerates weak signals to extend their transmission range.
- It copies the signal bit by bit and restores it to its original strength, allowing it to travel further.
- A repeater is a 2-port device used to strengthen signals in a network.Applications: Extending LANs or WANs over large distances.
- It cannot filter data.



9. Firewall

- A device or software that monitors and controls incoming/outgoing network traffic based on security rules.
- It operates at Network Layer and Transport Layer.
- It Protects against unauthorized access.
- It Blocks malicious traffic.
- Firewalls can be hardware, software, or cloud-based services(Delivered as a service via the cloud (SaaS).



Functions of a Firewall

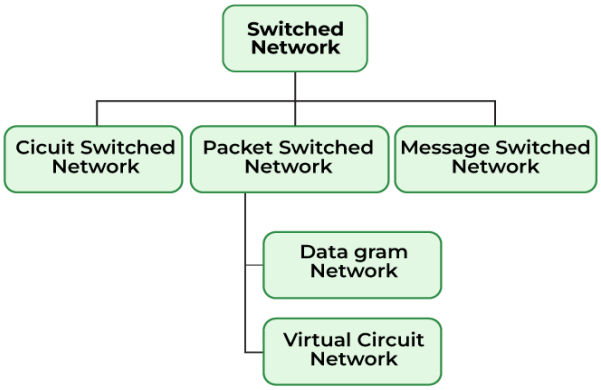
1. Traffic Filtering:
2. Access Control:
3. Packet Inspection:
4. Monitoring and Logging:
5. Protecting Against Attacks:

10. Network Interface Card (NIC)

- NIC stands for network interface card.
- NIC is a hardware component used to connect a computer with another computer onto a network
- 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.
- It operates at Data Link Layer.
- Applications: Connecting computers, printers, and servers to networks.

Switching Techniques in Communication Networks

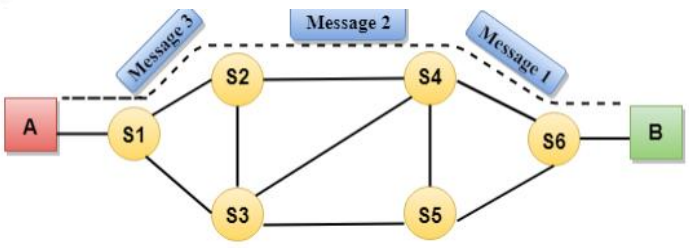
Switching techniques are the methods used to establish a path for data transmission between two points in a network. These techniques play a crucial role in ensuring efficient communication, especially in large and complex networks.



There are three primary types of switching techniques used in telecommunication systems:

1. Circuit Switching

- Circuit switching is a method of communication in which a dedicated communication path (or circuit) is established between two nodes (sender and receiver) for the duration of the transmission.
- Once the circuit is established, the entire bandwidth of the path is reserved for the communication session until it is terminated.
- It is used in real-time communication applications like voice calls, where a dedicated path is necessary.



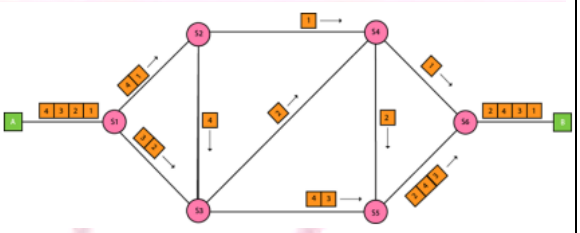
- Communication through circuit switching has 3 phases:
  1. **Circuit establishment**
  2. **Data transfer**
  3. **Circuit Disconnect Circuit**
- Example: Traditional Telephone Network: When you make a phone call, a circuit is established between your phone and the recipient's phone, and the entire connection is reserved for the duration of the call.

Advantages:
- Dedicated Path: Provides a constant, predictable, and stable connection.
- Low Latency: Because the path is dedicated, there is minimal delay during communication.
- No Interference: The reserved path ensures no data interference from other users.

Disadvantages:
- Inefficient Resource Usage: The dedicated path remains idle if no data is being transmitted, which leads to inefficient use of network resources.
- Scalability Issues: For large networks, circuit switching can become inefficient as each communication requires dedicated resources.

2. Packet Switching

- Packet switching is a method of communication in which data is divided into smaller chunks called packets, which are transmitted separately over the network.
- Each packet may take a different route to reach the destination, where they are reassembled into the original data.
- Example: Internet: When you send an email or load a web page, the data is split into packets that travel through various network routers. Once they reach the destination, they are reassembled to present the content.
- There are three main types of packet switching:
  1. Datagram Switching
  2. Virtual Circuit Switching
  3. Hybrid Switching



Datagram Switching: Datagram Switching is the simplest form of packet switching, where each packet is treated independently and can take different routes to reach the destination.

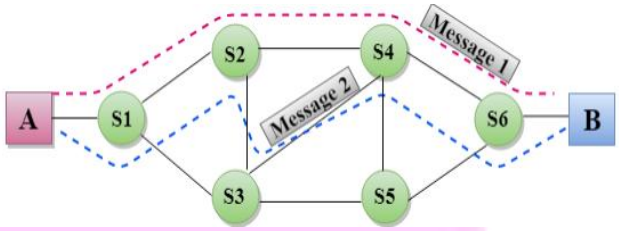
Virtual Circuit Switching: establishes a logical connection between the sender and receiver before transmitting data. Once the virtual circuit is set up, all packets follow the same predefined path.
Example: Telephone Networks (VoIP)

Advantages:
- Efficient Resource Usage: Network resources are shared among multiple users, allowing more flexible use of bandwidth.
- Fault Tolerance: If one path is congested or down, packets can be rerouted dynamically, ensuring better reliability.
- Scalability: Easier to scale because the network can handle multiple communications simultaneously without reserving dedicated paths.

Disadvantages:
- Delay and Jitter: As packets may take different routes, delays can occur, and packets may arrive out of order, causing jitter (variability in delay).
- Overhead: Additional overhead for managing packets (such as addressing and sequencing) can reduce the efficiency of the system.

3. Message Switching

- Message switching is a technique where the entire message is transmitted as a single unit (message) from the sender to the receiver.
- In message switching, each node stores the message temporarily and forwards it when the next node is available.
- It does not require a dedicated circuit like circuit switching.
- Example: Telegraph Networks: In older telegraph systems, messages would be stored at intermediate points and forwarded to the next station until they reached the recipient.



Advantages:

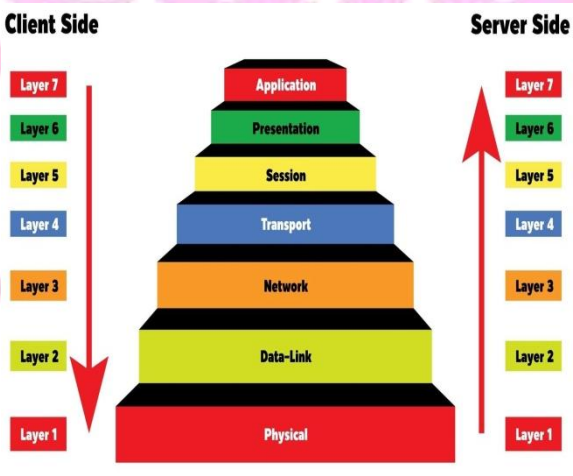
- No Dedicated Path: No need for a dedicated path to be reserved for communication, leading to better resource utilization.
- Efficient for Large Messages: Can handle large messages more efficiently than packet switching in some cases.

Disadvantages:

- Delay: Since the message is stored and forwarded at each node, it can introduce significant delays, especially if the network is congested.
- Limited Real-time Communication: Not suitable for real-time applications like voice or video communication, which require minimal delay.

OSI Model

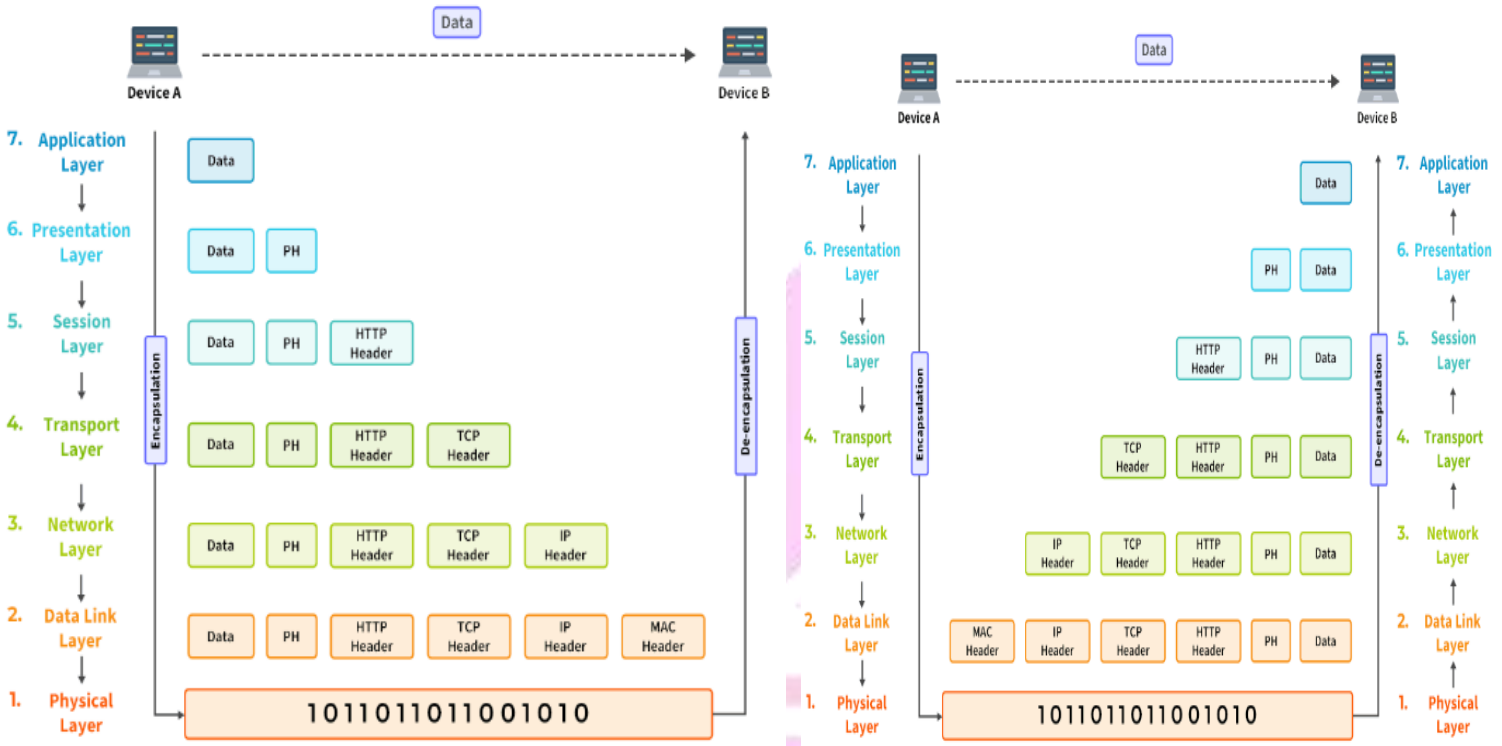
- The OSI (Open Systems Interconnection) Model is a conceptual or reference model that explains how different computer systems communicate over a network.
- OSI Model was developed by the International Organization for Standardization (ISO) in 1984.
- The OSI model creates a standard set of rules for all networking systems to follow.
- It helps different devices and technologies work together.
- The model divides networking tasks into smaller, easy-to-handle layers.
- It makes finding and fixing network problems simpler by focusing on specific layers.



Layers of the OSI Model

There are 7 layers in the OSI Model and each layer has specific roles and interacts with the layers directly above and below it.

1. Physical Layer
2. Data Link Layer
3. Network Layer
4. Transport Layer
5. Session Layer
6. Presentation Layer
7. Application Layer

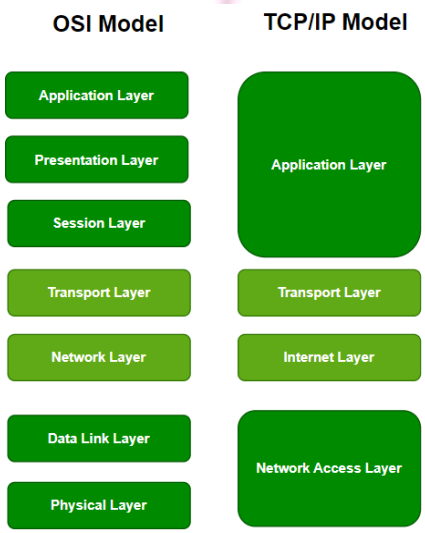


TCP/IP Model (Transmission Control Protocol/Internet Protocol Model)

The TCP/IP model was developed by the Department of Defense (DoD) in the 1970s and adopted as the protocol standard for ARPANET in 1983.

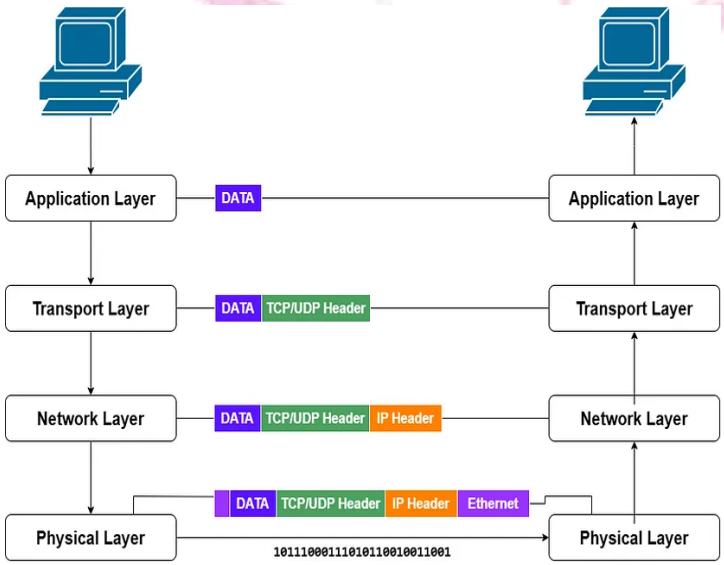
On the basis of OSI model TCP/IP model is implemented to communicate with different devices over the internet.

the OSI model serves as a theoretical foundation, while the TCP/IP model drives real-world network communications.



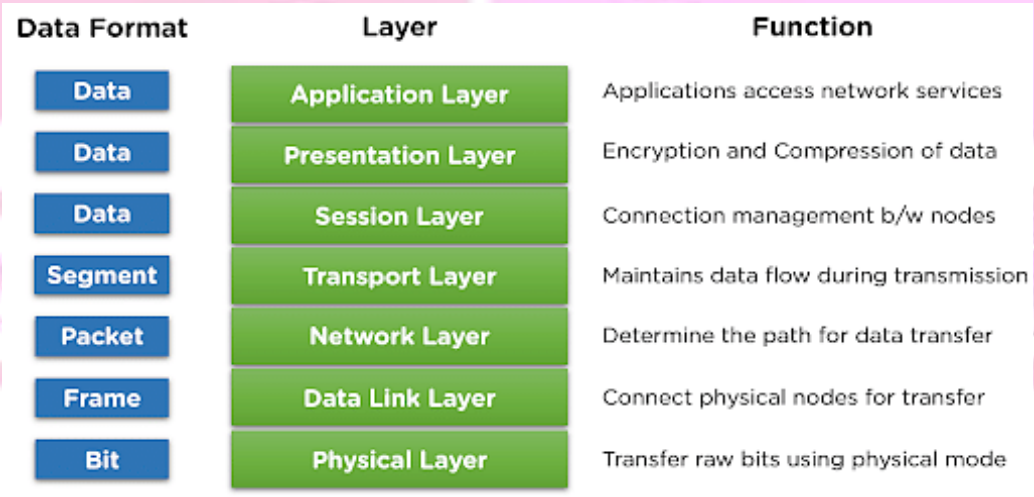
TCP/IP Model has 4 layers:

1. Network Access Layer (Physical and Data link Layer)
2. Internet Layer
3. Transport Layer
4. Application Layer



Comparison between OSI Model and TCP/IP Model

Aspect	OSI Model	TCP/IP Model
Purpose	Conceptual framework for understanding networking.	Practical model for internet communication.
Layers	Comprises 7 layers.	Comprises 4 layers.
Focus	Theoretical and modular understanding of networks.	Implementation and operation of real-world protocols.
Protocol Definition	Does not define specific protocols.	Defines specific protocols like TCP, IP, HTTP.
Flexibility	Rigid and standardized structure.	Flexible and adaptable for evolving technologies.
Error Handling	Distributed across multiple layers.	Managed primarily in the Transport Layer.
Real-World Usage	Ideal for network design and troubleshooting.	Backbone of the internet (e.g., web browsing, email).



Layers of the OSI Model

1. Physical Layer:

- The Physical Layer is the first and lowest layer in the OSI (Open Systems Interconnection) model.
- It deals with the physical and electrical aspects of data transmission over a network.
- This layer is responsible for the actual transmission of raw binary data (bits) as electrical signals, light pulses, or radio waves through physical media.

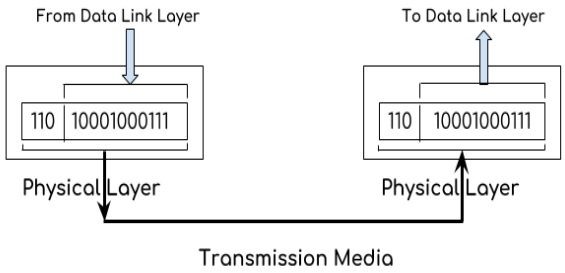
Responsibilities of the Physical Layer

1. Bit Transmission:

- Converts data into binary bits (0s and 1s) and transmits them as signals (electrical, optical, or radio).
- Ensures the accurate transmission and receipt of these signals between devices.

2. Communication Channel:

- It defines how devices can be connected physically, for examples include twisted-pair cables, fiber optics, and coaxial cables for wired communication and Wi-Fi, Bluetooth for wireless communication.



3. Signal Encoding and Modulation:

- It determines how binary data is encoded into signals suitable for transmission (e.g., NRZ, Manchester encoding) and handles modulation techniques (e.g., AM, FM, PM) for signal transmission over analog mediums.

4. Bit Synchronization:

- The physical layer provides the synchronization of the bits by providing a clock. This clock controls both sender and receiver thus providing synchronization at the bit level.

5. **Bit (data) Rate Control:** The Physical layer also defines the transmission rate i.e. the number of bits sent per second.
6. **Topology and Network Design:**
   It specifies the network topology, such as bus, star, ring, or mesh.
   It ensures proper configuration of devices for efficient communication.
7. **Physical Interfaces and Connectors:** It use standardizes interfaces like RJ45 for Ethernet, USB, and fiber optic connectors and ensures compatibility between different hardware components.
8. **Transmission Model:** It defines the direction of data flow like Simplex, Half-Duplex, Full-Duplex.
9. **Network Devices:** Hubs Repeaters Modems and cables are used in physical layer.
10. **Protocols:** No specific protocols; deals with hardware standards (e.g., RS-232, Ethernet physical standards).

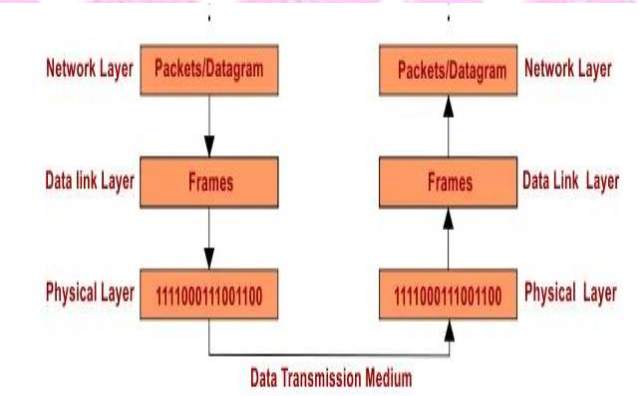
Challenges Addressed by the Physical Layer

1. **Signal Loss (Attenuation):** Over long distances, signals weaken and require amplification or regeneration (handled by repeaters).

2. **Interference (Noise):** External factors like electromagnetic interference (EMI) can distort signals. Shielded cables like STP (Shielded Twisted Pair) are used to mitigate this.

2. Data Link Layer

- The Data-link layer is the second layer from the bottom in the OSI (Open System Interconnection) network architecture model.
- It is responsible for the node-to-node delivery of data.
- Its major role is to ensure error-free transmission of information.
- DLL is also responsible to encode, decode and organize the outgoing and incoming data.
- This is considered the most complex layer of the OSI model as it hides all the underlying complexities of the hardware from the other above layers.
- It deals with MAC addresses. Mac address is physical address which is of 48 bits address.
- Networking devices used in data-link-layer are Bridges, Switches, Network Interface Card (NIC) etc.

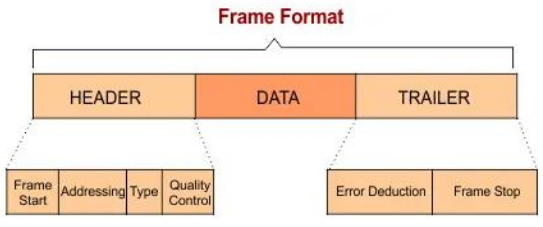


At Sender Side: Data link layer receives packets/datagram from network layer and convert these packets/datagrams to frames and transmit these frames to physical layer.

At Receiver Side: Data link layer receives bits from physical layer and convert these bits to frames and transmit these frames to network layer.

Responsibilities of the Data Link Layer

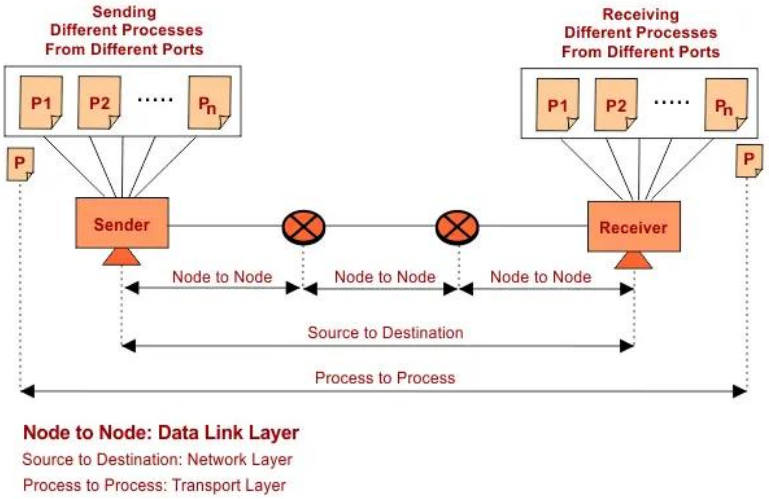
1. **Framing:**
   - It encapsulates raw bits from the Physical Layer into frames, which are structured units of data.
   - Each frame includes headers and trailers that provide necessary information for transmission and error handling.



2. **Node to Node Connection:**
   - To reach the data at destination it first pass through different intermediate nodes (i.e. Routers) which is done through data link layer.
   - Node is also known as hop.

3. **Addressing:** The data link layer encapsulates the source and destination's MAC address/ physical address in the header of each frame to ensure node-to-node delivery. MAC address is the unique hardware address that is assigned to the device while manufacturing.

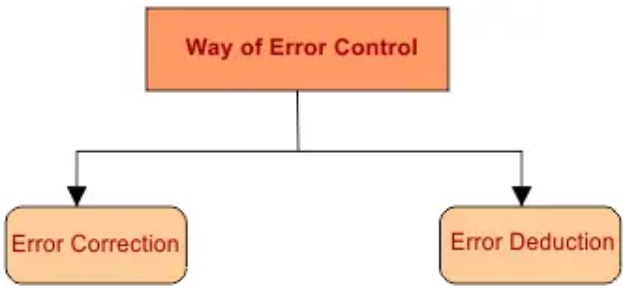
4. **Flow Control:**
   - Sometimes, one node has higher speed and capacity than other nodes. Then sending speed may be higher than receiver node. So, flow control comes into the picture.
   - Thus, data link layer control the flow of data node to node.
   - But the Transport layer deals with source to destination flow control.
   - It uses the Stop and wait and Sliding window protocols to control the flow of data.



5. **Error Control:**
   - The Data Link Layer uses error control to ensure accurate data frame transmission between sender and receiver.
   - It detects errors or losses during transmission and retransmits corrupted or missing frames.
   - While not mandatory, error control optimizes data accuracy and reliability in communication.
   - Errors can occur during data transmission due to noise, signal attenuation, interference, or hardware malfunctions.
   - These mechanisms identify errors and attempt to correct them when possible, ensuring data integrity.

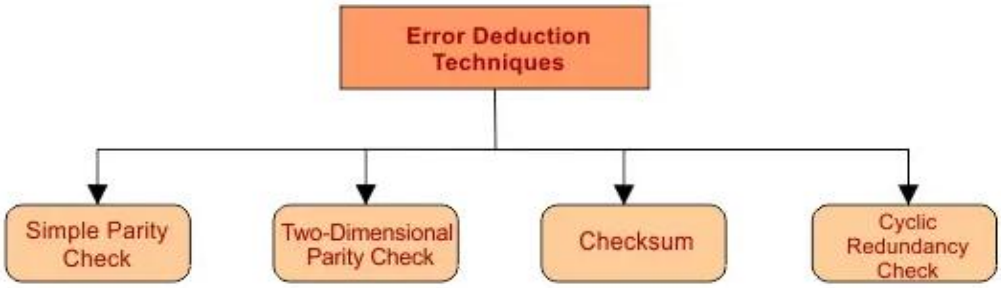
Types of Errors

1. **Single-Bit Error:**
   A single bit in the data unit is altered (e.g., 10110101 becomes 10110111).
   Example: A 0 becomes 1, or vice versa, due to electrical interference.
2. **Burst Error:**
   Two or more bits in the data unit are altered.
   Example: 10110101 becomes 11100101 due to a prolonged noise burst.
3. **Packet Loss:**
   Entire frames may get lost during transmission.
   Example: A frame sent over a congested network might never reach the destination.



Error Detection

Error detection means identification of errors.



Error Detection Techniques

1. **Parity Check:** Adds a single parity bit to the data to indicate whether the number of 1s in the data is odd or even.

Types:

- **Even Parity:** The parity bit is set to make the total number of 1s even.
- **Odd Parity:** The parity bit is set to make the total number of 1s odd.

Limitation: Detects only single-bit errors, not burst errors.

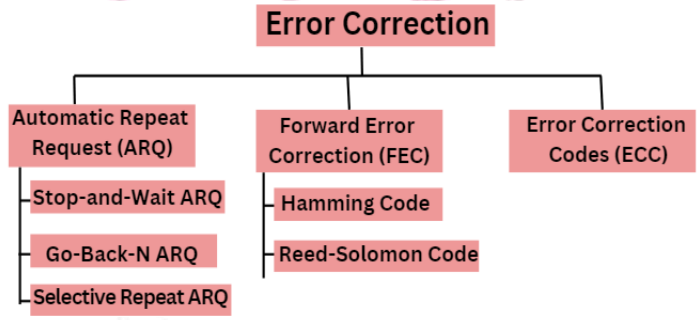
2. **Checksum:** Treats data as a sequence of integers. Calculates the sum of all integers and transmits it with the data. At the receiver, the sum is recalculated and compared with the received checksum.
This method uses a Checksum Generator on the sender side and a Checksum Checker on the receiver side.
Example: Data: 1001 1101 1010 Checksum: 110110
Transmitted: 1001 1101 1010 110110
Limitation: A checksum primarily detects single-bit errors and some multiple-bit errors, but it cannot guarantee detection of all multiple-bit errors i.e. less effective for detecting burst errors.

3. **Cyclic Redundancy Check (CRC):**
   - A polynomial-based method that adds a CRC value (remainder of a polynomial division) to the data.
   - At the receiver, the CRC is recalculated and compared to detect errors.

   Advantages: Highly effective for burst error detection.

Error Correction Techniques

Error correction means fixing the errors. The error correction method is very costly and hard as well. The best error correction technique at each node of the data link layer is the Hamming Code.



a. **Automatic Repeat Request (ARQ)**
   - Relies on retransmission to correct errors.
   - If an error is detected, the receiver requests the sender to resend the data.

Types:

- Stop-and-Wait ARQ: Sends one frame at a time, waits for acknowledgment before sending the next.
- Go-Back-N ARQ: Allows multiple frames in transit but retransmits from the error point.
- Selective Repeat ARQ: Retransmits only the erroneous frame.

2. Forward Error Correction (FEC)

- Corrects errors at the receiver without retransmission.
- Adds redundancy bits to the data to enable self-correction.

Types:

- Hamming Code: Detects and corrects single-bit errors.
- Reed-Solomon Code: Corrects burst errors in multimedia and storage devices.

3. Error Correction Codes (ECC):

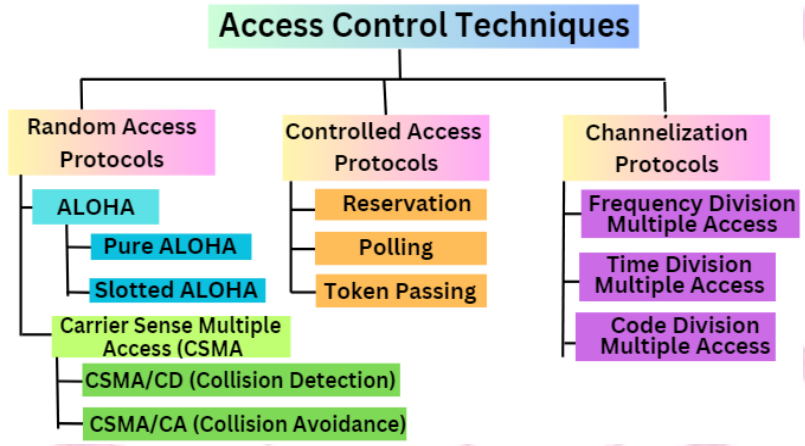
Codes like BCH (Bose–Chaudhuri–Hocquenghem) and LDPC (Low-Density Parity Check) are used in advanced communication systems like satellite and 5G networks.

6. Access Control:

Access control in data link layer manages how devices share and access a communication medium in networks.
It ensures efficient, fair, and collision-free communication, especially in shared or broadcast environments like Ethernet, Wi-Fi, or cellular networks.

Functions of Access Control

1. Medium Access Control (MAC): Manages how devices gain access to the communication medium. It prevents conflicts when multiple devices attempt to transmit data simultaneously.
2. Collision Handling: Detects and resolves collisions when multiple devices send data simultaneously in shared networks.
3. Fairness: Ensures every device gets a chance to transmit data without monopolizing the medium.
4. Efficiency: Optimizes utilization of the communication medium, minimizing idle or wasted time.



Access Control Techniques

1. Random Access Protocols:

Any station can send data depending on medium's state(idle or busy). It has two features:

- There is no fixed time for sending data
- There is no fixed sequence of stations sending data

Relies on techniques to detect or handle collisions.

Types of Random Access Protocols

1. ALOHA (Pure and Slotted): It was designed for wireless LAN but is also applicable for shared medium.

a) Pure ALOHA:

- Devices transmit whenever they have data.
- When a station sends data it waits for an acknowledgement. If the acknowledgement doesn't come within the allotted time then the station waits for a random amount of time called back-off time (Tb) and re-sends the data.

b) Slotted ALOHA:

- Slotted ALOHA is like Pure ALOHA but divides time into slots.
- Devices can only send data at the start of a slot.
- If a device misses its slot, it waits for the next one, reducing collisions.

2. Carrier Sense Multiple Access (CSMA):

- Devices sense the medium (for idle or busy) before transmitting data before transmitting to avoid collisions.
- However there is still chance of collision in CSMA due to propagation delay.

Types of CSMA

a) CSMA/CD (Collision Detection)

- It is used in wired Ethernet.
- Device monitors the medium after it sends a frame to see if the transmission was successful or to detect collisions during transmission.
- If a collision is detected, they stop transmitting and retry after a random backoff time.
- Example: Traditional Ethernet.

b) CSMA/CA (Collision Avoidance):

- Used in wireless networks where collisions cannot be easily detected.
- Devices avoid collisions by waiting for acknowledgments and waiting periods before transmission.
- Example: Wi-Fi networks (802.11).

2. Controlled Access Protocols:

Controlled access protocols ensure that only one device uses the network at a time.
Devices take turns or follow a defined sequence to access the medium, eliminating collisions.

Types of Controlled Access Protocols

a) Reservation: In the reservation method, a station needs to make a reservation before sending data.
The timeline has two kinds of periods:

- Reservation interval of fixed time length
- Data transmission period of variable frames.

If there are M stations, the reservation interval is divided into M slots, and each station has one slot.

b) Polling:

- A central controller polls each device to check if it has data to send.
- Ensures orderly and collision-free transmission.
- Example: Printer queues in a shared network.

c) Token Passing:

- A token (special frame) circulates in the network, granting the right to transmit.
- Only the device holding the token can send data.
- Example: Token Ring networks.

3. Channelization Protocols

- Divide the medium into separate channels to allow simultaneous transmission by multiple devices.
- It allows the total usable bandwidth in a shared channel to be shared across multiple stations based on their time, distance and codes. It can access all the stations at the same time to send the data frames to the channel.

Types of Channelization Protocols

1. **Frequency Division Multiple Access (FDMA)**
   - Assigns different frequency bands to each device.
   - Each device transmits in its designated frequency without interference.
   - Example: Analog cellular networks.

2. **Time Division Multiple Access (TDMA):**
   - Divides the medium into time slots, assigning each device a specific slot.
   - Devices transmit in their designated slots without overlap.
   - Example: GSM cellular networks.

3. **Code Division Multiple Access (CDMA):**
   - Assigns unique codes to each device for simultaneous data transmission over the same frequency.
   - Example: 3G cellular networks.

Data Link Layer Sublayers

1. **Logical Link Control (LLC):**
   - The role of logical link control is to provide logic thus it controls the frame synchronization, flow control, and error control in the data link layer.
   - The LLC sublayer handles both connection-oriented and connectionless transmissions, unlike the MAC sublayer.
   - Link addressing and sequencing also occur at the LLC sublayer.
   - It Interfaces with the Network Layer above and the MAC sublayer below.

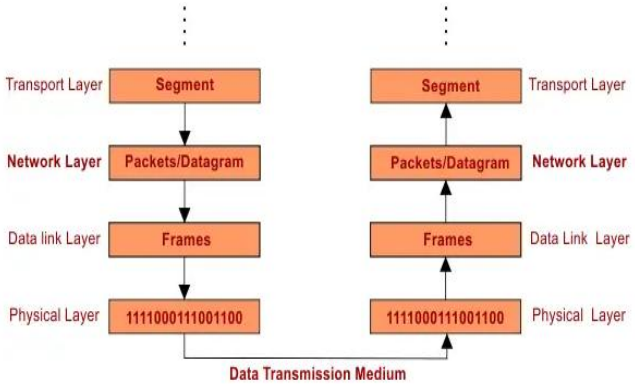
2. **Media Access Control (MAC):**
   - The second sublayer, Media Access Control, deals with the physical addressing of frames.
   - It encapsulates frames to prepare them for transmission, resolves situations that require more than one data frame transmission, and fixes collisions if they should occur.
   - It manages access to the physical medium and controls how frames are placed onto it.

Protocols used in Data link layer:

- Ethernet: Widely used in wired LANs for frame transmission.
- Wi-Fi (IEEE 802.11): Handles wireless communication.
- PPP (Point-to-Point Protocol): Used in direct links between two devices.
- HDLC (High-Level Data Link Control): Ensures reliable point-to-point communication.
- Synchronous Data Link Control (SDLC), which deals with error correction, error recovery, and multipoint link support
- Serial Line Interface Protocol (SLIP), which handles the transfer of IP packets
- Link Control Protocol (LCP), which establishes, configures, tests, maintains, and terminates links when transmitting data frames

3. Network Layer

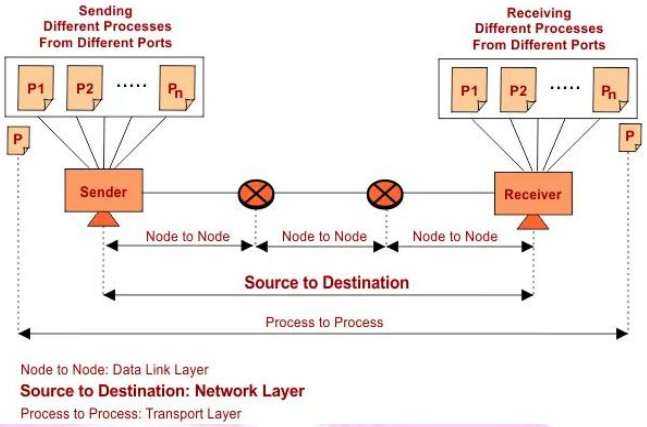
- The Network Layer is the third layer in the OSI model, positioned above the Data Link Layer and below the Transport Layer.
- Its primary role is to manage the delivery of data packets from the source to the destination, even across multiple networks.
- It is responsible for routing, addressing, and delivering data packets across networks.
- **At the Sender Side:** the Network layer receives segments from the transport layer, converts these segments into packets/datagrams, and transmits these packets/datagrams to the data link layer.
- **At the Receiver Side:** the Network layer receives frames from the data link layer, converts these frames to packets/datagrams, and then transmits them to the transport layer.



Functions of the Network Layer:

a. **Logical Addressing:**
- It provides unique addresses (IP addresses) for devices across networks.
- It differentiates devices and ensures accurate data delivery.
- Example: An IP address like 192.168.1.1.

b. **Source to Destination Delivery:**
The network layer provides Source to destination Delivery, which is also called HOST-to-HOST delivery.



c. **Routing:**
- Determines the optimal path for data to travel from source to destination.
- Uses routing algorithms and routing tables to make decisions.

d. **Fragmentation and Reassembly:**
- It breaks large data packets into smaller fragments to match the size limits of the network.
- Reassembles fragments at the destination.
- Example: A video file split into smaller packets for transmission.

e. **Error Handling and Diagnostics:**
- Identifies and resolves routing issues or unreachable destinations.
- ICMP (Internet Control Message Protocol) assist in diagnostics.
- Example: Using the ping command to check network connectivity.

f. **Congestion Control**
When too many devices send data to the same router simultaneously, even with fragmentation, the router's buffer can become full. This can lead to network overload. Managing this overload to ensure smooth data flow is called congestion control. Controlling traffic is called congestion control and it is an important responsibility of the Network Layer.

g. **Traffic Control and QoS (Quality of Service):**
Manages network traffic to ensure timely delivery of critical data.
Example: Prioritizing video call packets over regular emails.

Protocols used in Network Layer

1. **Internet Protocol (IP)**
IPv4 (Internet Protocol Version 4)
IPv6 (Internet Protocol Version 6)

2. **ICMP (Internet Control Message Protocol)**
- It provides error reporting and network diagnostics.
- It reports unreachable hosts, networks, or ports.
- Diagnoses issues using tools like ping and traceroute.
- Example: If a device cannot connect to a website, ICMP sends an error message to the source.

3. **ARP (Address Resolution Protocol)**
It resolves IP addresses to MAC (Media Access Control) addresses.
Example: A device sends an ARP request asking, "Who has IP X?"
The device with the corresponding IP replies with its MAC address.

4. **RARP (Reverse Address Resolution Protocol)**
   - It resolves MAC addresses to IP addresses.
   - Used by diskless workstations or devices to obtain an IP address from a server.

5. **NAT (Network Address Translation):**
   - Translates private IP addresses to a public IP address and vice versa.
   - Conserves IPv4 address space.
   - Provides an extra layer of security by hiding internal network details.
   - Example: A home router using one public IP for all connected devices.

6. **OSPF (Open Shortest Path First):**
   - A routing protocol for finding the shortest path in a network.
   - Uses link-state routing.
   - Suitable for large enterprise networks.
   - Example: Large organizations use OSPF to maintain efficient internal routing.

7. **BGP (Border Gateway Protocol)**
   - Manages routing between autonomous systems (AS) on the internet.
   - Provides path selection for data packets across different networks.
   - Handles internet traffic routing.
   - Example: Internet service providers (ISPs) use BGP to connect to other ISPs.

8. **RIP (Routing Information Protocol)**
   - An older protocol used for routing within small networks.
   - Uses distance-vector routing with hop count as the metric.
   - Limited to 15 hops.
   - Example: Small office networks.

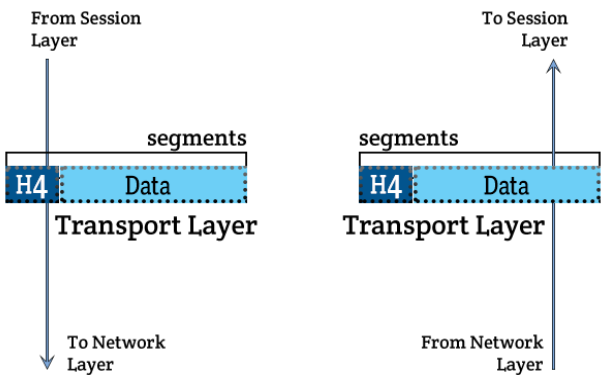
9. **IGMP (Internet Group Management Protocol)**
   - It manages multicast groups for one-to-many communication.
   - Used in video streaming or online gaming.
   - Example: Streaming live sports to multiple viewers.

4. Transport Layer

The Transport Layer is responsible for end-to-end communication between devices in a network.
End-to-end delivery is also called port-to-port or Process-to-process delivery.
It ensures that data is delivered reliably, efficiently, and in the correct order, regardless of the underlying network infrastructure.

Functions of Transport Layer

1. **End-to-end Delivery:**
   - The transport layer is responsible for Port-to-Port Delivery.
   - Transport Layer requires a Port number to correctly deliver the segments of data to the correct process amongst the multiple processes running on a particular host.
   - A port number is a 16-bit address used to identify any client-server program uniquely.



2. **Segmentation and Reassembly:**
- Byte streaming from upper layers is converted into segmentations. Through segmentation, larger pieces of data are divided into smaller segments/blocks. Each segment is identified by its unique segment number. These segments are converted into packets at the network layer.
- Reassembles segments at the receiver side.

3. **Reliable Delivery:**

The transport layer provides reliability by retransmitting the lost and damaged packets. The reliable delivery has four aspects:

a. **Error Control:** It used the checksum algorithm for error deduction. The basic purpose of reliability is Error Control. In this way, the packet has arrived correctly.

b. **Sequence Control:** Reliability also involves the factor of sequence control. It means sending and receiving orders must be the same so that various segments of a transmission can be correctly reassembled.

c. **Loss Control:** The reliability of the transport layer ensures that all the fragments arrive at the destination successfully without losing some of them.
If some segment is missing, then its sequence number identifies it while reassembling.

d. **Duplication Control:** The transport layer also ensures that no duplicate data arrive at the destination.
If some segment is duplicated, then its sequence number identifies it while reassembling. In this way, a duplicate segment is discarded.

4. **Flow Control:**
- If the receiver is overloaded due to the transmission of too much data by the sender, then the receiver discards some packets and requests for the retransmission of discarded packets. These phenomena cause a reduction in the system performance.
- Transport layer regulates the data flow between sender and receiver to prevent overwhelming the receiver.
- The transport layer uses the "sliding window protocol" to handle the flow control.

5. **Connection Establishment and Termination:** It sets up, maintains, and terminates connections between applications.
Example: Before sending data, a connection is established (e.g., using a three-way handshake in TCP).

6. **Multiplexing and Demultiplexing:** It allows multiple applications to share the same network connection by assigning unique port numbers.
Example: A computer can browse the web (port 80) and send emails (port 25) simultaneously using different port numbers.

Protocols in the Transport Layer

1. **Transmission Control Protocol (TCP):**
- Reliable, connection-oriented protocol.
- Ensures error checking, flow control, and retransmission of lost packets.
- Example: Web browsing (HTTP), email (SMTP), and file transfer (FTP) use TCP for reliable communication.

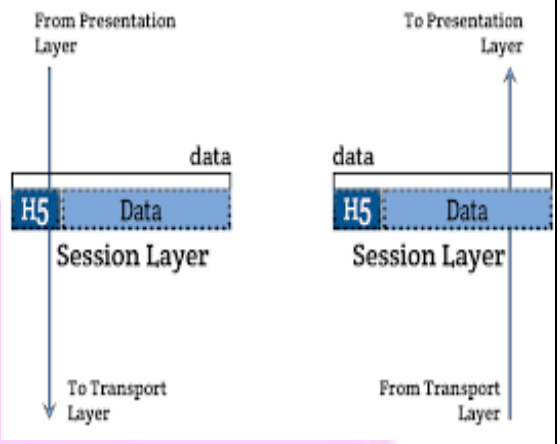
2. **User Datagram Protocol (UDP):**
- Unreliable, connectionless protocol.
- Does not guarantee delivery or order of packets but is faster.

5. Session Layer

- The Session Layer manages and controls the dialog between two devices in a network.
- It establishes, maintains, and terminates communication sessions, ensuring that the data exchange is properly synchronized and organized.

Function of Session Layer

1. **Session Establishment:**
   - Sets up a session between two devices or applications.
   - Example: When a user logs into a remote server using SSH, the Session Layer establishes a secure session.



2. **Session Maintenance:**
   - Keeps the session alive during communication.
   - Monitors the connection to detect interruptions and ensures continuity.
   - Example: During a video conference, the Session Layer maintains the session even if there are minor network fluctuations.

3. **Session Termination:**
   - Closes the session once the communication is complete.
   - Frees up resources and ensures a clean disconnection.
   - Example: When a user logs out of an email client, the session is terminated.

4. **Synchronization:**
   - Adds checkpoints (synchronization points) to the data stream to resume communication from a specific point in case of failure.
   - Example: In a file transfer, if the connection drops, the transfer can resume from the last checkpoint instead of starting over.

5. **Dialog Control:**
   - Manages the flow of data between devices, ensuring proper sequencing and avoiding conflicts.
   - Supports half-duplex (one-way communication at a time) or full-duplex (simultaneous two-way communication).
   - Example: In a chat application, the Session Layer ensures that messages are sent and received in the correct order.

Session Layer Protocols

1. **Remote Procedure Call (RPC):**
   - Allows a program to execute a procedure on a remote system as if it were local.
   - Example: Network File System (NFS) uses RPC to access files on a remote server.

2. **Session Initiation Protocol (SIP):**
   - Used for initiating, maintaining, and terminating real-time communication sessions like VoIP and video calls.
   - Example: SIP is used in Skype or Zoom calls.

3. **NetBIOS:**
   - Provides session management for applications on a local network.

4. **SQL Sessions:**
   - Database management systems use sessions to handle queries and transactions.
   - Example: A session is established when a user connects to a database to run SQL commands.

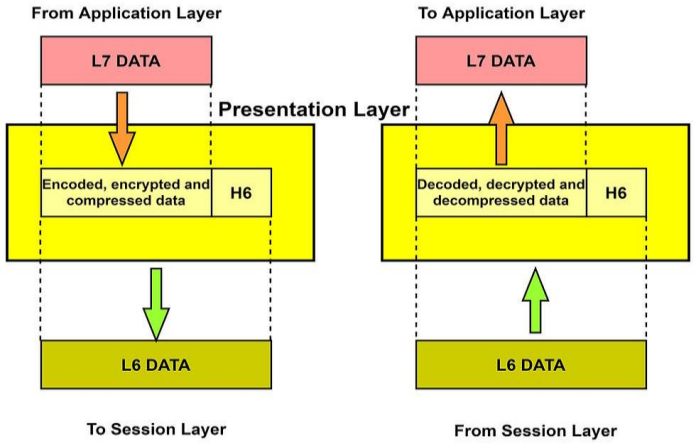
6. Presentation Layer

- The Presentation Layer is responsible for ensuring that data sent by the application layer of one system is readable by the application layer of another system.
- It acts as a translator and performs data formatting, encryption, and compression.

Functions of the Presentation Layer

1. **Data Translation:**
   - Converts data from one format to another to ensure compatibility between different systems.
   - Example: Translating EBCDIC (used in mainframes) to ASCII (used in personal computers).

2. **Data Encryption and Decryption:**
   - Encrypts data before sending it to ensure secure communication.
   - Decrypts received data so that the application can process it.
   - Example: HTTPS uses SSL/TLS protocols to encrypt data during web browsing.



3. **Data Compression and Decompression:**
   - Reduces the size of data to optimize bandwidth usage.
   - Decompresses data at the receiver's end to restore it to its original form.
   - Example: Compressing image files in JPEG format or video files in MP4 format for faster transmission.

4. **Data Formatting:**
   - Ensures data is in a structured format that the receiving application can understand.
   - Example: Converting text into a standard format like XML or JSON for transmission.

5. **Character Encoding:**
   - Handles character set conversions to ensure text data is displayed correctly across different systems.
   - Example: Converting Unicode to UTF-8.

Presentation Layer Protocols

1. **Secure Sockets Layer (SSL)/Transport Layer Security (TLS):**
   - Provides encryption and secure communication for applications like web browsers and email clients.
   - Example: Online banking and shopping websites use HTTPS (SSL/TLS).

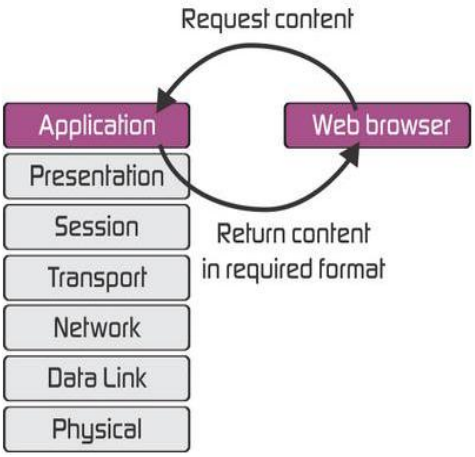
7. Application Layer

- The Application Layer is the topmost layer of the OSI model, directly interacting with the end user.
- It provides network services to applications, enabling communication between software applications on different devices.

Functions of the Application Layer

1. **User Interface:**
   - Provides a platform for users to interact with network services through applications.
   - Example: Web browsers, email clients, and file transfer tools.

2. **Application Services:**
   - Facilitates communication between software applications.
   - Example: Sending an email using an email client like Outlook or Gmail.



3. **Data Communication:**
   - Ensures data is properly structured and ready for transmission.
   - Example: Formatting HTTP requests for web browsing.

4. **Resource Sharing:**
   - Enables access to shared network resources like printers, files, and databases.
   - Example: Accessing a shared folder on a corporate network.

5. **Authentication and Authorization:**
   - Verifies user credentials and permissions for accessing services.
   - Example: Logging into a secured website using a username and password.

6. **Error Handling:**
   - Detects and manages errors in application-level communication.
   - Example: Displaying an error message when an email fails to send.

Application Layer Protocols

1. HTTP/HTTPS (Hypertext Transfer Protocol/Secure)
2. FTP (File Transfer Protocol)
3. SMTP (Simple Mail Transfer Protocol)
4. DNS (Domain Name System)
5. SNMP (Simple Network Management Protocol)
6. POP3: Retrieves emails from a mail server to a client.
7. IMAP: Retrieves emails from a server while keeping them synchronized across devices.
8. Telnet and SSH
9. DHCP (Dynamic Host Configuration Protocol)
10. TFTP (Trivial File Transfer Protocol): Transfers files without requiring authentication.
11. MIME (Multipurpose Internet Mail Extensions)